State of Oklahoma
Office of Management and Enterprise Services

STATE OF OKLAHOMA STATEWIDE CONTRACT WITH GARTNER, INC.

This State of Oklahoma Statewide Contract No. 1026 ("Contract") is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and Gartner, Inc. ("Supplier") and is effective as the date of the last signature to this Contract. The initial Contract term, which begins on the effective date of the Contract, is one (1) year and there are four (4) one-year options to renew the Contract.

Purpose

The State is awarding this Contract to Supplier for the provision of a non-mandatory statewide contract for Information Technology (IT) research and advisory subscription services and consultancy services, to support IT strategic, tactical and operational initiatives underway, as more particularly described in certain Contract Documents. Supplier submitted a proposal which contained additional terms, exceptions to the Solicitation, and with certain information requested to be considered confidential. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.

2. The following Contract Documents are attached hereto and incorporated herein:

   2.1. Solicitation, Attachment A;
   2.2. General Terms, Attachment B;
   2.3. Oklahoma Statewide Contract Terms, Attachment C;
   2.4. State of Oklahoma Information Technology Terms, Attachment D;
   2.5. Information Security Requirements, D1
   2.6. Additional Terms, Attachment E1;
   2.7. Master Terms, Attachment E2;
   2.8. Pricing, Attachment E3;
   2.9. Value-Add, Attachment E4;
   2.10. Third Party, Attachment E5;
   2.11. Negotiated Service Agreement Template, Attachment E6;

2.12. Negotiated Exceptions to Contract, Attachment F;
2.13. Template for Contract Modifications for Quotes, Statements of Work, or other Ordering Documents, Attachment F1; and
2.14. Negotiated Exceptions to State of Oklahoma Information Security, Policy, Information Security Policy, Procedures, and Guidelines, Attachment F2.

3. The parties additionally agree:

3.1. Except for information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.
3.2. Revisions to terms and documents initially proposed in the Bid are contained in Attachment F titled Exceptions.
3.3. Unless mutually agreed to in writing by the Chief Information Officer (CIO) utilizing Attachment F-1, no Contract Document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator shall supersede or conflict with the terms of this Contract or expand the State's or Customer's liability or reduce the rights of Customer or the State. If supplier is acting as a reseller, any third-party terms provided are also subject to the foregoing.
3.4. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.
3.5. To the extent any term or condition in Attachment E1 – Additional Terms or Attachment E3 – Pricing, including via hyperlink or uniform resource locator, conflicts with applicable terms in Attachments A-D1, F, and F2 the State and Supplier further agree that the terms and conditions in Attachments A-D1, F, and F2 take precedence over the embedded hyperlinks.

Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES

By: Joe McIntosh (Jun 3, 2024 17:04 CDT)

Name: Joe McIntosh

Title: CIO

Date: Jun 3, 2024

GARTNER, INC.

By: Kristin Ghanem (Jun 3, 2024 16:30 EDT)

Name: Kristin Ghanem

Title: Director, Contracts

Date: Jun 3, 2024

ATTACHMENT A

SOLICITATION NO. 0900000582

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

PURPOSE

The Contract is awarded as a statewide contract for This is a non-mandatory statewide contract. Information Technology (IT) research and advisory subscription services and consultancy services, to support IT strategic, tactical and operational initiatives underway.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are four (4) one-year options to renew the Contract.

2. Scope of Work

Certain Contract requirements and terms are attached hereto as **Exhibit 1** and incorporated herein.

Exhibit 1

SOLICITATION SCOPE

Overview

The State of Oklahoma Office of Management and Enterprise Services (OMES) is currently accepting proposals from qualified offerors for Information Technology (IT) research and advisory subscription services and consultancy services, to support IT strategic, tactical, and operational initiatives underway. The technical requirements are divided into two main parts.

Part One is IT Services. The services range from a pure self-service model wherein an authorized staff member may access and research the knowledge base to on-site consulting service wherein a Supplier's employee may provide on-site service on a critical IT project.

Part Two is the IT Topics. These topics would require in-depth knowledge of industry, market trends, global factors, trends, and supplier's product capabilities, etc.

Mandatory Specifications / Requirements

- **IT Services**

  Offerors shall provide the State of Oklahoma with a list and brief narrative illustrating their ability to provide the following types of research and advisory services in the area of Information and Communications Technologies:

- **Research and Advisory Services – these services are based on industry trends.**
  1) Access to knowledge repository of IT research via the internet/web.
  2) Ability to customize personal web pages to save queries to other clients, etc.
  3) Access to and ability to consult with IT Research Analysts to obtain latest thinking.
  4) Ability to combine research information within OK and provide customized advice/report.
- **Consultancy Services – these services require the offeror to provide the State of Oklahoma specific advice and require a good and thorough understanding of the organization, the key initiatives, and the underlying technologies.**
  1) On-site consultancy advice such as quality assurance and supplier selection assistance for IT projects.
  2) On-site/off-site presentations/workshops on IT topics.
  3) Customized consultancy services to help develop and review business cases and strategies, conduct studies, review RFP's, participate in panel interviews, etc.
  4) Dedicated and personalized Executive programs for CIOs.
  5) Industry advisory services.
  6) Product and supplier advisory services.
  7) Evaluate business requirements to propose solutions.
- **Other Services – These services relate to other informational series such as annual symposiums, seminars, conferences, boot camps, teleconferences, webcasts, webinars, white papers, etc. The State of Oklahoma would like to participate in various such events. Please provide details on:**

1) Number and type of conference conducted the typical content of the conference, duration, frequency, etc.
2) Any teleconferences and webcasts conducted with relevant information.
3) Other informational services offered.

Non-Mandatory Requirements

- **Variety of IT Topics**

  The IT topics of interest are listed below. This list is representative of the State of Oklahoma's current interests and should in no way be construed as exhaustive, as the interests may change. Bidder should indicate availability of research and consulting services for each topic below:

- **Information Management and IT Strategy**
  1) IT Standards/Policies
     a. Emerging IT Technologies and Trends
     b. Business Continuity and Disaster Recovery
     c. Identity and Security
     d. IT Usage Policies (email, equipment, internet/intranet, etc.)
     e. IT Operations Standards
     f. Best Practices
     g. Software Development Standards
     h. Systems and Storage Management
  2) IT Strategies
     a. Sourcing Strategies (Outsourcing, Offshoring, etc.)
     b. IT Operations Management
     c. IT Staffing
     d. IT Organizational Development & Training
     e. Help Desk
     f. Work Force Management
     g. Open-Source Strategies
     h. Green IT Strategies
     i. Contract Negotiations
     j. Legal Issues and Technology
  3) Program Management / Metrics / Analytics
     a. Balanced Scorecard
     b. Enterprise Program Management/Portfolio Management
     c. IT Costs and Performances
     d. RIO (Return on Investment on IT Projects)
     e. IT Benchmarking and Analytics
- **Tactics and Operations**
  1) Knowledge Management
     a. Content & Collaboration Applications – Workflow, Document Management, etc.
     b. Content Management
     c. Enterprise Analysis
  2) Enterprise Applications
     a. ERP
     b. CRM
     c. Enterprise Application Integration
     d. SCM
     e. Enterprise Messaging Collaboration
     f. Enterprise Directory Services
     g. Knowledge Management
     h. Document Management
     i. Content Management

j. Data Warehouse Development
k. eCommerce
l. eProcurement
m. eRecruitment
n. E-Learning / LRMS
o. Portal/Web Development and Services
p. Application and Database Security

3) Infrastructure
   a. Infrastructure Strategies
   b. Integration & Development
   c. Operations Consolidation
   d. Hardware and Software
   e. Networks
   f. Operating Systems
   g. Data Center
   h. Server Virtualization
   i. Data and Database Management
4) Security
   a. Security Management and Audit
   b. Identity Management
   c. Security Architecture
   d. Risk Management
   e. Information Protection
   f. Security Awareness Training
5) Telecommunications
   a. Satellite Communications
   b. Video and Audio Conferencing
   c. Mobile Computing
   d. IP Telephony
   e. WANs and MANs
   f. PBX
   g. Unified Communications
   h. E-Rate

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4 The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State exercises such option to extend ninety (90) days, the State shall notify the

Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

1.5 Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

2.1 Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2 Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

A. any Addendum;

B. any applicable Solicitation;

C. any Contract-specific terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D. the terms contained in this Contract Document;

E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F. any statement of work, work order, or other similar ordering document as applicable; and

G. other mutually agreed Contract Documents.

2.3 If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract Document or

Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract Documents

3.1 The Contract may only be modified, amended, or expanded by an Addendum. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Addendum** means a mutually executed, written modification to a Contract Document.

4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.

4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.

4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.

4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.13 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

4.14 **OAC** means the Oklahoma Administrative Code.

4.15 **OMES** means the Office of Management and Enterprise Services.

4.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.18 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

4.19 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

5.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

5.2 Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3 The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

6.1 Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.

6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

7.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

A. An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

E. If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

F. Supplier shall have no right of setoff.

G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $5,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $5,000,000 combined single limit each accident;

D. Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than $5,000,000 per occurrence;

E. Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $5,000,000 per occurrence; and

F. Additional coverage required in writing in connection with a particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

8.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C. Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at **www.dhs.gov/E-Verify**;

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at https://omes.ok.gov/sites/g/files/gmc316/f/InfoSecPPG_0.pdf. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory

contract provisions required in connection with the receipt of federal funds or other funding source.

9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

9.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

9.9 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.10 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format

usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3 Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

11.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer's prior express written

permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents,

representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is

related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

13.1 Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to

the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in subsection A above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property,

copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

17.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

18.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier’s performance or obligations under the Contract; (ii) Supplier’s material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence

of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

19.1 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but

there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

20.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.2 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:
State Purchasing Director
2401 N. Lincoln Blvd., Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 N. Lincoln Blvd., Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq*. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

The headings used in any Contract Document are for convenience only and do not constitute terms of the Contract.

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition,

understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

1.1 The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.

1.2 The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

2.1 Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

2.2 Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

2.3 Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract

management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Addendum.

6.2 While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

6.3 All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to **strategic.sourcing@omes.ok.gov**;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;

b. April 01 through June 30;

c. July 01 through September 30; and

d. October 01 through December 31.

v. Reports must include the following information:

a. Procuring entity;
b. Order date;
c. Purchase Order number or note that the transaction was paid by Purchase Card;
d. City in which products or services were received or specific office or subdivision title;
e. Product manufacturer or type of service;
f. Manufacturer item number, if applicable;
g. Product description;
h. General product category, if applicable;
i. Quantity;
j. Unit list price or MSRP, as applicable;
k. Unit price charged to the purchasing entity; and
l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 118
Oklahoma City, Oklahoma 73105

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s) and the amount of the contract management fee being paid for each contract number.

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, OMES-Information Services ("OMES-IS") is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 Definitions

1.1 **COTS** means software that is commercial off the shelf.

1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.

1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.

1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.

1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.8 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.9 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.

1.10 **State CIO** means the State Chief Information Officer or authorized designee.

1.11 **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

1.12 **Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

1.13 **Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to- practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

2.1 Customer removes the product for which the services are provided, from productive use or;

2.2 The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/accessibility-standards.html. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required, and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 Compliance with Technology Policies

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other

applicable Customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

In addition to extension rights of the State set forth in the Contract, the State CIO reserves the right to extend any Contract if the State CIO determines such extension to be in the best interest of the State.

9 Source Code Escrow

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1 A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;

9.2 An assignment by the Supplier for the benefit of its creditors;

9.3 A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;

9.4 The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;

9.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;

9.6 The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;

9.7 Supplier's ceasing of maintenance and support of the software; or

9.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as “Work for Hire”, Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

The following terms apply to ownership and rights related to Intellectual Property:

12.1 As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered "works made for hire" and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.

12.2 Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier's signature due to the dissolution of Supplier or Supplier's failure to respond to Customer's repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier's agent and Supplier's attorney-in-fact to act for and in Supplier's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer's sole expense, in the preparation and

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.

12.4 All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.

12.5 These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.

12.7 Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.

12.8 To the extent that any Third-Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third-Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the Work Product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third-Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third-Party Intellectual Property that may be embodied or reflected in the Work Product.

12.9 Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.

12.10 To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11 If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

13.1 If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any Customer Data accessed, processed or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.

3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.

4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. **Security Incident or Data Breach Notification:** Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.

2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).

3. Supplier shall:

a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;

b. Make summary information regarding such procedures available to Customer at Customer's request;

c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

1. Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

2. Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. Notices

In addition to notice requirements under the terms of the Contract and those set forth above, a request, an approval or a notice in connection with this Appendix provided by Supplier shall be provided to:

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

2. In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

3. Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination, if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

4. The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

5. Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. **Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy **plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.**

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist	Compliance checklist –
Policy Area 1	Information Exchange Agreements
Policy Area 2	Security Awareness Training
Policy Area 3	Incident Response
Policy Area 4	Auditing and Accountability
Policy Area 5	Access Control
Policy Area 6	Identification and Authentication
Policy Area 7	Configuration Management
Policy Area 8	Media Protection
Policy Area 9	Physical Protection
Policy Area 10	Systems and Communications Protection and Information Integrity
Policy Area 11	Formal Audits
Policy Area 12	Personnel Security

Attachment D-1
Information Security Requirements

1. General Information Security Requirements

a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.

b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.

d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

2. HIPAA Requirements (If applicable)

a. Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.

c. Business Associate Terms Definitions:

   i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business

Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.

iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.

v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:

i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;

ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;

iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;

v. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);

vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;

vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the

form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;

ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;

x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

xi. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;

xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;

xiv. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to

respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:

i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;

ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;

iii. disclose PHI to report violations of law to appropriate federal and state authorities; or

iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

v. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].

f. Obligations of Covered Entity
   i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
   ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.
   iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.
   iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.
   v. Covered Entity shall provide the minimum necessary PHI to Business Associate.

g. Term and Termination:
   i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:
      (1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
      (2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;
      (3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
      (4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and
      (5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

ii. All other applicable obligations of Business Associate under this Agreement shall survive termination.

iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

h. Miscellaneous Provisions:

i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

ii. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.

iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.

iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.

v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.

vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s)

to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

3. 42 C.F.R. Part 2 Related Provisions (If applicable)

a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of an kind;

iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

iv. Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

b. Data Security. The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

c. Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.

d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.

e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

4. Federal Tax Information Requirements IRS Publication 1075 (If Applicable)

a. PERFORMANCE: If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent

within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

i. All work will be performed under the supervision of the State of Oklahoma.
ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
vii. All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material

in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c. INSPECTION: The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

5. SSA Requirements (If applicable)

a. PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:

i. All work will be done under the supervision of the State of Oklahoma.

ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.
v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.
vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.
vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.
ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.
x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.
xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.
xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

xiii. If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

b. CRIMINAL/CIVIL SANCTIONS: The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

i. Civil Remedies.

(1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of —

(a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of $1,000; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where

parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(1).

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(2).

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements (If applicable)

a. Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. FERPA Requirements (If applicable)

a. If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. CJIS Requirements (If applicable)

a. INTRODUCTION

This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."

c. DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

ATTACHMENT E1

ADDITIONAL TERMS

1. **Preexisting Materials:** Customer shall retain its rights in any proprietary material that Customer supplies to Supplier. If the Customer provides Supplier with materials owned or controlled by Customer or with use of, or access to, such materials, the Customer grants to Supplier all rights and licenses that are necessary for Supplier to fulfill its obligations under each Statement of Work. Supplier grants to Customer for internal purposes only a worldwide, royalty-free, perpetual license to use, reproduce, display, distribute copies of, and prepare derivative works of any Supplier "Preexisting Intellectual Property" embodied in the Deliverables.

2. **Intellectual Property Ownership:** Supplier shall assign to Customer ownership of any project Deliverable(s) originally created for and submitted to Customer, provided, however, that Supplier may use, reproduce, display and distribute excerpts and data from the deliverables, either alone or together with other material, in the ordinary course of Supplier's business, so long as such excerpts and data do not identify Customer by name or contain any of Customer's confidential or proprietary information, and provided further that Supplier retains all right, title and interest in and to its processes, benchmarking data and data collection tools, assessment models and pertinent methodologies such as Strategic Planning, Supplier's copyrighted proprietary research and other pre-existing materials and data, such as Data Collection Templates and Survey Tools for Applications and Infrastructure, and benchmark comparisons ("Preexisting Intellectual Property"). Nothing contained in this Agreement shall preclude Supplier from rendering services to others or developing work products that are competitive with, or functionally comparable to, the Services. Supplier shall not be restricted in its use of ideas, concepts, know-how, data and techniques acquired or learned in the course of performing the Services, provided that Supplier shall not use or disclose any of Customer's confidential information.

3. **Warranty**. Supplier warrants that the Deliverables, in the form provided to Customer, do not infringe any copyright, trademark, trade secret or other right of any third party. SUPPLIER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE INFORMATION IN THE DELIVERABLES HAS BEEN OBTAINED FROM SOURCES THAT CONTRACTOR BELIEVES TO BE RELIABLE. ALL DELIVERABLES SPEAK AS OF THE DATE OF DELIVERY TO THE CUSTOMER.

RESEARCH & ADVISORY SERVICES TERMS ADDENDUM

1. ***Ownership and Use of the Services***. Supplier owns and retains all rights to the Services not expressly granted to Customer. Only the individuals named in the Service Agreement (each a "**Licensed User**") may access the Services. Each Licensed User will be issued a unique password, which may not be shared. Customer agrees to review and comply with the *Gartner Usage Policy,* which is accessible to all Licensed Users via the "Policies" section of gartner.com. Among other things, the *Gartner Usage Policy* describes

how Customer may substitute Licensed Users, excerpt from and/or share Supplier research documents within the Customer organization, and quote or excerpt from the Services externally.

ATTACHMENT E2

MASTER TERMS

Intentionally Left Blank.

ATTACHMENT E3

PRICING

The Oklahoma Prices herein are detailed in "Pricing Exhibit 1 – Gartner Research and Advisory Services" in a concise user-friendly format for ease of document review and incorporation into the final contract award agreement.

Services/Subscription/License	Unit of Measure	List Price	% off List Price	Oklahoma Price
Executive Programs V2 Guided Individual Access [1] - Single User	2023 RAS Subscriber	140,607	0.0%	140,607
Executive Programs V2 Guided Individual Access [1] - Multi-User	2023 RAS Subscriber	140,607	9.1%	127,778
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2023 RAS Subscriber	80,102	0.0%	80,102
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2023 RAS Subscriber	80,102	9.2%	72,728
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2023 RAS Subscriber	72,728	0.0%	72,728
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	72,728	0.0%	72,728
Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778

Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Guided Team [2] Advisor Member	2023 RAS Subscriber	56,970	0.0%	56,970
Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	56,970	0.0%	56,970
Executive Programs V2 Guided Team [2] Cross Function Member	2023 RAS Subscriber	37,172	0.0%	37,172
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2023 RAS Subscriber	72,728	0.0%	72,728
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2023 RAS Subscriber	72,728	0.0%	72,728
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	72,728	0.0%	72,728
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778

Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	127,778	0.0%	127,778
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	65,455	0.0%	65,455
Executive Programs V2 Self-Directed Team [2] Advisor Member	2023 RAS Subscriber	56,970	0.0%	56,970
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2023 RAS Subscriber	56,970	0.0%	56,970
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2023 RAS Subscriber	37,172	0.0%	37,172
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	48,586	0.0%	48,586
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	48,586	0.0%	48,586

Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	48,586	0.0%	48,586
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	43,233	0.0%	43,233
Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	43,233	0.0%	43,233
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2023 RAS Subscriber	43,233	0.0%	43,233
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2023 RAS Subscriber	56,970	0.0%	56,970
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2023 RAS Subscriber	37,172	0.0%	37,172
Gartner for CIOs Individual Access [1] - single user	2023 RAS Subscriber	72,930	0.0%	72,930
Gartner for CIOs Individual Access [1] - multi-user	2023 RAS Subscriber	72,930	9.0%	66,364
Gartner for CIOs Team Plus [2] - Team Leader	2023 RAS Subscriber	66,364	0.0%	66,364
Gartner for CIOs Team Plus [2] - Advisor Team Member	2023 RAS Subscriber	48,485	0.0%	48,485
Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2023 RAS Subscriber	48,485	0.0%	48,485
Gartner for CIOs Team Plus [2] - Cross Function Team Member	2023 RAS Subscriber	33,637	0.0%	33,637
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2023 RAS Subscriber	80,102	0.0%	80,102
Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2023 RAS Subscriber	80,102	9.2%	72,728
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2023 RAS Subscriber	72,728	0.0%	72,728
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	56,970	0.0%	56,970
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2023 RAS Subscriber	56,970	0.0%	56,970
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	37,172	0.0%	37,172
Executive Programs Member Individual Access [1] - single user	2023 RAS Subscriber	119,192	0.0%	119,192
Executive Programs Member Individual Access [1] - multi-user user	2023 RAS Subscriber	119,192	11.0%	106,061
Executive Programs Leadership Team [2] - Team Leader	2023 RAS Subscriber	108,081	0.0%	108,081
Executive Programs Leadership Team [2] - IT Executive Team Member	2023 RAS Subscriber	108,081	0.0%	108,081
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2023 RAS Subscriber	108,081	0.0%	108,081
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2023 RAS Subscriber	98,788	0.0%	98,788

Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2023 RAS Subscriber	98,788	0.0%	98,788
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2023 RAS Subscriber	57,778	0.0%	57,778
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2023 RAS Subscriber	57,778	0.0%	57,778
Executive Programs Leadership Team [2] - Advisor Team Member	2023 RAS Subscriber	39,293	0.0%	39,293
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2023 RAS Subscriber	39,293	0.0%	39,293
Executive Programs Leadership Team [2] - Cross Function Team Member	2023 RAS Subscriber	28,485	0.0%	28,485
Executive Programs Leadership Team [2] - Role Team Member	2023 RAS Subscriber	20,506	0.0%	20,506
Executive Programs Leadership Team Plus [2] - Team Leader	2023 RAS Subscriber	117,778	0.0%	117,778
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2023 RAS Subscriber	117,778	8.1%	108,182
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2023 RAS Subscriber	117,778	0.0%	117,778
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2023 RAS Subscriber	117,778	0.0%	117,778
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2023 RAS Subscriber	107,778	0.0%	107,778
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2023 RAS Subscriber	107,778	0.0%	107,778
Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2023 RAS Subscriber	62,930	0.0%	62,930
Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2023 RAS Subscriber	62,930	0.0%	62,930
Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2023 RAS Subscriber	62,930	8.3%	57,697
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2023 RAS Subscriber	42,930	0.0%	42,930
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2023 RAS Subscriber	42,930	0.0%	42,930
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2023 RAS Subscriber	31,112	0.0%	31,112
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2023 RAS Subscriber	128,283	0.0%	128,283
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2023 RAS Subscriber	128,283	10.2%	115,152
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2023 RAS Subscriber	117,576	0.0%	117,576
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2023 RAS Subscriber	117,576	0.0%	117,576

Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2023 RAS Subscriber	117,576	0.0%	117,576
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2023 RAS Subscriber	109,293	0.0%	109,293
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2023 RAS Subscriber	109,293	0.0%	109,293
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2023 RAS Subscriber	65,354	0.0%	65,354
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2023 RAS Subscriber	65,354	0.0%	65,354
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	47,475	0.0%	47,475
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2023 RAS Subscriber	47,475	0.0%	47,475
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	31,718	0.0%	31,718
Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2023 RAS Subscriber	22,930	0.0%	22,930
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2023 RAS Subscriber	128,182	0.0%	128,182
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2023 RAS Subscriber	128,182	0.0%	128,182
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2023 RAS Subscriber	128,182	0.0%	128,182
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2023 RAS Subscriber	119,394	0.0%	119,394
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2023 RAS Subscriber	119,394	0.0%	119,394
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2023 RAS Subscriber	71,011	0.0%	71,011

Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2023 RAS Subscriber	71,011	0.0%	71,011
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	51,617	0.0%	51,617
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2023 RAS Subscriber	51,617	0.0%	51,617
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	34,445	0.0%	34,445
Gartner for CDAOs Individual Access [1] - single user	2023 RAS Subscriber	71,920	0.0%	71,920
Gartner for CDAOs Individual Access [1] - multi-user	2023 RAS Subscriber	71,920	9.0%	65,455
Gartner for CDAOs Team [2] - Team Leader	2023 RAS Subscriber	65,455	0.0%	65,455
Gartner for CDAOs Team [2] - Team Member	2023 RAS Subscriber	43,233	0.0%	43,233
Gartner for CDAOs Team [2] - Tech Professional Team Member	2023 RAS Subscriber	16,364	0.0%	16,364
Gartner for CDAOs Executive Individual Access [1] - single user	2023 RAS Subscriber	140,607	0.0%	140,607
Gartner for CDAOs Executive Individual Access [1] - multi-user	2023 RAS Subscriber	140,607	9.1%	127,778
Gartner for CDAOs Executive Team [2] - Team Leader	2023 RAS Subscriber	127,778	0.0%	127,778
Gartner for CDAOs Executive Team [2] - Team Member	2023 RAS Subscriber	48,586	0.0%	48,586
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2023 RAS Subscriber	18,889	0.0%	18,889
Gartner for CISOs Individual Access [1] - single user	2023 RAS Subscriber	71,920	0.0%	71,920
Gartner for CISOs Individual Access [1] - multi-user	2023 RAS Subscriber	71,920	9.0%	65,455
Gartner for CISOs Team [2] - Team Leader	2023 RAS Subscriber	65,455	0.0%	65,455
Gartner for CISOs Team [2] - Team Member	2023 RAS Subscriber	43,233	0.0%	43,233
Gartner for CISOs Team [2] - Tech Professional Team Member	2023 RAS Subscriber	16,364	0.0%	16,364
Gartner for CISOs Executive Individual Access [1] - single user	2023 RAS Subscriber	140,607	0.0%	140,607
Gartner for CISOs Executive Individual Access [1] - multi-user	2023 RAS Subscriber	140,607	9.1%	127,778
Gartner for CISOs Executive Team [2] - Team Leader	2023 RAS Subscriber	127,778	0.0%	127,778
Gartner for CISOs Executive Team [2] - Team Member	2023 RAS Subscriber	48,586	0.0%	48,586
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2023 RAS Subscriber	18,889	0.0%	18,889
Gartner for Software Engineering Leaders Individual Access [1] - single user	2023 RAS Subscriber	71,920	0.0%	71,920
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2023 RAS Subscriber	71,920	9.0%	65,455
Gartner for Software Engineering Leaders Team [2] - Team Leader	2023 RAS Subscriber	65,455	0.0%	65,455
Gartner for Software Engineering Leaders Team [2] - Team Member	2023 RAS Subscriber	43,233	0.0%	43,233
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2023 RAS Subscriber	16,364	0.0%	16,364
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2023 RAS Subscriber	140,607	0.0%	140,607
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2023 RAS Subscriber	140,607	9.1%	127,778
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2023 RAS Subscriber	127,778	0.0%	127,778

Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2023 RAS Subscriber	48,586	0.0%	48,586
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2023 RAS Subscriber	18,889	0.0%	18,889
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2023 RAS Subscriber	91,516	0.0%	91,516
Enterprise IT Leadership Team [2] - Advisor Team Member	2023 RAS Subscriber	36,263	0.0%	36,263
Enterprise IT Leadership Team [2] - Cross Function Team Member	2023 RAS Subscriber	21,920	0.0%	21,920
Enterprise IT Leadership Team [2] - Role Team Member	2023 RAS Subscriber	13,738	0.0%	13,738
Enterprise IT Leadership Team [2] - Essentials Team Member	2023 RAS Subscriber	10,708	0.0%	10,708
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2023 RAS Subscriber	99,394	0.0%	99,394
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2023 RAS Subscriber	39,091	0.0%	39,091
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2023 RAS Subscriber	23,738	0.0%	23,738
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2023 RAS Subscriber	101,920	0.0%	101,920
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	42,930	0.0%	42,930
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	26,263	0.0%	26,263
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2023 RAS Subscriber	15,354	0.0%	15,354
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2023 RAS Subscriber	10,708	0.0%	10,708
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2023 RAS Subscriber	111,314	0.0%	111,314
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	46,768	0.0%	46,768
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	28,687	0.0%	28,687
IT Leader Individual Access Reference [1] - single user	2023 RAS Subscriber	34,142	0.0%	34,142
IT Leader Individual Access Reference [1] - multi-user	2023 RAS Subscriber	34,142	37.6%	21,314
IT Leader Individual Access Advisor [1] - single user	2023 RAS Subscriber	48,889	0.0%	48,889
IT Leader Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	48,889	25.8%	36,263
IT Leadership Team [2] - Team Leader	2023 RAS Subscriber	36,263	0.0%	36,263
IT Leadership Team [2] - Advisor Team Member	2023 RAS Subscriber	36,263	0.0%	36,263
IT Leadership Team [2] - Cross Function Team Member	2023 RAS Subscriber	21,920	0.0%	21,920
IT Leadership Team [2] - Role Team Member	2023 RAS Subscriber	13,738	0.0%	13,738
IT Leadership Team [2] - Essentials Team Member	2023 RAS Subscriber	10,708	0.0%	10,708
IT Leadership Team Plus [2] - Team Leader	2023 RAS Subscriber	39,091	0.0%	39,091
IT Leadership Team Plus [2] - Advisor Team Member	2023 RAS Subscriber	39,091	0.0%	39,091
IT Leadership Team Plus [2] - Cross Function Team Member	2023 RAS Subscriber	23,738	0.0%	23,738
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2023 RAS Subscriber	37,475	0.0%	37,475

Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2023 RAS Subscriber	37,475	31.8%	25,556
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2023 RAS Subscriber	55,455	0.0%	55,455
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2023 RAS Subscriber	55,455	22.6%	42,930
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2023 RAS Subscriber	42,930	0.0%	42,930
Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	42,930	0.0%	42,930
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	26,263	0.0%	26,263
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2023 RAS Subscriber	15,354	0.0%	15,354
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2023 RAS Subscriber	10,708	0.0%	10,708
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2023 RAS Subscriber	46,768	0.0%	46,768
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2023 RAS Subscriber	46,768	0.0%	46,768
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2023 RAS Subscriber	28,687	0.0%	28,687
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2023 RAS Subscriber	66,973	0.0%	66,973
Technical Professionals Team [4, 5] - Additional Team Member	2023 RAS Subscriber	12,829	0.0%	12,829
Technical Professionals Advisor Department [4, 5]	2023 RAS Subscriber	139,091	0.0%	139,091
Technical Professionals Reference Department [4, 5]	2023 RAS Subscriber	93,536	0.0%	93,536
Finance Leaders Individual Access Advisor [1] - single user	2023 RAS Subscriber	48,485	0.0%	48,485
Finance Leaders Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	48,485	25.2%	36,263
Finance Leaders Team [2] - Team Leader	2023 RAS Subscriber	36,263	0.0%	36,263
Finance Leaders Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
Finance Leaders Team [2] - Reference Member	2023 RAS Subscriber	16,869	0.0%	16,869
Chief Financial Officers Individual Access [1] - single user	2023 RAS Subscriber	118,182	0.0%	118,182
Chief Financial Officers Individual Access [1] - multi-user	2023 RAS Subscriber	118,182	9.4%	107,071
Chief Financial Officers Team [2] - Team Leader	2023 RAS Subscriber	107,071	0.0%	107,071
Chief Financial Officers Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2023 RAS Subscriber	36,263	0.0%	36,263
Chief Financial Officers Team [2] - Reference Member	2023 RAS Subscriber	16,869	0.0%	16,869
Human Resources Leaders Individual Access [1] - single user	2023 RAS Subscriber	48,485	0.0%	48,485
Human Resources Leaders Individual Access [1] - multi-user	2023 RAS Subscriber	48,485	25.2%	36,263
Human Resources Leaders Team [2] - Team Leader	2023 RAS Subscriber	36,263	0.0%	36,263
Human Resources Leaders Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
Human Resources Leaders Team [2] - Reference Member	2023 RAS Subscriber	19,899	0.0%	19,899
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2023 RAS Subscriber	44,445	0.0%	44,445
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2023 RAS Subscriber	27,677	0.0%	27,677

Chief Human Resources Officers Individual Access [1] - single user	2023 RAS Subscriber	118,182	0.0%	118,182
Chief Human Resources Officers Individual Access [1] - multi-user	2023 RAS Subscriber	118,182	9.4%	107,071
Chief Human Resources Officers Team [2] - Team Leader	2023 RAS Subscriber	107,071	0.0%	107,071
Chief Human Resources Officers Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2023 RAS Subscriber	36,263	0.0%	36,263
Chief Human Resources Officers Team 2 - Reference Member	2023 RAS Subscriber	19,899	0.0%	19,899
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2023 RAS Subscriber	41,516	0.0%	41,516
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2023 RAS Subscriber	41,516	24.3%	31,415
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2023 RAS Subscriber	31,415	0.0%	31,415
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2023 RAS Subscriber	31,415	0.0%	31,415
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2023 RAS Subscriber	12,526	0.0%	12,526
R&D Leaders Individual Access Advisor [1] - single user	2023 RAS Subscriber	48,485	0.0%	48,485
R&D Leaders Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	48,485	25.2%	36,263
R&D Leaders Team [2] - Leader	2023 RAS Subscriber	36,263	0.0%	36,263
R&D Leaders Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
R&D Leaders Team [2] - Reference Member	2023 RAS Subscriber	19,899	0.0%	19,899
Marketing Leaders Individual Access Advisor [1] - single user	2023 RAS Subscriber	55,051	0.0%	55,051
Marketing Leaders Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	55,051	16.7%	45,859
Marketing Leaders Team [2] - Leader	2023 RAS Subscriber	45,859	0.0%	45,859
Marketing Leaders Team [2] - Advisor Member	2023 RAS Subscriber	45,859	0.0%	45,859
Marketing Leaders Team [2] - Reference Member	2023 RAS Subscriber	18,081	0.0%	18,081
Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2023 RAS Subscriber	130,102	0.0%	130,102
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2023 RAS Subscriber	130,102	10.6%	116,364
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2023 RAS Subscriber	116,364	0.0%	116,364
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2023 RAS Subscriber	45,859	0.0%	45,859
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2023 RAS Subscriber	45,859	0.0%	45,859
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2023 RAS Subscriber	18,081	0.0%	18,081
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2023 RAS Subscriber	48,485	0.0%	48,485
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	48,485	25.2%	36,263

Customer Service & Support Leaders Team [2] - Leader	2023 RAS Subscriber	36,263	0.0%	36,263
Customer Service & Support Leaders Team [2] - Advisor Member	2023 RAS Subscriber	36,263	0.0%	36,263
Customer Service & Support Leaders Team [2] - Reference Member	2023 RAS Subscriber	16,263	0.0%	16,263
North America Gartner Conferences [7] - IT Symposium/Xpo	2023 Conference Ticket	5,430	0.0%	5,430
North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2023 Conference Ticket	3,687	0.0%	3,687
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2023 Conference Ticket	3,132	0.0%	3,132
North America Gartner Conferences [7] - Finance Conference	2023 Conference Ticket	3,208	0.0%	3,208
North America Gartner Conferences [7] - ReImagineHR Conference	2023 Conference Ticket	3,536	0.0%	3,536
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2023 Conference Ticket	3,889	0.0%	3,889
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2023 Conference Ticket	4,445	0.0%	4,445
Core Connect Individual Access Reference [1]- single user	2023 RAS Subscriber	29,394	0.0%	29,394
Core Connect Individual Access Reference [1]- multi-user	2023 RAS Subscriber	29,394	43.3%	16,667
Core Connect Individual Access Advisor [1] - single user	2023 RAS Subscriber	44,243	0.0%	44,243
Core Connect Individual Access Advisor [1] - multi-user	2023 RAS Subscriber	44,243	28.5%	31,617
IT News and Insights	2023 RAS Subscriber	768	0.0%	768
News and Insights	2023 RAS Subscriber	768	0.0%	768
Internal Advisory Session ** Limited Availability **	2023 RAS Session	22,425	0.0%	22,425
Remote Advisory Services ** Limited Availability **	2023 RAS Session	9,697	0.0%	9,697
Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2023 RAS Add-on	26,465	0.0%	26,465
Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2023 RAS Add-on	26,465	0.0%	26,465
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2023 RAS Add-on	26,465	0.0%	26,465
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2023 RAS Subscriber	70,304	0.0%	70,304
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2023 RAS Subscriber	46,667	0.0%	46,667
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2023 RAS Subscriber	70,304	0.0%	70,304
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2023 RAS Subscriber	46,667	0.0%	46,667
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2023 RAS Subscriber	34,142	0.0%	34,142

Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2023 RAS Subscriber	34,142	0.0%	34,142
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2023 RAS Subscriber	68,283	0.0%	68,283
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2023 RAS Subscriber	102,425	0.0%	102,425
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2023 RAS Subscriber	136,566	0.0%	136,566
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2023 RAS Subscriber	32,021	0.0%	32,021
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2023 RAS Subscriber	36,566	0.0%	36,566
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2023 RAS Subscriber	36,566	37.8%	22,728
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2023 RAS Subscriber	53,940	0.0%	53,940
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2023 RAS Subscriber	53,940	25.8%	40,000
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2023 RAS Subscriber	40,000	0.0%	40,000
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2023 RAS Subscriber	40,000	0.0%	40,000
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2023 RAS Subscriber	23,536	0.0%	23,536
Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2023 RAS Subscriber	10,607	0.0%	10,607
Executive Programs V2 Guided Individual Access [1] - Single User	2024 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Individual Access [1] - Multi-User	2024 RAS Subscriber	154,700	9.1%	140,623
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2024 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2024 RAS Subscriber	88,200	9.2%	80,086
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2024 RAS Subscriber	80,100	0.0%	80,100
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	80,100	0.0%	80,100

Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Guided Team [2] Advisor Member	2024 RAS Subscriber	62,700	0.0%	62,700

Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	62,700	0.0%	62,700
Executive Programs V2 Guided Team [2] Cross Function Member	2024 RAS Subscriber	40,900	0.0%	40,900
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2024 RAS Subscriber	80,100	0.0%	80,100
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2024 RAS Subscriber	80,100	0.0%	80,100
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	80,100	0.0%	80,100
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	140,600	0.0%	140,600
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100

Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	72,100	0.0%	72,100
Executive Programs V2 Self-Directed Team [2] Advisor Member	2024 RAS Subscriber	62,700	0.0%	62,700
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2024 RAS Subscriber	62,700	0.0%	62,700
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2024 RAS Subscriber	40,900	0.0%	40,900
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	53,500	0.0%	53,500
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	53,500	0.0%	53,500
Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	53,500	0.0%	53,500
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	47,600	0.0%	47,600
Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	47,600	0.0%	47,600
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2024 RAS Subscriber	47,600	0.0%	47,600
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2024 RAS Subscriber	62,700	0.0%	62,700
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2024 RAS Subscriber	40,900	0.0%	40,900
Gartner for CIOs Individual Access [1] - single user	2024 RAS Subscriber	80,300	0.0%	80,300
Gartner for CIOs Individual Access [1] - multi-user	2024 RAS Subscriber	80,300	9.0%	73,073
Gartner for CIOs Team Plus [2] - Team Leader	2024 RAS Subscriber	73,100	0.0%	73,100
Gartner for CIOs Team Plus [2] - Advisor Team Member	2024 RAS Subscriber	53,400	0.0%	53,400

Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2024 RAS Subscriber	53,400	0.0%	53,400
Gartner for CIOs Team Plus [2] - Cross Function Team Member	2024 RAS Subscriber	37,100	0.0%	37,100
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2024 RAS Subscriber	88,200	0.0%	88,200
Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2024 RAS Subscriber	88,200	9.2%	80,086
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2024 RAS Subscriber	80,100	0.0%	80,100
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	62,700	0.0%	62,700
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2024 RAS Subscriber	62,700	0.0%	62,700
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	40,900	0.0%	40,900
Executive Programs Member Individual Access [1] - single user	2024 RAS Subscriber	131,200	0.0%	131,200
Executive Programs Member Individual Access [1] - multi-user user	2024 RAS Subscriber	131,200	11.0%	116,768
Executive Programs Leadership Team [2] - Team Leader	2024 RAS Subscriber	118,900	0.0%	118,900
Executive Programs Leadership Team [2] - IT Executive Team Member	2024 RAS Subscriber	118,900	0.0%	118,900
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2024 RAS Subscriber	118,900	0.0%	118,900
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2024 RAS Subscriber	108,700	0.0%	108,700
Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2024 RAS Subscriber	108,700	0.0%	108,700
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2024 RAS Subscriber	63,600	0.0%	63,600
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2024 RAS Subscriber	63,600	0.0%	63,600
Executive Programs Leadership Team [2] - Advisor Team Member	2024 RAS Subscriber	43,300	0.0%	43,300
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2024 RAS Subscriber	43,300	0.0%	43,300
Executive Programs Leadership Team [2] - Cross Function Team Member	2024 RAS Subscriber	31,400	0.0%	31,400
Executive Programs Leadership Team [2] - Role Team Member	2024 RAS Subscriber	22,600	0.0%	22,600
Executive Programs Leadership Team Plus [2] - Team Leader	2024 RAS Subscriber	129,600	0.0%	129,600
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2024 RAS Subscriber	129,600	8.1%	119,103
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2024 RAS Subscriber	129,600	0.0%	129,600
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2024 RAS Subscriber	129,600	0.0%	129,600
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2024 RAS Subscriber	118,600	0.0%	118,600
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2024 RAS Subscriber	118,600	0.0%	118,600

Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2024 RAS Subscriber	69,300	0.0%	69,300
Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2024 RAS Subscriber	69,300	0.0%	69,300
Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2024 RAS Subscriber	69,300	8.3%	63,549
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2024 RAS Subscriber	47,300	0.0%	47,300
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2024 RAS Subscriber	47,300	0.0%	47,300
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2024 RAS Subscriber	34,300	0.0%	34,300
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2024 RAS Subscriber	141,200	0.0%	141,200
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2024 RAS Subscriber	141,200	10.2%	126,798
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2024 RAS Subscriber	129,400	0.0%	129,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2024 RAS Subscriber	129,400	0.0%	129,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2024 RAS Subscriber	129,400	0.0%	129,400
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2024 RAS Subscriber	120,300	0.0%	120,300
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2024 RAS Subscriber	120,300	0.0%	120,300
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2024 RAS Subscriber	71,900	0.0%	71,900
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2024 RAS Subscriber	71,900	0.0%	71,900
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	52,300	0.0%	52,300
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2024 RAS Subscriber	52,300	0.0%	52,300
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	34,900	0.0%	34,900

Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2024 RAS Subscriber	25,300	0.0%	25,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2024 RAS Subscriber	141,100	0.0%	141,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2024 RAS Subscriber	141,100	0.0%	141,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2024 RAS Subscriber	141,100	0.0%	141,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2024 RAS Subscriber	131,400	0.0%	131,400
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2024 RAS Subscriber	131,400	0.0%	131,400
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2024 RAS Subscriber	78,200	0.0%	78,200
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2024 RAS Subscriber	78,200	0.0%	78,200
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	56,800	0.0%	56,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2024 RAS Subscriber	56,800	0.0%	56,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	37,900	0.0%	37,900
Gartner for CDAOs Individual Access [1] - single user	2024 RAS Subscriber	79,200	0.0%	79,200
Gartner for CDAOs Individual Access [1] - multi-user	2024 RAS Subscriber	79,200	9.0%	72,072
Gartner for CDAOs Team [2] - Team Leader	2024 RAS Subscriber	72,100	0.0%	72,100
Gartner for CDAOs Team [2] - Team Member	2024 RAS Subscriber	47,600	0.0%	47,600
Gartner for CDAOs Team [2] - Tech Professional Team Member	2024 RAS Subscriber	18,100	0.0%	18,100
Gartner for CDAOs Executive Individual Access [1] - single user	2024 RAS Subscriber	154,700	0.0%	154,700
Gartner for CDAOs Executive Individual Access [1] - multi-user	2024 RAS Subscriber	154,700	9.1%	140,623
Gartner for CDAOs Executive Team [2] - Team Leader	2024 RAS Subscriber	140,600	0.0%	140,600
Gartner for CDAOs Executive Team [2] - Team Member	2024 RAS Subscriber	53,500	0.0%	53,500
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2024 RAS Subscriber	20,800	0.0%	20,800
Gartner for CISOs Individual Access [1] - single user	2024 RAS Subscriber	79,200	0.0%	79,200
Gartner for CISOs Individual Access [1] - multi-user	2024 RAS Subscriber	79,200	9.0%	72,072
Gartner for CISOs Team [2] - Team Leader	2024 RAS Subscriber	72,100	0.0%	72,100

Gartner for CISOs Team [2] - Team Member	2024 RAS Subscriber	47,600	0.0%	47,600
Gartner for CISOs Team [2] - Tech Professional Team Member	2024 RAS Subscriber	18,100	0.0%	18,100
Gartner for CISOs Executive Individual Access [1] - single user	2024 RAS Subscriber	154,700	0.0%	154,700
Gartner for CISOs Executive Individual Access [1] - multi-user	2024 RAS Subscriber	154,700	9.1%	140,623
Gartner for CISOs Executive Team [2] - Team Leader	2024 RAS Subscriber	140,600	0.0%	140,600
Gartner for CISOs Executive Team [2] - Team Member	2024 RAS Subscriber	53,500	0.0%	53,500
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2024 RAS Subscriber	20,800	0.0%	20,800
Gartner for Software Engineering Leaders Individual Access [1] - single user	2024 RAS Subscriber	79,200	0.0%	79,200
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2024 RAS Subscriber	79,200	9.0%	72,072
Gartner for Software Engineering Leaders Team [2] - Team Leader	2024 RAS Subscriber	72,100	0.0%	72,100
Gartner for Software Engineering Leaders Team [2] - Team Member	2024 RAS Subscriber	47,600	0.0%	47,600
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2024 RAS Subscriber	18,100	0.0%	18,100
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2024 RAS Subscriber	154,700	0.0%	154,700
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2024 RAS Subscriber	154,700	9.1%	140,623
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2024 RAS Subscriber	140,600	0.0%	140,600
Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2024 RAS Subscriber	53,500	0.0%	53,500
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2024 RAS Subscriber	20,800	0.0%	20,800
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2024 RAS Subscriber	100,700	0.0%	100,700
Enterprise IT Leadership Team [2] - Advisor Team Member	2024 RAS Subscriber	39,900	0.0%	39,900
Enterprise IT Leadership Team [2] - Cross Function Team Member	2024 RAS Subscriber	24,200	0.0%	24,200
Enterprise IT Leadership Team [2] - Role Team Member	2024 RAS Subscriber	15,200	0.0%	15,200
Enterprise IT Leadership Team [2] - Essentials Team Member	2024 RAS Subscriber	11,800	0.0%	11,800
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2024 RAS Subscriber	109,400	0.0%	109,400
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2024 RAS Subscriber	43,100	0.0%	43,100
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2024 RAS Subscriber	26,200	0.0%	26,200
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2024 RAS Subscriber	112,200	0.0%	112,200
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	47,300	0.0%	47,300
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	28,900	0.0%	28,900
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2024 RAS Subscriber	16,900	0.0%	16,900
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2024 RAS Subscriber	11,800	0.0%	11,800
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2024 RAS Subscriber	122,500	0.0%	122,500

Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	51,500	0.0%	51,500
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	31,600	0.0%	31,600
IT Leader Individual Access Reference [1] - single user	2024 RAS Subscriber	37,600	0.0%	37,600
IT Leader Individual Access Reference [1] - multi-user	2024 RAS Subscriber	37,600	37.6%	23,463
IT Leader Individual Access Advisor [1] - single user	2024 RAS Subscriber	53,800	0.0%	53,800
IT Leader Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	53,800	25.8%	39,920
IT Leadership Team [2] - Team Leader	2024 RAS Subscriber	39,900	0.0%	39,900
IT Leadership Team [2] - Advisor Team Member	2024 RAS Subscriber	39,900	0.0%	39,900
IT Leadership Team [2] - Cross Function Team Member	2024 RAS Subscriber	24,200	0.0%	24,200
IT Leadership Team [2] - Role Team Member	2024 RAS Subscriber	15,200	0.0%	15,200
IT Leadership Team [2] - Essentials Team Member	2024 RAS Subscriber	11,800	0.0%	11,800
IT Leadership Team Plus [2] - Team Leader	2024 RAS Subscriber	43,100	0.0%	43,100
IT Leadership Team Plus [2] - Advisor Team Member	2024 RAS Subscriber	43,100	0.0%	43,100
IT Leadership Team Plus [2] - Cross Function Team Member	2024 RAS Subscriber	26,200	0.0%	26,200
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2024 RAS Subscriber	41,300	0.0%	41,300
Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2024 RAS Subscriber	41,300	31.8%	28,167
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2024 RAS Subscriber	61,100	0.0%	61,100
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2024 RAS Subscriber	61,100	22.6%	47,292
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2024 RAS Subscriber	47,300	0.0%	47,300
Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	47,300	0.0%	47,300
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	28,900	0.0%	28,900
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2024 RAS Subscriber	16,900	0.0%	16,900
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2024 RAS Subscriber	11,800	0.0%	11,800
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2024 RAS Subscriber	51,500	0.0%	51,500
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2024 RAS Subscriber	51,500	0.0%	51,500
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2024 RAS Subscriber	31,600	0.0%	31,600
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2024 RAS Subscriber	73,700	0.0%	73,700
Technical Professionals Team [4, 5] - Additional Team Member	2024 RAS Subscriber	14,200	0.0%	14,200
Technical Professionals Advisor Department [4, 5]	2024 RAS Subscriber	153,100	0.0%	153,100
Technical Professionals Reference Department [4, 5]	2024 RAS Subscriber	102,900	0.0%	102,900
Finance Leaders Individual Access Advisor [1] - single user	2024 RAS Subscriber	53,400	0.0%	53,400

Finance Leaders Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	53,400	25.2%	39,944
Finance Leaders Team [2] - Team Leader	2024 RAS Subscriber	39,900	0.0%	39,900
Finance Leaders Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
Finance Leaders Team [2] - Reference Member	2024 RAS Subscriber	18,600	0.0%	18,600
Chief Financial Officers Individual Access [1] - single user	2024 RAS Subscriber	130,100	0.0%	130,100
Chief Financial Officers Individual Access [1] - multi-user	2024 RAS Subscriber	130,100	9.4%	117,871
Chief Financial Officers Team [2] - Team Leader	2024 RAS Subscriber	117,800	0.0%	117,800
Chief Financial Officers Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2024 RAS Subscriber	39,900	0.0%	39,900
Chief Financial Officers Team [2] - Reference Member	2024 RAS Subscriber	18,600	0.0%	18,600
Human Resources Leaders Individual Access [1] - single user	2024 RAS Subscriber	53,400	0.0%	53,400
Human Resources Leaders Individual Access [1] - multi-user	2024 RAS Subscriber	53,400	25.2%	39,944
Human Resources Leaders Team [2] - Team Leader	2024 RAS Subscriber	39,900	0.0%	39,900
Human Resources Leaders Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
Human Resources Leaders Team [2] - Reference Member	2024 RAS Subscriber	21,900	0.0%	21,900
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2024 RAS Subscriber	48,900	0.0%	48,900
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2024 RAS Subscriber	30,500	0.0%	30,500
Chief Human Resources Officers Individual Access [1] - single user	2024 RAS Subscriber	130,100	0.0%	130,100
Chief Human Resources Officers Individual Access [1] - multi-user	2024 RAS Subscriber	130,100	9.4%	117,871
Chief Human Resources Officers Team [2] - Team Leader	2024 RAS Subscriber	117,800	0.0%	117,800
Chief Human Resources Officers Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2024 RAS Subscriber	39,900	0.0%	39,900
Chief Human Resources Officers Team 2 - Reference Member	2024 RAS Subscriber	21,900	0.0%	21,900
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2024 RAS Subscriber	45,700	0.0%	45,700
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2024 RAS Subscriber	45,700	24.3%	34,595
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2024 RAS Subscriber	34,600	0.0%	34,600
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2024 RAS Subscriber	34,600	0.0%	34,600
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2024 RAS Subscriber	13,800	0.0%	13,800
R&D Leaders Individual Access Advisor [1] - single user	2024 RAS Subscriber	53,400	0.0%	53,400
R&D Leaders Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	53,400	25.2%	39,944
R&D Leaders Team [2] - Leader	2024 RAS Subscriber	39,900	0.0%	39,900
R&D Leaders Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
R&D Leaders Team [2] - Reference Member	2024 RAS Subscriber	21,900	0.0%	21,900
Marketing Leaders Individual Access Advisor [1] - single user	2024 RAS Subscriber	60,600	0.0%	60,600

Marketing Leaders Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	60,600	16.7%	50,480
Marketing Leaders Team [2] - Leader	2024 RAS Subscriber	50,500	0.0%	50,500
Marketing Leaders Team [2] - Advisor Member	2024 RAS Subscriber	50,500	0.0%	50,500
Marketing Leaders Team [2] - Reference Member	2024 RAS Subscriber	19,900	0.0%	19,900
Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2024 RAS Subscriber	143,200	0.0%	143,200
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2024 RAS Subscriber	143,200	10.6%	128,021
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2024 RAS Subscriber	128,100	0.0%	128,100
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2024 RAS Subscriber	50,500	0.0%	50,500
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2024 RAS Subscriber	50,500	0.0%	50,500
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2024 RAS Subscriber	19,900	0.0%	19,900
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2024 RAS Subscriber	53,400	0.0%	53,400
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	53,400	25.2%	39,944
Customer Service & Support Leaders Team [2] - Leader	2024 RAS Subscriber	39,900	0.0%	39,900
Customer Service & Support Leaders Team [2] - Advisor Member	2024 RAS Subscriber	39,900	0.0%	39,900
Customer Service & Support Leaders Team [2] - Reference Member	2024 RAS Subscriber	17,900	0.0%	17,900
North America Gartner Conferences [7] - IT Symposium/Xpo	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Finance Conference	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - ReImagineHR Conference	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2024 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2024 Conference Ticket	TBD	0.0%	TBD
Core Connect Individual Access Reference [1]- single user	2024 RAS Subscriber	32,400	0.0%	32,400
Core Connect Individual Access Reference [1]- multi-user	2024 RAS Subscriber	32,400	43.3%	18,371
Core Connect Individual Access Advisor [1] - single user	2024 RAS Subscriber	48,700	0.0%	48,700
Core Connect Individual Access Advisor [1] - multi-user	2024 RAS Subscriber	48,700	28.5%	34,821
IT News and Insights	2024 RAS Subscriber	850	0.0%	850
News and Insights	2024 RAS Subscriber	850	0.0%	850
Internal Advisory Session ** Limited Availability **	2024 RAS Session	24,700	0.0%	24,700

Remote Advisory Services ** Limited Availability **	2024 RAS Session	10,700	0.0%	10,700
Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2024 RAS Add-on	29,200	0.0%	29,200
Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2024 RAS Add-on	29,200	0.0%	29,200
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2024 RAS Add-on	29,200	0.0%	29,200
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2024 RAS Subscriber	77,400	0.0%	77,400
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2024 RAS Subscriber	51,400	0.0%	51,400
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2024 RAS Subscriber	77,400	0.0%	77,400
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2024 RAS Subscriber	51,400	0.0%	51,400
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2024 RAS Subscriber	37,600	0.0%	37,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2024 RAS Subscriber	37,600	0.0%	37,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2024 RAS Subscriber	75,200	0.0%	75,200
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2024 RAS Subscriber	112,700	0.0%	112,700
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2024 RAS Subscriber	150,300	0.0%	150,300
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2024 RAS Subscriber	35,300	0.0%	35,300
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2024 RAS Subscriber	40,300	0.0%	40,300
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2024 RAS Subscriber	40,300	37.8%	25,067
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2024 RAS Subscriber	59,400	0.0%	59,400
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2024 RAS Subscriber	59,400	25.8%	44,075
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2024 RAS Subscriber	44,000	0.0%	44,000
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2024 RAS Subscriber	44,000	0.0%	44,000
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2024 RAS Subscriber	25,900	0.0%	25,900

Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2024 RAS Subscriber	11,700	0.0%	11,700
Executive Programs V2 Guided Individual Access [1] - Single User	2025 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Individual Access [1] - Multi-User	2025 RAS Subscriber	170,200	9.1%	154,712
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2025 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2025 RAS Subscriber	97,100	9.2%	88,167
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2025 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400

Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Guided Team [2] Advisor Member	2025 RAS Subscriber	69,000	0.0%	69,000
Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	69,000	0.0%	69,000
Executive Programs V2 Guided Team [2] Cross Function Member	2025 RAS Subscriber	45,000	0.0%	45,000
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2025 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2025 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	88,200	0.0%	88,200
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700

Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	154,700	0.0%	154,700
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	79,400	0.0%	79,400
Executive Programs V2 Self-Directed Team [2] Advisor Member	2025 RAS Subscriber	69,000	0.0%	69,000
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2025 RAS Subscriber	69,000	0.0%	69,000
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2025 RAS Subscriber	45,000	0.0%	45,000
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	58,900	0.0%	58,900
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	58,900	0.0%	58,900
Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	58,900	0.0%	58,900
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	52,400	0.0%	52,400

Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	52,400	0.0%	52,400
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2025 RAS Subscriber	52,400	0.0%	52,400
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2025 RAS Subscriber	69,000	0.0%	69,000
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2025 RAS Subscriber	45,000	0.0%	45,000
Gartner for CIOs Individual Access [1] - single user	2025 RAS Subscriber	88,400	0.0%	88,400
Gartner for CIOs Individual Access [1] - multi-user	2025 RAS Subscriber	88,400	9.0%	80,444
Gartner for CIOs Team Plus [2] - Team Leader	2025 RAS Subscriber	80,500	0.0%	80,500
Gartner for CIOs Team Plus [2] - Advisor Team Member	2025 RAS Subscriber	58,800	0.0%	58,800
Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2025 RAS Subscriber	58,800	0.0%	58,800
Gartner for CIOs Team Plus [2] - Cross Function Team Member	2025 RAS Subscriber	40,900	0.0%	40,900
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2025 RAS Subscriber	97,100	0.0%	97,100
Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2025 RAS Subscriber	97,100	9.2%	88,167
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2025 RAS Subscriber	88,200	0.0%	88,200
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	69,000	0.0%	69,000
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2025 RAS Subscriber	69,000	0.0%	69,000
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	45,000	0.0%	45,000
Executive Programs Member Individual Access [1] - single user	2025 RAS Subscriber	144,400	0.0%	144,400
Executive Programs Member Individual Access [1] - multi-user user	2025 RAS Subscriber	144,400	11.0%	128,516
Executive Programs Leadership Team [2] - Team Leader	2025 RAS Subscriber	130,800	0.0%	130,800
Executive Programs Leadership Team [2] - IT Executive Team Member	2025 RAS Subscriber	130,800	0.0%	130,800
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2025 RAS Subscriber	130,800	0.0%	130,800
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2025 RAS Subscriber	119,600	0.0%	119,600
Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2025 RAS Subscriber	119,600	0.0%	119,600
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2025 RAS Subscriber	70,000	0.0%	70,000
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2025 RAS Subscriber	70,000	0.0%	70,000

Executive Programs Leadership Team [2] - Advisor Team Member	2025 RAS Subscriber	47,700	0.0%	47,700
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2025 RAS Subscriber	47,700	0.0%	47,700
Executive Programs Leadership Team [2] - Cross Function Team Member	2025 RAS Subscriber	34,600	0.0%	34,600
Executive Programs Leadership Team [2] - Role Team Member	2025 RAS Subscriber	24,900	0.0%	24,900
Executive Programs Leadership Team Plus [2] - Team Leader	2025 RAS Subscriber	142,600	0.0%	142,600
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2025 RAS Subscriber	142,600	8.1%	131,050
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2025 RAS Subscriber	142,600	0.0%	142,600
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2025 RAS Subscriber	142,600	0.0%	142,600
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2025 RAS Subscriber	130,500	0.0%	130,500
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2025 RAS Subscriber	130,500	0.0%	130,500
Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2025 RAS Subscriber	76,300	0.0%	76,300
Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2025 RAS Subscriber	76,300	0.0%	76,300
Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2025 RAS Subscriber	76,300	8.3%	69,968
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2025 RAS Subscriber	52,100	0.0%	52,100
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2025 RAS Subscriber	52,100	0.0%	52,100
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2025 RAS Subscriber	37,800	0.0%	37,800
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2025 RAS Subscriber	155,400	0.0%	155,400
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2025 RAS Subscriber	155,400	10.2%	139,550
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2025 RAS Subscriber	142,400	0.0%	142,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2025 RAS Subscriber	142,400	0.0%	142,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2025 RAS Subscriber	142,400	0.0%	142,400
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2025 RAS Subscriber	132,400	0.0%	132,400

Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2025 RAS Subscriber	132,400	0.0%	132,400
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2025 RAS Subscriber	79,100	0.0%	79,100
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2025 RAS Subscriber	79,100	0.0%	79,100
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	57,600	0.0%	57,600
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2025 RAS Subscriber	57,600	0.0%	57,600
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	38,400	0.0%	38,400
Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2025 RAS Subscriber	27,900	0.0%	27,900
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2025 RAS Subscriber	155,300	0.0%	155,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2025 RAS Subscriber	155,300	0.0%	155,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2025 RAS Subscriber	155,300	0.0%	155,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2025 RAS Subscriber	144,600	0.0%	144,600
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2025 RAS Subscriber	144,600	0.0%	144,600
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2025 RAS Subscriber	86,100	0.0%	86,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2025 RAS Subscriber	86,100	0.0%	86,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	62,500	0.0%	62,500

Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2025 RAS Subscriber	62,500	0.0%	62,500
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	41,700	0.0%	41,700
Gartner for CDAOs Individual Access [1] - single user	2025 RAS Subscriber	87,200	0.0%	87,200
Gartner for CDAOs Individual Access [1] - multi-user	2025 RAS Subscriber	87,200	9.0%	79,352
Gartner for CDAOs Team [2] - Team Leader	2025 RAS Subscriber	79,400	0.0%	79,400
Gartner for CDAOs Team [2] - Team Member	2025 RAS Subscriber	52,400	0.0%	52,400
Gartner for CDAOs Team [2] - Tech Professional Team Member	2025 RAS Subscriber	20,000	0.0%	20,000
Gartner for CDAOs Executive Individual Access [1] - single user	2025 RAS Subscriber	170,200	0.0%	170,200
Gartner for CDAOs Executive Individual Access [1] - multi-user	2025 RAS Subscriber	170,200	9.1%	154,712
Gartner for CDAOs Executive Team [2] - Team Leader	2025 RAS Subscriber	154,700	0.0%	154,700
Gartner for CDAOs Executive Team [2] - Team Member	2025 RAS Subscriber	58,900	0.0%	58,900
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2025 RAS Subscriber	22,900	0.0%	22,900
Gartner for CISOs Individual Access [1] - single user	2025 RAS Subscriber	87,200	0.0%	87,200
Gartner for CISOs Individual Access [1] - multi-user	2025 RAS Subscriber	87,200	9.0%	79,352
Gartner for CISOs Team [2] - Team Leader	2025 RAS Subscriber	79,400	0.0%	79,400
Gartner for CISOs Team [2] - Team Member	2025 RAS Subscriber	52,400	0.0%	52,400
Gartner for CISOs Team [2] - Tech Professional Team Member	2025 RAS Subscriber	20,000	0.0%	20,000
Gartner for CISOs Executive Individual Access [1] - single user	2025 RAS Subscriber	170,200	0.0%	170,200
Gartner for CISOs Executive Individual Access [1] - multi-user	2025 RAS Subscriber	170,200	9.1%	154,712
Gartner for CISOs Executive Team [2] - Team Leader	2025 RAS Subscriber	154,700	0.0%	154,700
Gartner for CISOs Executive Team [2] - Team Member	2025 RAS Subscriber	58,900	0.0%	58,900
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2025 RAS Subscriber	22,900	0.0%	22,900
Gartner for Software Engineering Leaders Individual Access [1] - single user	2025 RAS Subscriber	87,200	0.0%	87,200
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2025 RAS Subscriber	87,200	9.0%	79,352
Gartner for Software Engineering Leaders Team [2] - Team Leader	2025 RAS Subscriber	79,400	0.0%	79,400
Gartner for Software Engineering Leaders Team [2] - Team Member	2025 RAS Subscriber	52,400	0.0%	52,400
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2025 RAS Subscriber	20,000	0.0%	20,000
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2025 RAS Subscriber	170,200	0.0%	170,200
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2025 RAS Subscriber	170,200	9.1%	154,712
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2025 RAS Subscriber	154,700	0.0%	154,700
Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2025 RAS Subscriber	58,900	0.0%	58,900
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2025 RAS Subscriber	22,900	0.0%	22,900
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2025 RAS Subscriber	110,800	0.0%	110,800
Enterprise IT Leadership Team [2] - Advisor Team Member	2025 RAS Subscriber	43,900	0.0%	43,900

Enterprise IT Leadership Team [2] - Cross Function Team Member	2025 RAS Subscriber	26,700	0.0%	26,700
Enterprise IT Leadership Team [2] - Role Team Member	2025 RAS Subscriber	16,800	0.0%	16,800
Enterprise IT Leadership Team [2] - Essentials Team Member	2025 RAS Subscriber	13,000	0.0%	13,000
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2025 RAS Subscriber	120,400	0.0%	120,400
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2025 RAS Subscriber	47,500	0.0%	47,500
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2025 RAS Subscriber	28,900	0.0%	28,900
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2025 RAS Subscriber	123,500	0.0%	123,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	52,100	0.0%	52,100
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	31,800	0.0%	31,800
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2025 RAS Subscriber	18,600	0.0%	18,600
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2025 RAS Subscriber	13,000	0.0%	13,000
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2025 RAS Subscriber	134,800	0.0%	134,800
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	56,700	0.0%	56,700
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	34,800	0.0%	34,800
IT Leader Individual Access Reference [1] - single user	2025 RAS Subscriber	41,400	0.0%	41,400
IT Leader Individual Access Reference [1] - multi-user	2025 RAS Subscriber	41,400	37.6%	25,834
IT Leader Individual Access Advisor [1] - single user	2025 RAS Subscriber	59,200	0.0%	59,200
IT Leader Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	59,200	25.8%	43,927
IT Leadership Team [2] - Team Leader	2025 RAS Subscriber	43,900	0.0%	43,900
IT Leadership Team [2] - Advisor Team Member	2025 RAS Subscriber	43,900	0.0%	43,900
IT Leadership Team [2] - Cross Function Team Member	2025 RAS Subscriber	26,700	0.0%	26,700
IT Leadership Team [2] - Role Team Member	2025 RAS Subscriber	16,800	0.0%	16,800
IT Leadership Team [2] - Essentials Team Member	2025 RAS Subscriber	13,000	0.0%	13,000
IT Leadership Team Plus [2] - Team Leader	2025 RAS Subscriber	47,500	0.0%	47,500
IT Leadership Team Plus [2] - Advisor Team Member	2025 RAS Subscriber	47,500	0.0%	47,500
IT Leadership Team Plus [2] - Cross Function Team Member	2025 RAS Subscriber	28,900	0.0%	28,900
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2025 RAS Subscriber	45,500	0.0%	45,500
Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2025 RAS Subscriber	45,500	31.8%	31,031
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2025 RAS Subscriber	67,300	0.0%	67,300
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2025 RAS Subscriber	67,300	22.6%	52,091
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2025 RAS Subscriber	52,100	0.0%	52,100

Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	52,100	0.0%	52,100
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	31,800	0.0%	31,800
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2025 RAS Subscriber	18,600	0.0%	18,600
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2025 RAS Subscriber	13,000	0.0%	13,000
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2025 RAS Subscriber	56,700	0.0%	56,700
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2025 RAS Subscriber	56,700	0.0%	56,700
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2025 RAS Subscriber	34,800	0.0%	34,800
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2025 RAS Subscriber	81,100	0.0%	81,100
Technical Professionals Team [4, 5] - Additional Team Member	2025 RAS Subscriber	15,700	0.0%	15,700
Technical Professionals Advisor Department [4, 5]	2025 RAS Subscriber	168,500	0.0%	168,500
Technical Professionals Reference Department [4, 5]	2025 RAS Subscriber	113,200	0.0%	113,200
Finance Leaders Individual Access Advisor [1] - single user	2025 RAS Subscriber	58,800	0.0%	58,800
Finance Leaders Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	58,800	25.2%	43,983
Finance Leaders Team [2] - Team Leader	2025 RAS Subscriber	43,900	0.0%	43,900
Finance Leaders Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900
Finance Leaders Team [2] - Reference Member	2025 RAS Subscriber	20,500	0.0%	20,500
Chief Financial Officers Individual Access [1] - single user	2025 RAS Subscriber	143,200	0.0%	143,200
Chief Financial Officers Individual Access [1] - multi-user	2025 RAS Subscriber	143,200	9.4%	129,740
Chief Financial Officers Team [2] - Team Leader	2025 RAS Subscriber	129,600	0.0%	129,600
Chief Financial Officers Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2025 RAS Subscriber	43,900	0.0%	43,900
Chief Financial Officers Team [2] - Reference Member	2025 RAS Subscriber	20,500	0.0%	20,500
Human Resources Leaders Individual Access [1] - single user	2025 RAS Subscriber	58,800	0.0%	58,800
Human Resources Leaders Individual Access [1] - multi-user	2025 RAS Subscriber	58,800	25.2%	43,983
Human Resources Leaders Team [2] - Team Leader	2025 RAS Subscriber	43,900	0.0%	43,900
Human Resources Leaders Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900
Human Resources Leaders Team [2] - Reference Member	2025 RAS Subscriber	24,100	0.0%	24,100
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2025 RAS Subscriber	53,800	0.0%	53,800
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2025 RAS Subscriber	33,600	0.0%	33,600
Chief Human Resources Officers Individual Access [1] - single user	2025 RAS Subscriber	143,200	0.0%	143,200
Chief Human Resources Officers Individual Access [1] - multi-user	2025 RAS Subscriber	143,200	9.4%	129,740
Chief Human Resources Officers Team [2] - Team Leader	2025 RAS Subscriber	129,600	0.0%	129,600
Chief Human Resources Officers Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900

Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2025 RAS Subscriber	43,900	0.0%	43,900
Chief Human Resources Officers Team 2 - Reference Member	2025 RAS Subscriber	24,100	0.0%	24,100
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2025 RAS Subscriber	50,300	0.0%	50,300
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2025 RAS Subscriber	50,300	24.3%	38,078
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2025 RAS Subscriber	38,100	0.0%	38,100
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2025 RAS Subscriber	38,100	0.0%	38,100
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2025 RAS Subscriber	15,200	0.0%	15,200
R&D Leaders Individual Access Advisor [1] - single user	2025 RAS Subscriber	58,800	0.0%	58,800
R&D Leaders Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	58,800	25.2%	43,983
R&D Leaders Team [2] - Leader	2025 RAS Subscriber	43,900	0.0%	43,900
R&D Leaders Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900
R&D Leaders Team [2] - Reference Member	2025 RAS Subscriber	24,100	0.0%	24,100
Marketing Leaders Individual Access Advisor [1] - single user	2025 RAS Subscriber	66,700	0.0%	66,700
Marketing Leaders Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	66,700	16.7%	55,562
Marketing Leaders Team [2] - Leader	2025 RAS Subscriber	55,600	0.0%	55,600
Marketing Leaders Team [2] - Advisor Member	2025 RAS Subscriber	55,600	0.0%	55,600
Marketing Leaders Team [2] - Reference Member	2025 RAS Subscriber	21,900	0.0%	21,900
Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2025 RAS Subscriber	157,600	0.0%	157,600
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2025 RAS Subscriber	157,600	10.6%	140,895
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2025 RAS Subscriber	141,000	0.0%	141,000
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2025 RAS Subscriber	55,600	0.0%	55,600
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2025 RAS Subscriber	55,600	0.0%	55,600
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2025 RAS Subscriber	21,900	0.0%	21,900
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2025 RAS Subscriber	58,800	0.0%	58,800
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	58,800	25.2%	43,983
Customer Service & Support Leaders Team [2] - Leader	2025 RAS Subscriber	43,900	0.0%	43,900
Customer Service & Support Leaders Team [2] - Advisor Member	2025 RAS Subscriber	43,900	0.0%	43,900
Customer Service & Support Leaders Team [2] - Reference Member	2025 RAS Subscriber	19,700	0.0%	19,700
North America Gartner Conferences [7] - IT Symposium/Xpo	2025 Conference Ticket	TBD	0.0%	TBD

North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2025 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2025 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Finance Conference	2025 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - ReImagineHR Conference	2025 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2025 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2025 Conference Ticket	TBD	0.0%	TBD
Core Connect Individual Access Reference [1]- single user	2025 RAS Subscriber	35,700	0.0%	35,700
Core Connect Individual Access Reference [1]- multi-user	2025 RAS Subscriber	35,700	43.3%	20,242
Core Connect Individual Access Advisor [1] - single user	2025 RAS Subscriber	53,600	0.0%	53,600
Core Connect Individual Access Advisor [1] - multi-user	2025 RAS Subscriber	53,600	28.5%	38,324
IT News and Insights	2025 RAS Subscriber	940	0.0%	940
News and Insights	2025 RAS Subscriber	940	0.0%	940
Internal Advisory Session ** Limited Availability **	2025 RAS Session	27,200	0.0%	27,200
Remote Advisory Services ** Limited Availability **	2025 RAS Session	11,800	0.0%	11,800
Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2025 RAS Add-on	32,200	0.0%	32,200
Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2025 RAS Add-on	32,200	0.0%	32,200
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2025 RAS Add-on	32,200	0.0%	32,200
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2025 RAS Subscriber	85,200	0.0%	85,200
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2025 RAS Subscriber	56,600	0.0%	56,600
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2025 RAS Subscriber	85,200	0.0%	85,200
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2025 RAS Subscriber	56,600	0.0%	56,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2025 RAS Subscriber	41,400	0.0%	41,400
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2025 RAS Subscriber	41,400	0.0%	41,400
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2025 RAS Subscriber	82,800	0.0%	82,800

Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2025 RAS Subscriber	124,000	0.0%	124,000
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2025 RAS Subscriber	165,400	0.0%	165,400
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2025 RAS Subscriber	38,900	0.0%	38,900
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2025 RAS Subscriber	44,400	0.0%	44,400
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2025 RAS Subscriber	44,400	37.8%	27,617
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2025 RAS Subscriber	65,400	0.0%	65,400
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2025 RAS Subscriber	65,400	25.8%	48,527
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2025 RAS Subscriber	48,400	0.0%	48,400
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2025 RAS Subscriber	48,400	0.0%	48,400
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2025 RAS Subscriber	28,500	0.0%	28,500
Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2025 RAS Subscriber	12,900	0.0%	12,900
Executive Programs V2 Guided Individual Access [1] - Single User	2026 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Individual Access [1] - Multi-User	2026 RAS Subscriber	187,300	9.1%	170,256
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2026 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2026 RAS Subscriber	106,900	9.2%	97,066
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2026 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200

Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Guided Team [2] Advisor Member	2026 RAS Subscriber	75,900	0.0%	75,900
Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	75,900	0.0%	75,900

Executive Programs V2 Guided Team [2] Cross Function Member	2026 RAS Subscriber	49,500	0.0%	49,500
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2026 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2026 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	97,100	0.0%	97,100
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	170,200	0.0%	170,200
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400

Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	87,400	0.0%	87,400
Executive Programs V2 Self-Directed Team [2] Advisor Member	2026 RAS Subscriber	75,900	0.0%	75,900
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2026 RAS Subscriber	75,900	0.0%	75,900
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2026 RAS Subscriber	49,500	0.0%	49,500
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	64,800	0.0%	64,800
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	64,800	0.0%	64,800
Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	64,800	0.0%	64,800
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	57,700	0.0%	57,700
Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	57,700	0.0%	57,700
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2026 RAS Subscriber	57,700	0.0%	57,700
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2026 RAS Subscriber	75,900	0.0%	75,900
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2026 RAS Subscriber	49,500	0.0%	49,500
Gartner for CIOs Individual Access [1] - single user	2026 RAS Subscriber	97,300	0.0%	97,300
Gartner for CIOs Individual Access [1] - multi-user	2026 RAS Subscriber	97,300	9.0%	88,543
Gartner for CIOs Team Plus [2] - Team Leader	2026 RAS Subscriber	88,600	0.0%	88,600
Gartner for CIOs Team Plus [2] - Advisor Team Member	2026 RAS Subscriber	64,700	0.0%	64,700
Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2026 RAS Subscriber	64,700	0.0%	64,700

Gartner for CIOs Team Plus [2] - Cross Function Team Member	2026 RAS Subscriber	45,000	0.0%	45,000
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2026 RAS Subscriber	106,900	0.0%	106,900
Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2026 RAS Subscriber	106,900	9.2%	97,066
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2026 RAS Subscriber	97,100	0.0%	97,100
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	75,900	0.0%	75,900
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2026 RAS Subscriber	75,900	0.0%	75,900
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	49,500	0.0%	49,500
Executive Programs Member Individual Access [1] - single user	2026 RAS Subscriber	158,900	0.0%	158,900
Executive Programs Member Individual Access [1] - multi-user user	2026 RAS Subscriber	158,900	11.0%	141,421
Executive Programs Leadership Team [2] - Team Leader	2026 RAS Subscriber	143,900	0.0%	143,900
Executive Programs Leadership Team [2] - IT Executive Team Member	2026 RAS Subscriber	143,900	0.0%	143,900
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2026 RAS Subscriber	143,900	0.0%	143,900
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2026 RAS Subscriber	131,600	0.0%	131,600
Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2026 RAS Subscriber	131,600	0.0%	131,600
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2026 RAS Subscriber	77,000	0.0%	77,000
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2026 RAS Subscriber	77,000	0.0%	77,000
Executive Programs Leadership Team [2] - Advisor Team Member	2026 RAS Subscriber	52,500	0.0%	52,500
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2026 RAS Subscriber	52,500	0.0%	52,500
Executive Programs Leadership Team [2] - Cross Function Team Member	2026 RAS Subscriber	38,100	0.0%	38,100
Executive Programs Leadership Team [2] - Role Team Member	2026 RAS Subscriber	27,400	0.0%	27,400
Executive Programs Leadership Team Plus [2] - Team Leader	2026 RAS Subscriber	156,900	0.0%	156,900
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2026 RAS Subscriber	156,900	8.1%	144,192
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2026 RAS Subscriber	156,900	0.0%	156,900
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2026 RAS Subscriber	156,900	0.0%	156,900
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2026 RAS Subscriber	143,600	0.0%	143,600
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2026 RAS Subscriber	143,600	0.0%	143,600
Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2026 RAS Subscriber	84,000	0.0%	84,000

Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2026 RAS Subscriber	84,000	0.0%	84,000
Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2026 RAS Subscriber	84,000	8.3%	77,028
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2026 RAS Subscriber	57,400	0.0%	57,400
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2026 RAS Subscriber	57,400	0.0%	57,400
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2026 RAS Subscriber	41,600	0.0%	41,600
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2026 RAS Subscriber	171,000	0.0%	171,000
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2026 RAS Subscriber	171,000	10.2%	153,558
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2026 RAS Subscriber	156,700	0.0%	156,700
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2026 RAS Subscriber	156,700	0.0%	156,700
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2026 RAS Subscriber	156,700	0.0%	156,700
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2026 RAS Subscriber	145,700	0.0%	145,700
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2026 RAS Subscriber	145,700	0.0%	145,700
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2026 RAS Subscriber	87,100	0.0%	87,100
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2026 RAS Subscriber	87,100	0.0%	87,100
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	63,400	0.0%	63,400
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2026 RAS Subscriber	63,400	0.0%	63,400
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	42,300	0.0%	42,300
Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2026 RAS Subscriber	30,700	0.0%	30,700

Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2026 RAS Subscriber	170,900	0.0%	170,900
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2026 RAS Subscriber	170,900	0.0%	170,900
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2026 RAS Subscriber	170,900	0.0%	170,900
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2026 RAS Subscriber	159,100	0.0%	159,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2026 RAS Subscriber	159,100	0.0%	159,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2026 RAS Subscriber	94,800	0.0%	94,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2026 RAS Subscriber	94,800	0.0%	94,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	68,800	0.0%	68,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2026 RAS Subscriber	68,800	0.0%	68,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	45,900	0.0%	45,900
Gartner for CDAOs Individual Access [1] - single user	2026 RAS Subscriber	96,000	0.0%	96,000
Gartner for CDAOs Individual Access [1] - multi-user	2026 RAS Subscriber	96,000	9.0%	87,360
Gartner for CDAOs Team [2] - Team Leader	2026 RAS Subscriber	87,400	0.0%	87,400
Gartner for CDAOs Team [2] - Team Member	2026 RAS Subscriber	57,700	0.0%	57,700
Gartner for CDAOs Team [2] - Tech Professional Team Member	2026 RAS Subscriber	22,000	0.0%	22,000
Gartner for CDAOs Executive Individual Access [1] - single user	2026 RAS Subscriber	187,300	0.0%	187,300
Gartner for CDAOs Executive Individual Access [1] - multi-user	2026 RAS Subscriber	187,300	9.1%	170,256
Gartner for CDAOs Executive Team [2] - Team Leader	2026 RAS Subscriber	170,200	0.0%	170,200
Gartner for CDAOs Executive Team [2] - Team Member	2026 RAS Subscriber	64,800	0.0%	64,800
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2026 RAS Subscriber	25,200	0.0%	25,200
Gartner for CISOs Individual Access [1] - single user	2026 RAS Subscriber	96,000	0.0%	96,000
Gartner for CISOs Individual Access [1] - multi-user	2026 RAS Subscriber	96,000	9.0%	87,360
Gartner for CISOs Team [2] - Team Leader	2026 RAS Subscriber	87,400	0.0%	87,400
Gartner for CISOs Team [2] - Team Member	2026 RAS Subscriber	57,700	0.0%	57,700

Gartner for CISOs Team [2] - Tech Professional Team Member	2026 RAS Subscriber	22,000	0.0%	22,000
Gartner for CISOs Executive Individual Access [1] - single user	2026 RAS Subscriber	187,300	0.0%	187,300
Gartner for CISOs Executive Individual Access [1] - multi-user	2026 RAS Subscriber	187,300	9.1%	170,256
Gartner for CISOs Executive Team [2] - Team Leader	2026 RAS Subscriber	170,200	0.0%	170,200
Gartner for CISOs Executive Team [2] - Team Member	2026 RAS Subscriber	64,800	0.0%	64,800
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2026 RAS Subscriber	25,200	0.0%	25,200
Gartner for Software Engineering Leaders Individual Access [1] - single user	2026 RAS Subscriber	96,000	0.0%	96,000
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2026 RAS Subscriber	96,000	9.0%	87,360
Gartner for Software Engineering Leaders Team [2] - Team Leader	2026 RAS Subscriber	87,400	0.0%	87,400
Gartner for Software Engineering Leaders Team [2] - Team Member	2026 RAS Subscriber	57,700	0.0%	57,700
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2026 RAS Subscriber	22,000	0.0%	22,000
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2026 RAS Subscriber	187,300	0.0%	187,300
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2026 RAS Subscriber	187,300	9.1%	170,256
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2026 RAS Subscriber	170,200	0.0%	170,200
Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2026 RAS Subscriber	64,800	0.0%	64,800
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2026 RAS Subscriber	25,200	0.0%	25,200
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2026 RAS Subscriber	121,900	0.0%	121,900
Enterprise IT Leadership Team [2] - Advisor Team Member	2026 RAS Subscriber	48,300	0.0%	48,300
Enterprise IT Leadership Team [2] - Cross Function Team Member	2026 RAS Subscriber	29,400	0.0%	29,400
Enterprise IT Leadership Team [2] - Role Team Member	2026 RAS Subscriber	18,500	0.0%	18,500
Enterprise IT Leadership Team [2] - Essentials Team Member	2026 RAS Subscriber	14,300	0.0%	14,300
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2026 RAS Subscriber	132,500	0.0%	132,500
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2026 RAS Subscriber	52,300	0.0%	52,300
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2026 RAS Subscriber	31,800	0.0%	31,800
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2026 RAS Subscriber	135,900	0.0%	135,900
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	57,400	0.0%	57,400
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	35,000	0.0%	35,000
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2026 RAS Subscriber	20,500	0.0%	20,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2026 RAS Subscriber	14,300	0.0%	14,300
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2026 RAS Subscriber	148,300	0.0%	148,300
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	62,400	0.0%	62,400

Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	38,300	0.0%	38,300
IT Leader Individual Access Reference [1] - single user	2026 RAS Subscriber	45,600	0.0%	45,600
IT Leader Individual Access Reference [1] - multi-user	2026 RAS Subscriber	45,600	37.6%	28,455
IT Leader Individual Access Advisor [1] - single user	2026 RAS Subscriber	65,200	0.0%	65,200
IT Leader Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	65,200	25.8%	48,379
IT Leadership Team [2] - Team Leader	2026 RAS Subscriber	48,300	0.0%	48,300
IT Leadership Team [2] - Advisor Team Member	2026 RAS Subscriber	48,300	0.0%	48,300
IT Leadership Team [2] - Cross Function Team Member	2026 RAS Subscriber	29,400	0.0%	29,400
IT Leadership Team [2] - Role Team Member	2026 RAS Subscriber	18,500	0.0%	18,500
IT Leadership Team [2] - Essentials Team Member	2026 RAS Subscriber	14,300	0.0%	14,300
IT Leadership Team Plus [2] - Team Leader	2026 RAS Subscriber	52,300	0.0%	52,300
IT Leadership Team Plus [2] - Advisor Team Member	2026 RAS Subscriber	52,300	0.0%	52,300
IT Leadership Team Plus [2] - Cross Function Team Member	2026 RAS Subscriber	31,800	0.0%	31,800
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2026 RAS Subscriber	50,100	0.0%	50,100
Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2026 RAS Subscriber	50,100	31.8%	34,169
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2026 RAS Subscriber	74,100	0.0%	74,100
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2026 RAS Subscriber	74,100	22.6%	57,354
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2026 RAS Subscriber	57,400	0.0%	57,400
Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	57,400	0.0%	57,400
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	35,000	0.0%	35,000
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2026 RAS Subscriber	20,500	0.0%	20,500
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2026 RAS Subscriber	14,300	0.0%	14,300
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2026 RAS Subscriber	62,400	0.0%	62,400
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2026 RAS Subscriber	62,400	0.0%	62,400
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2026 RAS Subscriber	38,300	0.0%	38,300
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2026 RAS Subscriber	89,300	0.0%	89,300
Technical Professionals Team [4, 5] - Additional Team Member	2026 RAS Subscriber	17,300	0.0%	17,300
Technical Professionals Advisor Department [4, 5]	2026 RAS Subscriber	185,400	0.0%	185,400
Technical Professionals Reference Department [4, 5]	2026 RAS Subscriber	124,600	0.0%	124,600
Finance Leaders Individual Access Advisor [1] - single user	2026 RAS Subscriber	64,700	0.0%	64,700
Finance Leaders Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	64,700	25.2%	48,396
Finance Leaders Team [2] - Team Leader	2026 RAS Subscriber	48,300	0.0%	48,300
Finance Leaders Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300

Finance Leaders Team [2] - Reference Member	2026 RAS Subscriber	22,600	0.0%	22,600
Chief Financial Officers Individual Access [1] - single user	2026 RAS Subscriber	157,600	0.0%	157,600
Chief Financial Officers Individual Access [1] - multi-user	2026 RAS Subscriber	157,600	9.4%	142,786
Chief Financial Officers Team [2] - Team Leader	2026 RAS Subscriber	142,600	0.0%	142,600
Chief Financial Officers Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2026 RAS Subscriber	48,300	0.0%	48,300
Chief Financial Officers Team [2] - Reference Member	2026 RAS Subscriber	22,600	0.0%	22,600
Human Resources Leaders Individual Access [1] - single user	2026 RAS Subscriber	64,700	0.0%	64,700
Human Resources Leaders Individual Access [1] - multi-user	2026 RAS Subscriber	64,700	25.2%	48,396
Human Resources Leaders Team [2] - Team Leader	2026 RAS Subscriber	48,300	0.0%	48,300
Human Resources Leaders Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300
Human Resources Leaders Team [2] - Reference Member	2026 RAS Subscriber	26,600	0.0%	26,600
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2026 RAS Subscriber	59,200	0.0%	59,200
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2026 RAS Subscriber	37,000	0.0%	37,000
Chief Human Resources Officers Individual Access [1] - single user	2026 RAS Subscriber	157,600	0.0%	157,600
Chief Human Resources Officers Individual Access [1] - multi-user	2026 RAS Subscriber	157,600	9.4%	142,786
Chief Human Resources Officers Team [2] - Team Leader	2026 RAS Subscriber	142,600	0.0%	142,600
Chief Human Resources Officers Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300
Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2026 RAS Subscriber	48,300	0.0%	48,300
Chief Human Resources Officers Team 2 - Reference Member	2026 RAS Subscriber	26,600	0.0%	26,600
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2026 RAS Subscriber	55,400	0.0%	55,400
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2026 RAS Subscriber	55,400	24.3%	41,938
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2026 RAS Subscriber	42,000	0.0%	42,000
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2026 RAS Subscriber	42,000	0.0%	42,000
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2026 RAS Subscriber	16,800	0.0%	16,800
R&D Leaders Individual Access Advisor [1] - single user	2026 RAS Subscriber	64,700	0.0%	64,700
R&D Leaders Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	64,700	25.2%	48,396
R&D Leaders Team [2] - Leader	2026 RAS Subscriber	48,300	0.0%	48,300
R&D Leaders Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300
R&D Leaders Team [2] - Reference Member	2026 RAS Subscriber	26,600	0.0%	26,600
Marketing Leaders Individual Access Advisor [1] - single user	2026 RAS Subscriber	73,400	0.0%	73,400
Marketing Leaders Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	73,400	16.7%	61,143
Marketing Leaders Team [2] - Leader	2026 RAS Subscriber	61,200	0.0%	61,200
Marketing Leaders Team [2] - Advisor Member	2026 RAS Subscriber	61,200	0.0%	61,200

Marketing Leaders Team [2] - Reference Member	2026 RAS Subscriber	24,100	0.0%	24,100
Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2026 RAS Subscriber	173,400	0.0%	173,400
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2026 RAS Subscriber	173,400	10.6%	155,020
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2026 RAS Subscriber	155,100	0.0%	155,100
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2026 RAS Subscriber	61,200	0.0%	61,200
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2026 RAS Subscriber	61,200	0.0%	61,200
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2026 RAS Subscriber	24,100	0.0%	24,100
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2026 RAS Subscriber	64,700	0.0%	64,700
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	64,700	25.2%	48,396
Customer Service & Support Leaders Team [2] - Leader	2026 RAS Subscriber	48,300	0.0%	48,300
Customer Service & Support Leaders Team [2] - Advisor Member	2026 RAS Subscriber	48,300	0.0%	48,300
Customer Service & Support Leaders Team [2] - Reference Member	2026 RAS Subscriber	21,700	0.0%	21,700
North America Gartner Conferences [7] - IT Symposium/Xpo	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Finance Conference	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - ReImagineHR Conference	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2026 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2026 Conference Ticket	TBD	0.0%	TBD
Core Connect Individual Access Reference [1]- single user	2026 RAS Subscriber	39,300	0.0%	39,300
Core Connect Individual Access Reference [1]- multi-user	2026 RAS Subscriber	39,300	43.3%	22,284
Core Connect Individual Access Advisor [1] - single user	2026 RAS Subscriber	59,000	0.0%	59,000
Core Connect Individual Access Advisor [1] - multi-user	2026 RAS Subscriber	59,000	28.5%	42,185
IT News and Insights	2026 RAS Subscriber	1,040	0.0%	1,040
News and Insights	2026 RAS Subscriber	1,040	0.0%	1,040
Internal Advisory Session ** Limited Availability **	2026 RAS Session	30,000	0.0%	30,000
Remote Advisory Services ** Limited Availability **	2026 RAS Session	13,000	0.0%	13,000

Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2026 RAS Add-on	35,500	0.0%	35,500
Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2026 RAS Add-on	35,500	0.0%	35,500
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2026 RAS Add-on	35,500	0.0%	35,500
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2026 RAS Subscriber	93,800	0.0%	93,800
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2026 RAS Subscriber	62,300	0.0%	62,300
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2026 RAS Subscriber	93,800	0.0%	93,800
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2026 RAS Subscriber	62,300	0.0%	62,300
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2026 RAS Subscriber	45,600	0.0%	45,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2026 RAS Subscriber	45,600	0.0%	45,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2026 RAS Subscriber	91,100	0.0%	91,100
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2026 RAS Subscriber	136,400	0.0%	136,400
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2026 RAS Subscriber	182,000	0.0%	182,000
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2026 RAS Subscriber	42,800	0.0%	42,800
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2026 RAS Subscriber	48,900	0.0%	48,900
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2026 RAS Subscriber	48,900	37.8%	30,416
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2026 RAS Subscriber	72,000	0.0%	72,000
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2026 RAS Subscriber	72,000	25.8%	53,424
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2026 RAS Subscriber	53,300	0.0%	53,300
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2026 RAS Subscriber	53,300	0.0%	53,300
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2026 RAS Subscriber	31,400	0.0%	31,400
Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2026 RAS Subscriber	14,200	0.0%	14,200

Executive Programs V2 Guided Individual Access [1] - Single User	2027 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Individual Access [1] - Multi-User	2027 RAS Subscriber	206,100	9.1%	187,345
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2027 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2027 RAS Subscriber	117,600	9.2%	106,781
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2027 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200

Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Guided Team [2] Advisor Member	2027 RAS Subscriber	83,500	0.0%	83,500
Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	83,500	0.0%	83,500
Executive Programs V2 Guided Team [2] Cross Function Member	2027 RAS Subscriber	54,500	0.0%	54,500
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2027 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2027 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	106,900	0.0%	106,900
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300

Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	187,300	0.0%	187,300
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	96,200	0.0%	96,200
Executive Programs V2 Self-Directed Team [2] Advisor Member	2027 RAS Subscriber	83,500	0.0%	83,500
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2027 RAS Subscriber	83,500	0.0%	83,500
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2027 RAS Subscriber	54,500	0.0%	54,500
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	71,300	0.0%	71,300
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	71,300	0.0%	71,300
Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	71,300	0.0%	71,300
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	63,500	0.0%	63,500

Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	63,500	0.0%	63,500
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2027 RAS Subscriber	63,500	0.0%	63,500
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2027 RAS Subscriber	83,500	0.0%	83,500
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2027 RAS Subscriber	54,500	0.0%	54,500
Gartner for CIOs Individual Access [1] - single user	2027 RAS Subscriber	107,100	0.0%	107,100
Gartner for CIOs Individual Access [1] - multi-user	2027 RAS Subscriber	107,100	9.0%	97,461
Gartner for CIOs Team Plus [2] - Team Leader	2027 RAS Subscriber	97,500	0.0%	97,500
Gartner for CIOs Team Plus [2] - Advisor Team Member	2027 RAS Subscriber	71,200	0.0%	71,200
Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2027 RAS Subscriber	71,200	0.0%	71,200
Gartner for CIOs Team Plus [2] - Cross Function Team Member	2027 RAS Subscriber	49,500	0.0%	49,500
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2027 RAS Subscriber	117,600	0.0%	117,600
Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2027 RAS Subscriber	117,600	9.2%	106,781
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2027 RAS Subscriber	106,900	0.0%	106,900
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	83,500	0.0%	83,500
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2027 RAS Subscriber	83,500	0.0%	83,500
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	54,500	0.0%	54,500
Executive Programs Member Individual Access [1] - single user	2027 RAS Subscriber	174,800	0.0%	174,800
Executive Programs Member Individual Access [1] - multi-user user	2027 RAS Subscriber	174,800	11.0%	155,572
Executive Programs Leadership Team [2] - Team Leader	2027 RAS Subscriber	158,300	0.0%	158,300
Executive Programs Leadership Team [2] - IT Executive Team Member	2027 RAS Subscriber	158,300	0.0%	158,300
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2027 RAS Subscriber	158,300	0.0%	158,300
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2027 RAS Subscriber	144,800	0.0%	144,800
Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2027 RAS Subscriber	144,800	0.0%	144,800
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2027 RAS Subscriber	84,700	0.0%	84,700
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2027 RAS Subscriber	84,700	0.0%	84,700

Executive Programs Leadership Team [2] - Advisor Team Member	2027 RAS Subscriber	57,800	0.0%	57,800
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2027 RAS Subscriber	57,800	0.0%	57,800
Executive Programs Leadership Team [2] - Cross Function Team Member	2027 RAS Subscriber	42,000	0.0%	42,000
Executive Programs Leadership Team [2] - Role Team Member	2027 RAS Subscriber	30,200	0.0%	30,200
Executive Programs Leadership Team Plus [2] - Team Leader	2027 RAS Subscriber	172,600	0.0%	172,600
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2027 RAS Subscriber	172,600	8.1%	158,620
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2027 RAS Subscriber	172,600	0.0%	172,600
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2027 RAS Subscriber	172,600	0.0%	172,600
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2027 RAS Subscriber	158,000	0.0%	158,000
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2027 RAS Subscriber	158,000	0.0%	158,000
Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2027 RAS Subscriber	92,400	0.0%	92,400
Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2027 RAS Subscriber	92,400	0.0%	92,400
Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2027 RAS Subscriber	92,400	8.3%	84,731
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2027 RAS Subscriber	63,200	0.0%	63,200
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2027 RAS Subscriber	63,200	0.0%	63,200
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2027 RAS Subscriber	45,800	0.0%	45,800
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2027 RAS Subscriber	188,100	0.0%	188,100
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2027 RAS Subscriber	188,100	10.2%	168,914
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2027 RAS Subscriber	172,400	0.0%	172,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2027 RAS Subscriber	172,400	0.0%	172,400
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2027 RAS Subscriber	172,400	0.0%	172,400
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2027 RAS Subscriber	160,300	0.0%	160,300

Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2027 RAS Subscriber	160,300	0.0%	160,300
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2027 RAS Subscriber	95,900	0.0%	95,900
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2027 RAS Subscriber	95,900	0.0%	95,900
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	69,800	0.0%	69,800
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2027 RAS Subscriber	69,800	0.0%	69,800
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	46,600	0.0%	46,600
Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2027 RAS Subscriber	33,800	0.0%	33,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2027 RAS Subscriber	188,000	0.0%	188,000
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2027 RAS Subscriber	188,000	0.0%	188,000
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2027 RAS Subscriber	188,000	0.0%	188,000
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2027 RAS Subscriber	175,100	0.0%	175,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2027 RAS Subscriber	175,100	0.0%	175,100
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2027 RAS Subscriber	104,300	0.0%	104,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2027 RAS Subscriber	104,300	0.0%	104,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	75,700	0.0%	75,700

Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2027 RAS Subscriber	75,700	0.0%	75,700
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	50,500	0.0%	50,500
Gartner for CDAOs Individual Access [1] - single user	2027 RAS Subscriber	105,600	0.0%	105,600
Gartner for CDAOs Individual Access [1] - multi-user	2027 RAS Subscriber	105,600	9.0%	96,096
Gartner for CDAOs Team [2] - Team Leader	2027 RAS Subscriber	96,200	0.0%	96,200
Gartner for CDAOs Team [2] - Team Member	2027 RAS Subscriber	63,500	0.0%	63,500
Gartner for CDAOs Team [2] - Tech Professional Team Member	2027 RAS Subscriber	24,200	0.0%	24,200
Gartner for CDAOs Executive Individual Access [1] - single user	2027 RAS Subscriber	206,100	0.0%	206,100
Gartner for CDAOs Executive Individual Access [1] - multi-user	2027 RAS Subscriber	206,100	9.1%	187,345
Gartner for CDAOs Executive Team [2] - Team Leader	2027 RAS Subscriber	187,300	0.0%	187,300
Gartner for CDAOs Executive Team [2] - Team Member	2027 RAS Subscriber	71,300	0.0%	71,300
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2027 RAS Subscriber	27,800	0.0%	27,800
Gartner for CISOs Individual Access [1] - single user	2027 RAS Subscriber	105,600	0.0%	105,600
Gartner for CISOs Individual Access [1] - multi-user	2027 RAS Subscriber	105,600	9.0%	96,096
Gartner for CISOs Team [2] - Team Leader	2027 RAS Subscriber	96,200	0.0%	96,200
Gartner for CISOs Team [2] - Team Member	2027 RAS Subscriber	63,500	0.0%	63,500
Gartner for CISOs Team [2] - Tech Professional Team Member	2027 RAS Subscriber	24,200	0.0%	24,200
Gartner for CISOs Executive Individual Access [1] - single user	2027 RAS Subscriber	206,100	0.0%	206,100
Gartner for CISOs Executive Individual Access [1] - multi-user	2027 RAS Subscriber	206,100	9.1%	187,345
Gartner for CISOs Executive Team [2] - Team Leader	2027 RAS Subscriber	187,300	0.0%	187,300
Gartner for CISOs Executive Team [2] - Team Member	2027 RAS Subscriber	71,300	0.0%	71,300
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2027 RAS Subscriber	27,800	0.0%	27,800
Gartner for Software Engineering Leaders Individual Access [1] - single user	2027 RAS Subscriber	105,600	0.0%	105,600
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2027 RAS Subscriber	105,600	9.0%	96,096
Gartner for Software Engineering Leaders Team [2] - Team Leader	2027 RAS Subscriber	96,200	0.0%	96,200
Gartner for Software Engineering Leaders Team [2] - Team Member	2027 RAS Subscriber	63,500	0.0%	63,500
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2027 RAS Subscriber	24,200	0.0%	24,200
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2027 RAS Subscriber	206,100	0.0%	206,100
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2027 RAS Subscriber	206,100	9.1%	187,345
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2027 RAS Subscriber	187,300	0.0%	187,300
Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2027 RAS Subscriber	71,300	0.0%	71,300
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2027 RAS Subscriber	27,800	0.0%	27,800
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2027 RAS Subscriber	134,100	0.0%	134,100
Enterprise IT Leadership Team [2] - Advisor Team Member	2027 RAS Subscriber	53,200	0.0%	53,200

Enterprise IT Leadership Team [2] - Cross Function Team Member	2027 RAS Subscriber	32,400	0.0%	32,400
Enterprise IT Leadership Team [2] - Role Team Member	2027 RAS Subscriber	20,400	0.0%	20,400
Enterprise IT Leadership Team [2] - Essentials Team Member	2027 RAS Subscriber	15,800	0.0%	15,800
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2027 RAS Subscriber	145,800	0.0%	145,800
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2027 RAS Subscriber	57,600	0.0%	57,600
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2027 RAS Subscriber	35,000	0.0%	35,000
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2027 RAS Subscriber	149,500	0.0%	149,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	63,200	0.0%	63,200
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	38,500	0.0%	38,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2027 RAS Subscriber	22,600	0.0%	22,600
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2027 RAS Subscriber	15,800	0.0%	15,800
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2027 RAS Subscriber	163,200	0.0%	163,200
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	68,700	0.0%	68,700
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	42,200	0.0%	42,200
IT Leader Individual Access Reference [1] - single user	2027 RAS Subscriber	50,200	0.0%	50,200
IT Leader Individual Access Reference [1] - multi-user	2027 RAS Subscriber	50,200	37.6%	31,325
IT Leader Individual Access Advisor [1] - single user	2027 RAS Subscriber	71,800	0.0%	71,800
IT Leader Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	71,800	25.8%	53,276
IT Leadership Team [2] - Team Leader	2027 RAS Subscriber	53,200	0.0%	53,200
IT Leadership Team [2] - Advisor Team Member	2027 RAS Subscriber	53,200	0.0%	53,200
IT Leadership Team [2] - Cross Function Team Member	2027 RAS Subscriber	32,400	0.0%	32,400
IT Leadership Team [2] - Role Team Member	2027 RAS Subscriber	20,400	0.0%	20,400
IT Leadership Team [2] - Essentials Team Member	2027 RAS Subscriber	15,800	0.0%	15,800
IT Leadership Team Plus [2] - Team Leader	2027 RAS Subscriber	57,600	0.0%	57,600
IT Leadership Team Plus [2] - Advisor Team Member	2027 RAS Subscriber	57,600	0.0%	57,600
IT Leadership Team Plus [2] - Cross Function Team Member	2027 RAS Subscriber	35,000	0.0%	35,000
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2027 RAS Subscriber	55,200	0.0%	55,200
Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2027 RAS Subscriber	55,200	31.8%	37,647
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2027 RAS Subscriber	81,600	0.0%	81,600
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2027 RAS Subscriber	81,600	22.6%	63,159
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2027 RAS Subscriber	63,200	0.0%	63,200

Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	63,200	0.0%	63,200
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	38,500	0.0%	38,500
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2027 RAS Subscriber	22,600	0.0%	22,600
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2027 RAS Subscriber	15,800	0.0%	15,800
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2027 RAS Subscriber	68,700	0.0%	68,700
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2027 RAS Subscriber	68,700	0.0%	68,700
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2027 RAS Subscriber	42,200	0.0%	42,200
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2027 RAS Subscriber	98,300	0.0%	98,300
Technical Professionals Team [4, 5] - Additional Team Member	2027 RAS Subscriber	19,100	0.0%	19,100
Technical Professionals Advisor Department [4, 5]	2027 RAS Subscriber	204,000	0.0%	204,000
Technical Professionals Reference Department [4, 5]	2027 RAS Subscriber	137,100	0.0%	137,100
Finance Leaders Individual Access Advisor [1] - single user	2027 RAS Subscriber	71,200	0.0%	71,200
Finance Leaders Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	71,200	25.2%	53,258
Finance Leaders Team [2] - Team Leader	2027 RAS Subscriber	53,200	0.0%	53,200
Finance Leaders Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200
Finance Leaders Team [2] - Reference Member	2027 RAS Subscriber	24,900	0.0%	24,900
Chief Financial Officers Individual Access [1] - single user	2027 RAS Subscriber	173,400	0.0%	173,400
Chief Financial Officers Individual Access [1] - multi-user	2027 RAS Subscriber	173,400	9.4%	157,101
Chief Financial Officers Team [2] - Team Leader	2027 RAS Subscriber	156,900	0.0%	156,900
Chief Financial Officers Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2027 RAS Subscriber	53,200	0.0%	53,200
Chief Financial Officers Team [2] - Reference Member	2027 RAS Subscriber	24,900	0.0%	24,900
Human Resources Leaders Individual Access [1] - single user	2027 RAS Subscriber	71,200	0.0%	71,200
Human Resources Leaders Individual Access [1] - multi-user	2027 RAS Subscriber	71,200	25.2%	53,258
Human Resources Leaders Team [2] - Team Leader	2027 RAS Subscriber	53,200	0.0%	53,200
Human Resources Leaders Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200
Human Resources Leaders Team [2] - Reference Member	2027 RAS Subscriber	29,300	0.0%	29,300
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2027 RAS Subscriber	65,200	0.0%	65,200
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2027 RAS Subscriber	40,700	0.0%	40,700
Chief Human Resources Officers Individual Access [1] - single user	2027 RAS Subscriber	173,400	0.0%	173,400
Chief Human Resources Officers Individual Access [1] - multi-user	2027 RAS Subscriber	173,400	9.4%	157,101
Chief Human Resources Officers Team [2] - Team Leader	2027 RAS Subscriber	156,900	0.0%	156,900
Chief Human Resources Officers Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200

Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2027 RAS Subscriber	53,200	0.0%	53,200
Chief Human Resources Officers Team 2 - Reference Member	2027 RAS Subscriber	29,300	0.0%	29,300
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2027 RAS Subscriber	61,000	0.0%	61,000
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2027 RAS Subscriber	61,000	24.3%	46,177
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2027 RAS Subscriber	46,200	0.0%	46,200
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2027 RAS Subscriber	46,200	0.0%	46,200
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2027 RAS Subscriber	18,500	0.0%	18,500
R&D Leaders Individual Access Advisor [1] - single user	2027 RAS Subscriber	71,200	0.0%	71,200
R&D Leaders Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	71,200	25.2%	53,258
R&D Leaders Team [2] - Leader	2027 RAS Subscriber	53,200	0.0%	53,200
R&D Leaders Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200
R&D Leaders Team [2] - Reference Member	2027 RAS Subscriber	29,300	0.0%	29,300
Marketing Leaders Individual Access Advisor [1] - single user	2027 RAS Subscriber	80,800	0.0%	80,800
Marketing Leaders Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	80,800	16.7%	67,307
Marketing Leaders Team [2] - Leader	2027 RAS Subscriber	67,400	0.0%	67,400
Marketing Leaders Team [2] - Advisor Member	2027 RAS Subscriber	67,400	0.0%	67,400
Marketing Leaders Team [2] - Reference Member	2027 RAS Subscriber	26,600	0.0%	26,600
Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2027 RAS Subscriber	190,800	0.0%	190,800
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2027 RAS Subscriber	190,800	10.6%	170,576
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2027 RAS Subscriber	170,700	0.0%	170,700
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2027 RAS Subscriber	67,400	0.0%	67,400
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2027 RAS Subscriber	67,400	0.0%	67,400
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2027 RAS Subscriber	26,600	0.0%	26,600
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2027 RAS Subscriber	71,200	0.0%	71,200
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	71,200	25.2%	53,258
Customer Service & Support Leaders Team [2] - Leader	2027 RAS Subscriber	53,200	0.0%	53,200
Customer Service & Support Leaders Team [2] - Advisor Member	2027 RAS Subscriber	53,200	0.0%	53,200
Customer Service & Support Leaders Team [2] - Reference Member	2027 RAS Subscriber	23,900	0.0%	23,900

North America Gartner Conferences [7] - IT Symposium/Xpo	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Finance Conference	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - ReImagineHR Conference	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2027 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2027 Conference Ticket	TBD	0.0%	TBD
Core Connect Individual Access Reference [1]- single user	2027 RAS Subscriber	43,300	0.0%	43,300
Core Connect Individual Access Reference [1]- multi-user	2027 RAS Subscriber	43,300	43.3%	24,552
Core Connect Individual Access Advisor [1] - single user	2027 RAS Subscriber	64,900	0.0%	64,900
Core Connect Individual Access Advisor [1] - multi-user	2027 RAS Subscriber	64,900	28.5%	46,404
IT News and Insights	2027 RAS Subscriber	1,150	0.0%	1,150
News and Insights	2027 RAS Subscriber	1,150	0.0%	1,150
Internal Advisory Session ** Limited Availability **	2027 RAS Session	33,000	0.0%	33,000
Remote Advisory Services ** Limited Availability **	2027 RAS Session	14,300	0.0%	14,300
Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2027 RAS Add-on	39,100	0.0%	39,100
Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2027 RAS Add-on	39,100	0.0%	39,100
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2027 RAS Add-on	39,100	0.0%	39,100
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2027 RAS Subscriber	103,200	0.0%	103,200
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2027 RAS Subscriber	68,600	0.0%	68,600
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2027 RAS Subscriber	103,200	0.0%	103,200
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2027 RAS Subscriber	68,600	0.0%	68,600
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2027 RAS Subscriber	50,200	0.0%	50,200
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2027 RAS Subscriber	50,200	0.0%	50,200

Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2027 RAS Subscriber	100,300	0.0%	100,300
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2027 RAS Subscriber	150,100	0.0%	150,100
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2027 RAS Subscriber	200,200	0.0%	200,200
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2027 RAS Subscriber	47,100	0.0%	47,100
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2027 RAS Subscriber	53,800	0.0%	53,800
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2027 RAS Subscriber	53,800	37.8%	33,464
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2027 RAS Subscriber	79,200	0.0%	79,200
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2027 RAS Subscriber	79,200	25.8%	58,767
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2027 RAS Subscriber	58,700	0.0%	58,700
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2027 RAS Subscriber	58,700	0.0%	58,700
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2027 RAS Subscriber	34,600	0.0%	34,600
Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2027 RAS Subscriber	15,700	0.0%	15,700
Executive Programs V2 Guided Individual Access [1] - Single User	2028 RAS Subscriber	226,800	0.0%	226,800
Executive Programs V2 Guided Individual Access [1] - Multi-User	2028 RAS Subscriber	226,800	9.1%	206,162
Executive Programs V2 Self-Directed Individual Access [1] - Single User	2028 RAS Subscriber	129,400	0.0%	129,400
Executive Programs V2 Self-Directed Individual Access [1] - Multi-User	2028 RAS Subscriber	129,400	9.2%	117,496
Executive Programs V2 Guided Team [2] Guided Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CIO Guided Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CIO Guided Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CIO Self-Directed Member	2028 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Guided Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Guided Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100

Executive Programs V2 Guided Team [2] CDAO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CISO Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] Software Engineering Leaders Guided Leader Member Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Guided Team [2] Partner Member Must align to a coterminous Executive Programs V2 Guided Team Leader.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] Partner Leader Member Must align to a coterminous Executive Programs V2 Guided Team Leader. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Guided Team [2] Advisor Member	2028 RAS Subscriber	91,900	0.0%	91,900
Executive Programs V2 Guided Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	91,900	0.0%	91,900

Executive Programs V2 Guided Team [2] Cross Function Member	2028 RAS Subscriber	60,000	0.0%	60,000
Executive Programs V2 Self-Directed Team [2] Self-Directed Team Leader One Team Leader per team. Must purchase a coterminous Executive Programs V2 Team Member listed below.	2028 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Member	2028 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Self-Directed Team [2] CIO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	117,600	0.0%	117,600
Executive Programs V2 Self-Directed Team [2] CDAO Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] CDAO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] CISO Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] CISO Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Guided Leader Member Other role-based domains may be available; check with account representative. Leader Member must purchase a coterminous Executive Programs V2 Extended Team Guided Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	206,100	0.0%	206,100
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Self-Directed Team [2] CDAO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Self-Directed Team [2] CISO Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Member Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900

Executive Programs V2 Self-Directed Team [2] Software Engineering Leaders Self-Directed Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Self-Directed Team Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	105,900	0.0%	105,900
Executive Programs V2 Self-Directed Team [2] Advisor Member	2028 RAS Subscriber	91,900	0.0%	91,900
Executive Programs V2 Self-Directed Team [2] Advisor Leader Member Must purchase a coterminous Executive Programs V2 Extended Team Advisor or Cross Function Member.	2028 RAS Subscriber	91,900	0.0%	91,900
Executive Programs V2 Self-Directed Team [2] Cross Function Member	2028 RAS Subscriber	60,000	0.0%	60,000
Executive Programs V2 Extended Team [2] Guided CDAO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	78,500	0.0%	78,500
Executive Programs V2 Extended Team [2] Guided CISO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	78,500	0.0%	78,500
Executive Programs V2 Extended Team [2] Guided Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	78,500	0.0%	78,500
Executive Programs V2 Extended Team [2] Self-Directed CDAO Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	69,900	0.0%	69,900
Executive Programs V2 Extended Team [2] Self-Directed CISO Team Member Must align to a coterminous Executive Programs V2 Team Guided Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	69,900	0.0%	69,900
Executive Programs V2 Extended Team [2] Self-Directed Software Engineering Leaders Team Member Must align to a coterminous Executive Programs V2 Team Self-Directed Leader Member of the same role-based domain. Other role-based domains may be available; check with account representative.	2028 RAS Subscriber	69,900	0.0%	69,900
Executive Programs V2 Extended Team [2] Advisor Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2028 RAS Subscriber	91,900	0.0%	91,900
Executive Programs V2 Extended Team [2] Cross Function Member Must align to a coterminous Executive Programs V2 Team CIO Leader Member, Partner Leader Member, or Advisor Leader Member.	2028 RAS Subscriber	60,000	0.0%	60,000
Gartner for CIOs Individual Access [1] - single user	2028 RAS Subscriber	117,900	0.0%	117,900
Gartner for CIOs Individual Access [1] - multi-user	2028 RAS Subscriber	117,900	9.0%	107,289
Gartner for CIOs Team Plus [2] - Team Leader	2028 RAS Subscriber	107,300	0.0%	107,300
Gartner for CIOs Team Plus [2] - Advisor Team Member	2028 RAS Subscriber	78,400	0.0%	78,400
Gartner for CIOs Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2028 RAS Subscriber	78,400	0.0%	78,400
Gartner for CIOs Team Plus [2] - Cross Function Team Member	2028 RAS Subscriber	54,500	0.0%	54,500
Gartner for CIOs with Industry Individual Access [1] (one industry) - single user	2028 RAS Subscriber	129,400	0.0%	129,400

Gartner for CIOs with Industry Individual Access [1] (one industry) - multi-user	2028 RAS Subscriber	129,400	9.2%	117,496
Gartner for CIOs Team Plus with Industry [2] (one industry) - Team Leader	2028 RAS Subscriber	117,600	0.0%	117,600
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	91,900	0.0%	91,900
Gartner for CIOs Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2028 RAS Subscriber	91,900	0.0%	91,900
Gartner for CIOs Team Plus with Industry [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	60,000	0.0%	60,000
Executive Programs Member Individual Access [1] - single user	2028 RAS Subscriber	192,300	0.0%	192,300
Executive Programs Member Individual Access [1] - multi-user user	2028 RAS Subscriber	192,300	11.0%	171,147
Executive Programs Leadership Team [2] - Team Leader	2028 RAS Subscriber	174,200	0.0%	174,200
Executive Programs Leadership Team [2] - IT Executive Team Member	2028 RAS Subscriber	174,200	0.0%	174,200
Executive Programs Leadership Team [2] - IT Executive Team Leader (must purchase IT Leadership Team Members)	2028 RAS Subscriber	174,200	0.0%	174,200
Executive Programs Leadership Team [2] - Partner Team Member ** Invitation Only **	2028 RAS Subscriber	159,300	0.0%	159,300
Executive Programs Leadership Team [2] - Partner Team Leader ** Invitation Only ** (Partner Team Leader must purchase Enterprise IT Leadership Team Members)	2028 RAS Subscriber	159,300	0.0%	159,300
Executive Programs Leadership Team [2] - Delegate Team Member ** Renewal Only [6] **	2028 RAS Subscriber	93,200	0.0%	93,200
Executive Programs Leadership Team [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Members)	2028 RAS Subscriber	93,200	0.0%	93,200
Executive Programs Leadership Team [2] - Advisor Team Member	2028 RAS Subscriber	63,600	0.0%	63,600
Executive Programs Leadership Team [2] - Advisor Team Leader (Advisor Team Leader must purchase IT Leadership Team Members)	2028 RAS Subscriber	63,600	0.0%	63,600
Executive Programs Leadership Team [2] - Cross Function Team Member	2028 RAS Subscriber	46,200	0.0%	46,200
Executive Programs Leadership Team [2] - Role Team Member	2028 RAS Subscriber	33,300	0.0%	33,300
Executive Programs Leadership Team Plus [2] - Team Leader	2028 RAS Subscriber	189,900	0.0%	189,900
Executive Programs Leadership Team Plus 2 - Team Leader ** Renewal Only [6] ** Renewing subscriber license purchased before 01-Feb-2022 with continuous renewal.	2028 RAS Subscriber	189,900	8.1%	174,519
Executive Programs Leadership Team Plus [2] - IT Executive Team Member	2028 RAS Subscriber	189,900	0.0%	189,900
Executive Programs Leadership Team Plus [2] - IT Executive Team Leader (IT Executive Team Leader must purchase IT Leadership Team Plus Members)	2028 RAS Subscriber	189,900	0.0%	189,900
Executive Programs Leadership Team Plus [2] - Partner Team Member ** Invitation Only **	2028 RAS Subscriber	173,800	0.0%	173,800
Executive Programs Leadership Team Plus 2 - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus Members)	2028 RAS Subscriber	173,800	0.0%	173,800
Executive Programs Leadership Team Plus [2] - Delegate Team Member ** Renewal Only [6] **	2028 RAS Subscriber	101,700	0.0%	101,700
Executive Programs Leadership Team Plus [2] - Delegate Team Leader ** Renewal Only [6] ** (must purchase IT Leadership Team Plus Members)	2028 RAS Subscriber	101,700	0.0%	101,700

Executive Programs Leadership Team Plus [2] - Delegate Team Member or Delegate Team Leader ** Renewal Only [6] ** Renewing g subscriber license purchased before 01-Feb-2022 with continuous renewal.	2028 RAS Subscriber	101,700	8.3%	93,259
Executive Programs Leadership Team Plus [2] - Advisor Team Member	2028 RAS Subscriber	69,600	0.0%	69,600
Executive Programs Leadership Team Plus [2] - Advisor Team Leader (must purchase IT Leadership Team Plus Members)	2028 RAS Subscriber	69,600	0.0%	69,600
Executive Programs Leadership Team Plus [2] - Cross Function Team Member	2028 RAS Subscriber	50,400	0.0%	50,400
Executive Programs Member with Industry Individual Access [1] (one industry) - single user	2028 RAS Subscriber	207,000	0.0%	207,000
Executive Programs Member with Industry Individual Access [1] (one industry) - multi-user	2028 RAS Subscriber	207,000	10.2%	185,886
Executive Programs Leadership Team with Industry [2] (one industry) - Team Leader	2028 RAS Subscriber	189,700	0.0%	189,700
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Member	2028 RAS Subscriber	189,700	0.0%	189,700
Executive Programs Leadership Team with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2028 RAS Subscriber	189,700	0.0%	189,700
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2028 RAS Subscriber	176,400	0.0%	176,400
Executive Programs Leadership Team with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team with Industry Members)	2028 RAS Subscriber	176,400	0.0%	176,400
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2028 RAS Subscriber	105,500	0.0%	105,500
Executive Programs Leadership Team with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Members)	2028 RAS Subscriber	105,500	0.0%	105,500
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	76,800	0.0%	76,800
Executive Programs Leadership Team with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Members)	2028 RAS Subscriber	76,800	0.0%	76,800
Executive Programs Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	51,300	0.0%	51,300
Executive Programs Leadership Team with Industry [2] (one industry) - Role Team Member	2028 RAS Subscriber	37,200	0.0%	37,200
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Team Leader	2028 RAS Subscriber	206,800	0.0%	206,800

Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Member	2028 RAS Subscriber	206,800	0.0%	206,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - IT Executive Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2028 RAS Subscriber	206,800	0.0%	206,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Member ** Invitation Only **	2028 RAS Subscriber	192,700	0.0%	192,700
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Partner Team Leader ** Invitation Only ** (must purchase Enterprise IT Leadership Team Plus with Industry Members)	2028 RAS Subscriber	192,700	0.0%	192,700
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Member ** Renewal Only [6] **	2028 RAS Subscriber	114,800	0.0%	114,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Delegate Team Leader ** Renewal Only [6] ** (must purchase Industry Advisory Services Leadership Team Plus Members)	2028 RAS Subscriber	114,800	0.0%	114,800
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	83,300	0.0%	83,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Advisor Team Leader (must purchase Industry Advisory Services Leadership Team Plus Members)	2028 RAS Subscriber	83,300	0.0%	83,300
Executive Programs Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	55,600	0.0%	55,600
Gartner for CDAOs Individual Access [1] - single user	2028 RAS Subscriber	116,200	0.0%	116,200
Gartner for CDAOs Individual Access [1] - multi-user	2028 RAS Subscriber	116,200	9.0%	105,742
Gartner for CDAOs Team [2] - Team Leader	2028 RAS Subscriber	105,900	0.0%	105,900
Gartner for CDAOs Team [2] - Team Member	2028 RAS Subscriber	69,900	0.0%	69,900
Gartner for CDAOs Team [2] - Tech Professional Team Member	2028 RAS Subscriber	26,700	0.0%	26,700
Gartner for CDAOs Executive Individual Access [1] - single user	2028 RAS Subscriber	226,800	0.0%	226,800
Gartner for CDAOs Executive Individual Access [1] - multi-user	2028 RAS Subscriber	226,800	9.1%	206,162
Gartner for CDAOs Executive Team [2] - Team Leader	2028 RAS Subscriber	206,100	0.0%	206,100
Gartner for CDAOs Executive Team [2] - Team Member	2028 RAS Subscriber	78,500	0.0%	78,500
Gartner for CDAOs Executive Team [2] - Tech Professional Team Member	2028 RAS Subscriber	30,600	0.0%	30,600
Gartner for CISOs Individual Access [1] - single user	2028 RAS Subscriber	116,200	0.0%	116,200
Gartner for CISOs Individual Access [1] - multi-user	2028 RAS Subscriber	116,200	9.0%	105,742
Gartner for CISOs Team [2] - Team Leader	2028 RAS Subscriber	105,900	0.0%	105,900
Gartner for CISOs Team [2] - Team Member	2028 RAS Subscriber	69,900	0.0%	69,900
Gartner for CISOs Team [2] - Tech Professional Team Member	2028 RAS Subscriber	26,700	0.0%	26,700
Gartner for CISOs Executive Individual Access [1] - single user	2028 RAS Subscriber	226,800	0.0%	226,800

Gartner for CISOs Executive Individual Access [1] - multi-user	2028 RAS Subscriber	226,800	9.1%	206,162
Gartner for CISOs Executive Team [2] - Team Leader	2028 RAS Subscriber	206,100	0.0%	206,100
Gartner for CISOs Executive Team [2] - Team Member	2028 RAS Subscriber	78,500	0.0%	78,500
Gartner for CISOs Executive Team [2] - Tech Professional Team Member	2028 RAS Subscriber	30,600	0.0%	30,600
Gartner for Software Engineering Leaders Individual Access [1] - single user	2028 RAS Subscriber	116,200	0.0%	116,200
Gartner for Software Engineering Leaders Individual Access [1] - multi-user	2028 RAS Subscriber	116,200	9.0%	105,742
Gartner for Software Engineering Leaders Team [2] - Team Leader	2028 RAS Subscriber	105,900	0.0%	105,900
Gartner for Software Engineering Leaders Team [2] - Team Member	2028 RAS Subscriber	69,900	0.0%	69,900
Gartner for Software Engineering Leaders Team [2] - Tech Professional Team Member	2028 RAS Subscriber	26,700	0.0%	26,700
Gartner for Software Engineering Leaders Executive Individual Access [1] - single user	2028 RAS Subscriber	226,800	0.0%	226,800
Gartner for Software Engineering Leaders Executive Individual Access [1] - multi-user	2028 RAS Subscriber	226,800	9.1%	206,162
Gartner for Software Engineering Leaders Executive Team [2] - Team Leader	2028 RAS Subscriber	206,100	0.0%	206,100
Gartner for Software Engineering Leaders Executive Team [2] - Team Member	2028 RAS Subscriber	78,500	0.0%	78,500
Gartner for Software Engineering Leaders Executive Team [2] - Tech Professional Team Member	2028 RAS Subscriber	30,600	0.0%	30,600
Enterprise IT Leadership Team [2] - Team Leader ** Invitation Only **	2028 RAS Subscriber	147,600	0.0%	147,600
Enterprise IT Leadership Team [2] - Advisor Team Member	2028 RAS Subscriber	58,600	0.0%	58,600
Enterprise IT Leadership Team [2] - Cross Function Team Member	2028 RAS Subscriber	35,700	0.0%	35,700
Enterprise IT Leadership Team [2] - Role Team Member	2028 RAS Subscriber	22,500	0.0%	22,500
Enterprise IT Leadership Team [2] - Essentials Team Member	2028 RAS Subscriber	17,400	0.0%	17,400
Enterprise IT Leadership Team Plus [2] - Team Leader ** Invitation Only **	2028 RAS Subscriber	160,400	0.0%	160,400
Enterprise IT Leadership Team Plus [2] - Advisor Team Member	2028 RAS Subscriber	63,400	0.0%	63,400
Enterprise IT Leadership Team Plus [2] - Cross Function Team Member	2028 RAS Subscriber	38,500	0.0%	38,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Team Leader ** Invitation Only **	2028 RAS Subscriber	164,500	0.0%	164,500
Enterprise IT Leadership Team with Industry [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	69,600	0.0%	69,600
Enterprise IT Leadership Team with Industry [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	42,400	0.0%	42,400
Enterprise IT Leadership Team with Industry [2] (one industry) - Role Team Member	2028 RAS Subscriber	24,900	0.0%	24,900
Enterprise IT Leadership Team with Industry [2] (one industry) - Essentials Team Member	2028 RAS Subscriber	17,400	0.0%	17,400
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Team Leader ** Invitation Only **	2028 RAS Subscriber	179,600	0.0%	179,600
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	75,600	0.0%	75,600
Enterprise IT Leadership Team Plus with Industry [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	46,500	0.0%	46,500

IT Leader Individual Access Reference [1] - single user	2028 RAS Subscriber	55,300	0.0%	55,300
IT Leader Individual Access Reference [1] - multi-user	2028 RAS Subscriber	55,300	37.6%	34,508
IT Leader Individual Access Advisor [1] - single user	2028 RAS Subscriber	79,000	0.0%	79,000
IT Leader Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	79,000	25.8%	58,618
IT Leadership Team [2] - Team Leader	2028 RAS Subscriber	58,600	0.0%	58,600
IT Leadership Team [2] - Advisor Team Member	2028 RAS Subscriber	58,600	0.0%	58,600
IT Leadership Team [2] - Cross Function Team Member	2028 RAS Subscriber	35,700	0.0%	35,700
IT Leadership Team [2] - Role Team Member	2028 RAS Subscriber	22,500	0.0%	22,500
IT Leadership Team [2] - Essentials Team Member	2028 RAS Subscriber	17,400	0.0%	17,400
IT Leadership Team Plus [2] - Team Leader	2028 RAS Subscriber	63,400	0.0%	63,400
IT Leadership Team Plus [2] - Advisor Team Member	2028 RAS Subscriber	63,400	0.0%	63,400
IT Leadership Team Plus [2] - Cross Function Team Member	2028 RAS Subscriber	38,500	0.0%	38,500
Industry Advisory Services Individual Access Reference [1] (one industry) - single user	2028 RAS Subscriber	60,800	0.0%	60,800
Industry Advisory Services Individual Access Reference [1] (one industry) - multi-user	2028 RAS Subscriber	60,800	31.8%	41,466
Industry Advisory Services Individual Access Advisor [1] (one industry) - single user	2028 RAS Subscriber	89,800	0.0%	89,800
Industry Advisory Services Individual Access Advisor [1] (one industry) - multi-user	2028 RAS Subscriber	89,800	22.6%	69,506
Industry Advisory Services Leadership Team [2] (one industry) - Team Leader	2028 RAS Subscriber	69,600	0.0%	69,600
Industry Advisory Services Leadership Team [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	69,600	0.0%	69,600
Industry Advisory Services Leadership Team [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	42,400	0.0%	42,400
Industry Advisory Services Leadership Team [2] (one industry) - Role Team Member	2028 RAS Subscriber	24,900	0.0%	24,900
Industry Advisory Services Leadership Team [2] (one industry) - Essentials Team Member	2028 RAS Subscriber	17,400	0.0%	17,400
Industry Advisory Services Leadership Team Plus [2] (one industry) - Team Leader	2028 RAS Subscriber	75,600	0.0%	75,600
Industry Advisory Services Leadership Team Plus [2] (one industry) - Advisor Team Member	2028 RAS Subscriber	75,600	0.0%	75,600
Industry Advisory Services Leadership Team Plus [2] (one industry) - Cross Function Team Member	2028 RAS Subscriber	46,500	0.0%	46,500
Technical Professionals Team [4, 5] Includes 1 Team Leader and up to 4 Team Member	2028 RAS Subscriber	108,200	0.0%	108,200
Technical Professionals Team [4, 5] - Additional Team Member	2028 RAS Subscriber	21,100	0.0%	21,100
Technical Professionals Advisor Department [4, 5]	2028 RAS Subscriber	224,400	0.0%	224,400
Technical Professionals Reference Department [4, 5]	2028 RAS Subscriber	150,900	0.0%	150,900
Finance Leaders Individual Access Advisor [1] - single user	2028 RAS Subscriber	78,400	0.0%	78,400
Finance Leaders Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	78,400	25.2%	58,644
Finance Leaders Team [2] - Team Leader	2028 RAS Subscriber	58,600	0.0%	58,600
Finance Leaders Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
Finance Leaders Team [2] - Reference Member	2028 RAS Subscriber	27,400	0.0%	27,400
Chief Financial Officers Individual Access [1] - single user	2028 RAS Subscriber	190,800	0.0%	190,800

Chief Financial Officers Individual Access [1] - multi-user	2028 RAS Subscriber	190,800	9.4%	172,865
Chief Financial Officers Team [2] - Team Leader	2028 RAS Subscriber	172,600	0.0%	172,600
Chief Financial Officers Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
Chief Financial Officers Team [2] - Advisor Leader (must purchase coterminous Finance Leader Team Members)	2028 RAS Subscriber	58,600	0.0%	58,600
Chief Financial Officers Team [2] - Reference Member	2028 RAS Subscriber	27,400	0.0%	27,400
Human Resources Leaders Individual Access [1] - single user	2028 RAS Subscriber	78,400	0.0%	78,400
Human Resources Leaders Individual Access [1] - multi-user	2028 RAS Subscriber	78,400	25.2%	58,644
Human Resources Leaders Team [2] - Team Leader	2028 RAS Subscriber	58,600	0.0%	58,600
Human Resources Leaders Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
Human Resources Leaders Team [2] - Reference Member	2028 RAS Subscriber	32,300	0.0%	32,300
Human Resources Professionals Reference [4] - Up to 20 HR Professionals	2028 RAS Subscriber	71,800	0.0%	71,800
Human Resources Professionals Reference [4] - Up to 5 HR Professionals	2028 RAS Subscriber	44,800	0.0%	44,800
Chief Human Resources Officers Individual Access [1] - single user	2028 RAS Subscriber	190,800	0.0%	190,800
Chief Human Resources Officers Individual Access [1] - multi-user	2028 RAS Subscriber	190,800	9.4%	172,865
Chief Human Resources Officers Team [2] - Team Leader	2028 RAS Subscriber	172,600	0.0%	172,600
Chief Human Resources Officers Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
Chief Human Resources Officers Team [2] - Advisor Leader (must purchase coterminous Human Resources Leaders Team Members)	2028 RAS Subscriber	58,600	0.0%	58,600
Chief Human Resources Officers Team 2 - Reference Member	2028 RAS Subscriber	32,300	0.0%	32,300
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - single user	2028 RAS Subscriber	67,100	0.0%	67,100
Legal, Risk & Compliance Leaders Individual Access or Legal, Risk & Compliance Leaders for Audit & Risk Individual Access [1] - multi-user	2028 RAS Subscriber	67,100	24.3%	50,795
Legal, Risk & Compliance Leaders Team - Leader or Legal, Risk & Compliance Leaders Team for Audit & Risk - Leader [2]	2028 RAS Subscriber	50,900	0.0%	50,900
Legal, Risk & Compliance Leaders Team- Advisor Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Advisor Member [2]	2028 RAS Subscriber	50,900	0.0%	50,900
Legal, Risk & Compliance Leaders Team- Reference Member or Legal, Risk & Compliance Leaders Team for Audit & Risk- Reference Member [2]	2028 RAS Subscriber	20,400	0.0%	20,400
R&D Leaders Individual Access Advisor [1] - single user	2028 RAS Subscriber	78,400	0.0%	78,400
R&D Leaders Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	78,400	25.2%	58,644
R&D Leaders Team [2] - Leader	2028 RAS Subscriber	58,600	0.0%	58,600
R&D Leaders Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
R&D Leaders Team [2] - Reference Member	2028 RAS Subscriber	32,300	0.0%	32,300
Marketing Leaders Individual Access Advisor [1] - single user	2028 RAS Subscriber	88,900	0.0%	88,900
Marketing Leaders Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	88,900	16.7%	74,054
Marketing Leaders Team [2] - Leader	2028 RAS Subscriber	74,200	0.0%	74,200
Marketing Leaders Team [2] - Advisor Member	2028 RAS Subscriber	74,200	0.0%	74,200
Marketing Leaders Team [2] - Reference Member	2028 RAS Subscriber	29,300	0.0%	29,300

Gartner for Chief Marketing Executives Individual Access [1] - single user ** Invitation Only **	2028 RAS Subscriber	209,900	0.0%	209,900
Gartner for Chief Marketing Executives Individual Access [1] - multi-user ** Invitation Only **	2028 RAS Subscriber	209,900	10.6%	187,651
Gartner for Chief Marketing Executives Team [2] - Team Leader ** Invitation Only **	2028 RAS Subscriber	187,800	0.0%	187,800
Gartner for Chief Marketing Executives Team [2] - Advisor Team Member ** Invitation Only **	2028 RAS Subscriber	74,200	0.0%	74,200
Gartner for Chief Marketing Executives Team [2] - Advisor Team Leader ** Invitation Only ** (must purchase Marketing Leaders Team Members)	2028 RAS Subscriber	74,200	0.0%	74,200
Gartner for Chief Marketing Executives Team [2] - Reference Team Member ** Invitation Only **	2028 RAS Subscriber	29,300	0.0%	29,300
Customer Service & Support Leaders Individual Access Advisor [1] - single user	2028 RAS Subscriber	78,400	0.0%	78,400
Customer Service & Support Leaders Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	78,400	25.2%	58,644
Customer Service & Support Leaders Team [2] - Leader	2028 RAS Subscriber	58,600	0.0%	58,600
Customer Service & Support Leaders Team [2] - Advisor Member	2028 RAS Subscriber	58,600	0.0%	58,600
Customer Service & Support Leaders Team [2] - Reference Member	2028 RAS Subscriber	26,300	0.0%	26,300
North America Gartner Conferences [7] - IT Symposium/Xpo	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (BI, Data Center, Security, or Apps)	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Summit (excludes BI, Data Center, Security, and Apps)	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Finance Conference	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - ReImagineHR Conference	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Marketing Symposium/Xpo	2028 Conference Ticket	TBD	0.0%	TBD
North America Gartner Conferences [7] - Supply Chain Symposium/Xpo	2028 Conference Ticket	TBD	0.0%	TBD
Core Connect Individual Access Reference [1]- single user	2028 RAS Subscriber	47,700	0.0%	47,700
Core Connect Individual Access Reference [1]- multi-user	2028 RAS Subscriber	47,700	43.3%	27,046
Core Connect Individual Access Advisor [1] - single user	2028 RAS Subscriber	71,400	0.0%	71,400
Core Connect Individual Access Advisor [1] - multi-user	2028 RAS Subscriber	71,400	28.5%	51,051
IT News and Insights	2028 RAS Subscriber	1,270	0.0%	1,270
News and Insights	2028 RAS Subscriber	1,270	0.0%	1,270
Internal Advisory Session ** Limited Availability **	2028 RAS Session	36,300	0.0%	36,300
Remote Advisory Services ** Limited Availability **	2028 RAS Session	15,800	0.0%	15,800
Executive Programs - Two Additional Meetings Add-on [3] ** Limited Availability **	2028 RAS Add-on	43,100	0.0%	43,100

Enterprise IT Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2028 RAS Add-on	43,100	0.0%	43,100
Enterprise Supply Chain Leaders - Two Additional Meetings Add-on [3] ** Limited Availability **	2028 RAS Add-on	43,100	0.0%	43,100
Technical Professionals Small & Midsize Business (SMB) Advisor SMB [3, 4] ** Limited Availability **	2028 RAS Subscriber	113,600	0.0%	113,600
Technical Professionals Small & Midsize Business (SMB) Reference SMB [3, 4] ** Limited Availability **	2028 RAS Subscriber	75,500	0.0%	75,500
Technical Professionals for Higher Education Advisor [3, 4, 8] ** Limited Availability **	2028 RAS Subscriber	113,600	0.0%	113,600
Technical Professionals for Higher Education Reference [3, 4, 8] ** Limited Availability **	2028 RAS Subscriber	75,500	0.0%	75,500
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a community college	2028 RAS Subscriber	55,300	0.0%	55,300
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 1 to 4,999 Student FTE	2028 RAS Subscriber	55,300	0.0%	55,300
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 5,000 to 9,999 Student FTE	2028 RAS Subscriber	110,400	0.0%	110,400
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 10,000 to 24,999 Student FTE	2028 RAS Subscriber	165,200	0.0%	165,200
Core Reference for Higher Education Campus [3, 8] ** Limited Availability ** - for a college or university with 25,000+ Student FTE	2028 RAS Subscriber	220,300	0.0%	220,300
Gartner for IT Associates 100 Research Notes [3, 4] ** Limited Availability **	2028 RAS Subscriber	51,900	0.0%	51,900
Supply Chain Leaders Reference [1] - single user ** Limited Availability **	2028 RAS Subscriber	59,200	0.0%	59,200
Supply Chain Leaders Reference [1] - multi-user ** Limited Availability **	2028 RAS Subscriber	59,200	37.8%	36,823
Supply Chain Leaders Individual Access Advisor [1] - single user ** Limited Availability **	2028 RAS Subscriber	87,200	0.0%	87,200
Supply Chain Leaders Individual Access Advisor [1] - multi-user ** Limited Availability **	2028 RAS Subscriber	87,200	25.8%	64,703
Supply Chain Leaders Team [2] - Team Leader ** Limited Availability **	2028 RAS Subscriber	64,600	0.0%	64,600
Supply Chain Leaders Team [2] - Advisor Team Member ** Limited Availability **	2028 RAS Subscriber	64,600	0.0%	64,600
Supply Chain Leaders Team [2] - Cross Function Team Member ** Limited Availability **	2028 RAS Subscriber	38,100	0.0%	38,100
Supply Chain Leaders Team [2] - Essentials Team Member ** Limited Availability **	2028 RAS Subscriber	17,300	0.0%	17,300

Confidential - For evaluation purposes.

The Oklahoma Prices herein are detailed in "Pricing Exhibit 1 – Gartner Research and Advisory Services" in a concise user-friendly format for ease of document review and incorporation into the final contract award agreement.

Services/Subscription/License	Unit of Measure	List Price	% off List Price	Oklahoma Price
Project Executive	2023 Hourly Rate	696.30	0.0%	696.30
Quality Assurance Specialist	2023 Hourly Rate	661.10	0.0%	661.10
Senior Subject Matter Expert	2023 Hourly Rate	646.80	0.0%	646.80
Program Director	2023 Hourly Rate	600.60	0.0%	600.60
Technical Architect	2023 Hourly Rate	550.00	0.0%	550.00
Subject Matter Expert	2023 Hourly Rate	550.00	0.0%	550.00
Engagement Manager	2023 Hourly Rate	550.00	0.0%	550.00
Senior Business Analyst	2023 Hourly Rate	462.00	0.0%	462.00
Senior Technical Analyst	2023 Hourly Rate	462.00	0.0%	462.00
Project Manager	2023 Hourly Rate	462.00	0.0%	462.00
Senior Delivery Consultant	2023 Hourly Rate	382.80	0.0%	382.80
Business Analyst	2023 Hourly Rate	297.00	0.0%	297.00
Technical Analyst	2023 Hourly Rate	297.00	0.0%	297.00
Delivery Consultant	2023 Hourly Rate	297.00	0.0%	297.00
Analyst	2023 Hourly Rate	249.70	0.0%	249.70
Project Executive	2024 Hourly Rate	724.15	0.0%	724.15
Quality Assurance Specialist	2024 Hourly Rate	687.54	0.0%	687.54
Senior Subject Matter Expert	2024 Hourly Rate	672.67	0.0%	672.67
Program Director	2024 Hourly Rate	624.62	0.0%	624.62
Technical Architect	2024 Hourly Rate	572.00	0.0%	572.00
Subject Matter Expert	2024 Hourly Rate	572.00	0.0%	572.00
Engagement Manager	2024 Hourly Rate	572.00	0.0%	572.00
Senior Business Analyst	2024 Hourly Rate	480.48	0.0%	480.48
Senior Technical Analyst	2024 Hourly Rate	480.48	0.0%	480.48
Project Manager	2024 Hourly Rate	480.48	0.0%	480.48
Senior Delivery Consultant	2024 Hourly Rate	398.11	0.0%	398.11
Business Analyst	2024 Hourly Rate	308.88	0.0%	308.88
Technical Analyst	2024 Hourly Rate	308.88	0.0%	308.88
Delivery Consultant	2024 Hourly Rate	308.88	0.0%	308.88
Analyst	2024 Hourly Rate	259.69	0.0%	259.69
Project Executive	2025 Hourly Rate	753.12	0.0%	753.12
Quality Assurance Specialist	2025 Hourly Rate	715.05	0.0%	715.05
Senior Subject Matter Expert	2025 Hourly Rate	699.58	0.0%	699.58
Program Director	2025 Hourly Rate	649.61	0.0%	649.61
Technical Architect	2025 Hourly Rate	594.88	0.0%	594.88
Subject Matter Expert	2025 Hourly Rate	594.88	0.0%	594.88
Engagement Manager	2025 Hourly Rate	594.88	0.0%	594.88
Senior Business Analyst	2025 Hourly Rate	499.70	0.0%	499.70
Senior Technical Analyst	2025 Hourly Rate	499.70	0.0%	499.70
Project Manager	2025 Hourly Rate	499.70	0.0%	499.70
Senior Delivery Consultant	2025 Hourly Rate	414.04	0.0%	414.04
Business Analyst	2025 Hourly Rate	321.24	0.0%	321.24
Technical Analyst	2025 Hourly Rate	321.24	0.0%	321.24
Delivery Consultant	2025 Hourly Rate	321.24	0.0%	321.24
Analyst	2025 Hourly Rate	270.08	0.0%	270.08
Project Executive	2026 Hourly Rate	783.24	0.0%	783.24
Quality Assurance Specialist	2026 Hourly Rate	743.65	0.0%	743.65
Senior Subject Matter Expert	2026 Hourly Rate	727.56	0.0%	727.56
Program Director	2026 Hourly Rate	675.59	0.0%	675.59
Technical Architect	2026 Hourly Rate	618.68	0.0%	618.68
Subject Matter Expert	2026 Hourly Rate	618.68	0.0%	618.68
Engagement Manager	2026 Hourly Rate	618.68	0.0%	618.68
Senior Business Analyst	2026 Hourly Rate	519.69	0.0%	519.69
Senior Technical Analyst	2026 Hourly Rate	519.69	0.0%	519.69
Project Manager	2026 Hourly Rate	519.69	0.0%	519.69
Senior Delivery Consultant	2026 Hourly Rate	430.60	0.0%	430.60
Business Analyst	2026 Hourly Rate	334.08	0.0%	334.08
Technical Analyst	2026 Hourly Rate	334.08	0.0%	334.08
Delivery Consultant	2026 Hourly Rate	334.08	0.0%	334.08
Analyst	2026 Hourly Rate	280.88	0.0%	280.88
Project Executive	2027 Hourly Rate	814.57	0.0%	814.57
Quality Assurance Specialist	2027 Hourly Rate	773.39	0.0%	773.39
Senior Subject Matter Expert	2027 Hourly Rate	756.66	0.0%	756.66
Program Director	2027 Hourly Rate	702.62	0.0%	702.62
Technical Architect	2027 Hourly Rate	643.42	0.0%	643.42
Subject Matter Expert	2027 Hourly Rate	643.42	0.0%	643.42
Engagement Manager	2027 Hourly Rate	643.42	0.0%	643.42

Senior Business Analyst	2027 Hourly Rate	540.47	0.0%	540.47
Senior Technical Analyst	2027 Hourly Rate	540.47	0.0%	540.47
Project Manager	2027 Hourly Rate	540.47	0.0%	540.47
Senior Delivery Consultant	2027 Hourly Rate	447.82	0.0%	447.82
Business Analyst	2027 Hourly Rate	347.45	0.0%	347.45
Technical Analyst	2027 Hourly Rate	347.45	0.0%	347.45
Delivery Consultant	2027 Hourly Rate	347.45	0.0%	347.45
Analyst	2027 Hourly Rate	292.11	0.0%	292.11
Project Executive	2028 Hourly Rate	847.16	0.0%	847.16
Quality Assurance Specialist	2028 Hourly Rate	804.33	0.0%	804.33
Senior Subject Matter Expert	2028 Hourly Rate	786.93	0.0%	786.93
Program Director	2028 Hourly Rate	730.72	0.0%	730.72
Technical Architect	2028 Hourly Rate	669.16	0.0%	669.16
Subject Matter Expert	2028 Hourly Rate	669.16	0.0%	669.16
Engagement Manager	2028 Hourly Rate	669.16	0.0%	669.16
Senior Business Analyst	2028 Hourly Rate	562.09	0.0%	562.09
Senior Technical Analyst	2028 Hourly Rate	562.09	0.0%	562.09
Project Manager	2028 Hourly Rate	562.09	0.0%	562.09
Senior Delivery Consultant	2028 Hourly Rate	465.73	0.0%	465.73
Business Analyst	2028 Hourly Rate	361.35	0.0%	361.35
Technical Analyst	2028 Hourly Rate	361.35	0.0%	361.35
Delivery Consultant	2028 Hourly Rate	361.35	0.0%	361.35
Analyst	2028 Hourly Rate	303.80	0.0%	303.80

Pricing Notes

Work to be performed is on a fixed-fee basis. The total cost set forth in an order shall be a fixed price for all the required services and work products. The Gartner team is fully committed to delivering the proposed scope of work described in a given task order proposal using the fixed priced deliverables-based model. The estimated hours provided in a proposal are for estimation purposes only to derive our proposed fixed price. As with all fixed priced deliverables-based engagements, the actual number of hours to perform the work will vary and the estimated hours proposed may not reflect the actual required hours. Moreover, Gartner anticipates leveraging other labor categories as needed to deliver exceptional service in the most efficient manner. Similarly, Gartner may need to move hours/level of effort across personnel and labor categories to enable efficient and high value service delivery — provided the total firm fixed price is not exceeded. Given Gartner will only perform fixed price orders, and not time-and-materials orders, we will not be providing any information regarding actual hours expended and/or labor rates of actual resources utilized to complete the work.

ATTACHMENT E4

VALUE ADD TERMS

Gartner Buy Smart

Gartner BuySmart is available at no additional cost with many of our research license products. Acquiring technology is often a long and complicated process that can lead to purchase dissatisfaction, even when decisions are made by the most talented and informed procurement teams. Balancing opinions and inputs from members of buying groups, bringing stakeholders together to make evaluation decisions and making informed trade-offs between vendors are all obstacles to purchase satisfaction.

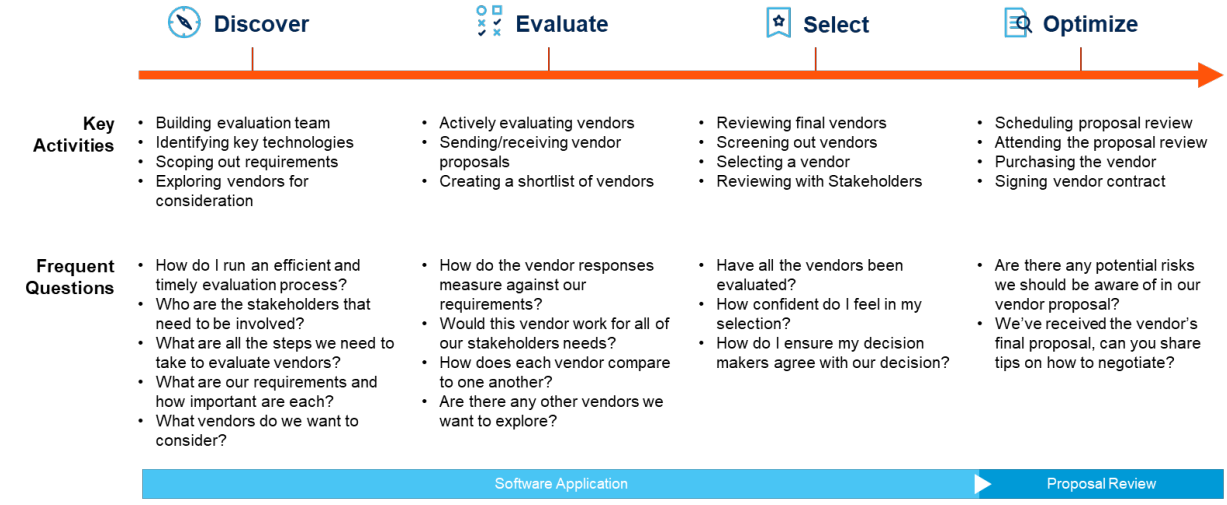
BuySmart embeds Gartner insights and research directly into the evaluation process to help navigate purchasing intricacies and avoid buyer's remorse.

The **Gartner BuySmart** application can help the State confidently manage the technology acquisition life cycle by streamlining the path to better technology purchasing decisions. This proprietary tool is fueled by both the expertise of over 2,200 Gartner research experts and the perspectives of peer organizations that have made similar acquisitions.

Gartner is offering a live BuySmart demo on Gartner.com on 21 June 2023, hosted by Gartner analysts Sarah Alread, Austin Jordan and Kailin Mariot.

BuySmart uses these insights to accelerate and optimize the State's activities through each step of a technology purchase. BuySmart combines the power of curated research, peer and expert insights and intuitive workflow processes to help State license holders make informed decisions and acquire technology that delivers results for the organization's mission-critical priorities. The application is designed to help the State optimize costs, save time and select the right vendor with confidence.

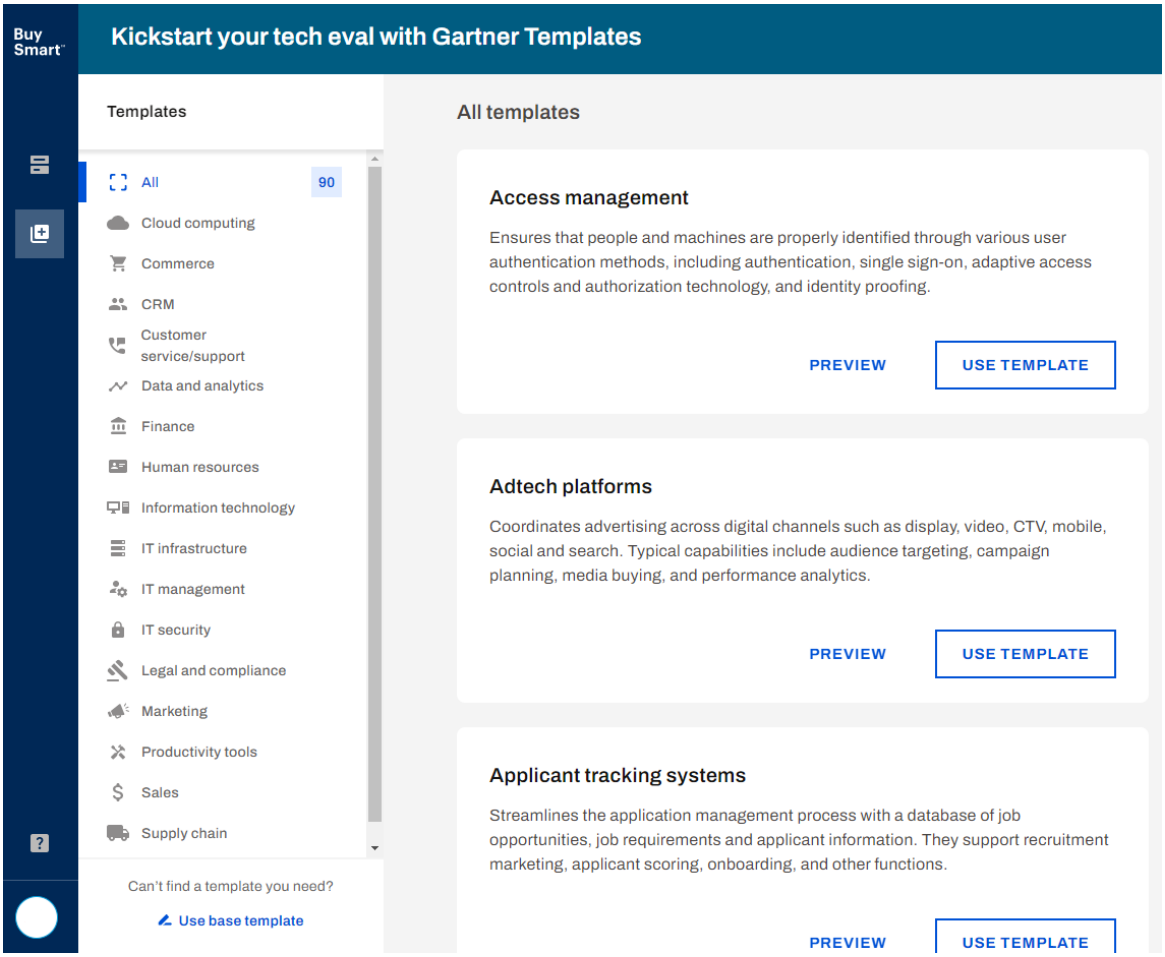
Figure 1. During each step of a technology purchase, BuySmart empowers executives and their teams with actionable Gartner insights and a collaborative workflow within a structured process designed to streamline vendor evaluations



The BuySmart application is available through the My Gartner online insights platform and currently includes **90 templates for purchasing products** categorized into different logical

groupings, such as IT Management, IT Infrastructure, IT Security, Analytics, Cloud Computing and more. The application is a comprehensive, self-serve platform that acts as a central workspace where the State can manage all milestones and tasks involved in a technology purchase, with Gartner providing insights and recommendations along the way.

Figure 2. Initiate the search for technology by selecting a BuySmart template, with each containing detailed requirements, a list of potentially relevant vendors and a comprehensive evaluation checklist

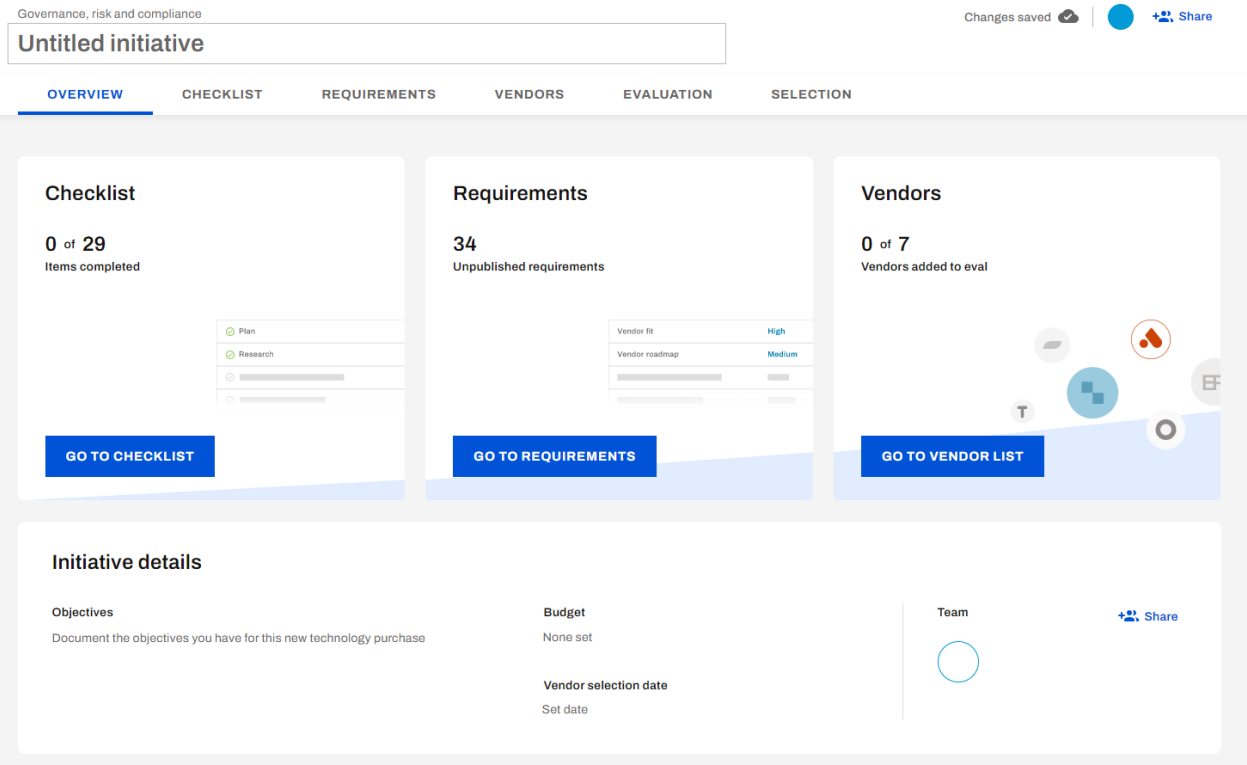


Once a State Entity selects a template, a new technology purchasing initiative is created within the BuySmart application. The initiative features a centralized workspace where users can access and edit information provided by the selected template, such as requirements and vendors. The BuySmart dashboard contains the following six sections:

- **Overview** — Use this window to set objectives, establish budget and invite participants while monitoring the progress of technology evaluation tasks. **Team members are not required to hold a Gartner subscription license to participate in the initiative.**
- **Checklist** — Follow a comprehensive checklist through each critical milestone or task for evaluating and purchasing technology. A State Entity can assign owners, set deadlines and monitor progress by task.

- **Requirements** — BuySmart gets the process started by generating a robust and fully customizable list of suggested requirements to prioritize for that technology initiative, with requirements broken down into multiple categories.
- **Vendors** — Select vendors for inclusion in the evaluation, using either Gartner's list of relevant vendors based on Magic Quadrant research and Peer Insight data, or additional companies identified by the State Entity.
- **Evaluation** — BuySmart provides a consistent rating system used to score and compare vendors during the evaluation cycle, with a detailed scorecard showing how each vendor rates within the State Entity's requirement criteria.
- **Selection** — Once the State Entity has chosen a vendor, BuySmart can generate a selection report that explains the decision, selection criteria and vendors considered during the process. The selection report can be used to secure buy-in from critical stakeholders within the organization, maximize understanding of the evaluation process and ultimately inspire confidence in the final decision.

Figure 3. BuySmart creates a fully customizable purchasing initiative in a central workspace



During each phase of the technology purchasing process, Gartner BuySmart helps:

1. **Discover** key technologies, requirements and vendors for consideration using proprietary Gartner insights.
2. **Evaluate** and manage requirements and vendor evaluations in a central workspace with an efficient, customizable process.
3. **Select** the right vendor for the organization and build confidence in the final decision.

4. **Optimize** spend and reduce risk with an optional proposal review from a Gartner research expert. Our analysts review over 11,000 proposals annually for over 15,000 client enterprises, who rely on Gartner research analysts for their expert insights regarding technology investments.

ATTACHMENT E5

THIRD PARTY TERMS

Intentionally Left Blank.

ATTACHMENT E6

SERVICE AGREEMENT TEMPLATE

The Service Agreement Template is hereby amended as set forth below and supersedes all prior documents submitted by Gartner, Inc. or discussed by the parties. The parties agree to use this Service Agreement Template or a document substantially similar in the for of this Service Agreement Template.

Gartner, Inc. Service Agreement for _____ ("Client")

This Service Agreement ("**SA**") is between Gartner, Inc. of 56 Top Gallant Road, Stamford, CT 06902 ("**Gartner**") on behalf of itself and all wholly-owned affiliates of Gartner, Inc. and Client of **<Insert Client Company Address>** ("**Client**"), and includes the Master Client Agreement (SW1026) between Gartner and Client or Client's parent or affiliate dated **<Insert Month/Year>** the terms of which are incorporated by reference, and all applicable Service Descriptions. This SA and SW1026 constitutes the complete agreement between Gartner and Client. . In the event, any additional terms conflict with the Master Agreement (SW1026) the terms in the Master Agreement shall prevail. Client agrees to subscribe to the following Services for the term and fees set forth below.

1. DEFINITIONS AND ORDER SCHEDULE:

Services are the subscription-based research and related services purchased by Client in the Order Schedule below and described in the Service Descriptions. Service Names and Levels of Access are defined in the Service Descriptions. Gartner may periodically update the names and the deliverables for each Service. If Client adds Services or upgrades the level of service or access, an additional Service Agreement will be required.

Service Descriptions describe each Service purchased, specify the deliverables for each Service, and set forth any additional terms unique to a specific Service. Service Descriptions for the Services purchased in this SA may be viewed and downloaded through the hyperlinks listed in Section 2 below or may be attached to this SA in hard copy and are incorporated by reference into this SA.

Service Name	Level of Access	Quantity	Name of User to be Licensed	Contract Term Start Date	Contract Term End Date	Annual Fee $	Total Fee $
				Total Services:	**(Excluding applicable sales tax)**		

2. SERVICE DESCRIPTIONS:

Service Name/ Level of Access	Service Description URL

3. PAYMENT TERMS
Upon submission of an accurate and proper invoice, the invoice shall be paid in arrears after products have been delivered or services provided and in accordance with applicable law, net 45 (forty-five) days. Client shall pay the fixed price agreed on by both parties.

If applicable, please attach any required Purchase Order ("**PO**") to this SA and enter the PO number below.. If an annual PO is required for multi-year contracts, Client will issue the new PO at least thirty (30) days prior to the beginning of each subsequent contract year. Any pre-printed or additional contract terms included on the PO shall be inapplicable and of no force or effect. All PO's are to be sent to purchaseorders@gartner.com. This SA may be signed in counterparts.

4. CLIENT BILLING INFORMATION (This section is not applicable if billing instructions are included on PO.)

_____	_____	
Purchase Order Number	*Billing Address*	
_____	_____	----------
Invoice Recipient Name	*Invoice Recipient Email*	*Invoice Recipient Tel. No.*

5. AUTHORIZATION

Client:	**Gartner, Inc.**
_____	_____
Signature/Date	*Signature/Date*
_____	_____
Print Name and Title	*Print Name and Title*

ATTACHMENT F

EXCEPTIONS TO SOLICITATION NO. 0900000582

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Gartner, Inc. or discussed by the parties.

REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

Term & Section	Language
Attachment B, State of Oklahoma General Terms, Section 16.5(B)	The following language shall be added to Section 16.5(B) Except for the Suppliers indemnification obligations related to (1) breach of confidentiality; (2) third party intellectual property infringement; (3) bodily injury and property damage; (4) gross negligence or willful misconduct; neither party's total liability under this Agreement will exceed an amount equal to 1.5x the fee payable by the State under the statement of work under which such liability arises or $1,000,000, whichever is greater.
Attachment D State of Oklahoma Information Technology Terms Section 6.1	Section 6.1 shall be modified to read as follows: The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines available at https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf except for the policies, procedures, or guidelines redlined and accepted by the State as attached hereto as Attachment F-2. Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards.html
Attachment D State of Oklahoma Information Technology Terms, Section 6.2 (pg 4)	Section 6.2 is modified to read as follows: Supplier shall comply with applicable the National Institute of Standards and Technology NIST 800-171. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards.
Attachment D State of Oklahoma Information Technology Terms, Section 6.3 (pg 6)	Section 6.3 is deleted in its entirety.
Attachment D State of Oklahoma Information Technology Terms, Section 11 (pg 7)	Section 11 is modified to include the following language: State and Supplier agree that Supplier is not planning to provide Customer customized computer software developed or modified exclusively for a state agency or the State. Should Supplier and State explicitly agree, in writing, to the acquisition of customized computer software developed or modified exclusively, then the following terms will apply:
Attachment D State of Oklahoma Information Technology Terms, Section 12 (pg 8)	Section 12 is modified to include the following language: State and Supplier agree that Supplier is not planning to provide Customer customized computer software developed or modified exclusively for a state agency or the State. Should Supplier and State explicitly agree, in writing, to the acquisition of customized computer software developed or modified exclusively, then the following terms will apply:
Attachment D State of Oklahoma Information Technology Terms, Appendix 1, Section	Section B6 shall be modified as follows: Supplier shall perform an independent audit of its data centers at least annually at its expense and provide Customer a copy of its certificate evidencing said audit.

B6 (pg. 13)	
Attachment D State of Oklahoma Information Technology Terms, Appendix 1, Section C (pg. 13)	Section C shall be modified as follows: The parties don't anticipate any entity or third-party supplier to host Oklahoma Customer Data under this Agreement; however, if the vendor or third-party does host Oklahoma Customer Data the terms below shall apply.
Attachment D State of Oklahoma Information Technology Terms, Appendix 1, Section D2 (pg. 14)	Section D2 shall be modified to read as follows: Supplier shall report a Security Incident involving Customer data to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
Attachment D State of Oklahoma Information Technology Terms, Appendix 1, Section D4 (pg. 15)	Section D4 shall be modified to read as follows: If Supplier has actual knowledge of a Data Breach involving Customer data, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.
Attachment D, State of Oklahoma Information Technology Terms, Section 1.13	Section 1.13 Work Product shall be modified to read as follows: **Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived exclusively for a state agency or the State including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to- practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
Attachment D, State of Oklahoma Information Technology Terms, Section 12	Section 12 shall be modified as follows: The parties don't anticipate any entity or third-party supplier to host Oklahoma Customer Data under this Agreement; however, if the vendor or third-party do host Oklahoma Customer Data the terms below shall apply.

ATTACHMENT F2

State of Oklahoma

Information Security

Policy, Information Security Policy, Procedures, Guidelines

TABLE OF CONTENTS

PREFACE

The contents of this document include the minimum Information Security Policy, as well as procedures, guidelines and best practices for the protection of the information assets of the State of Oklahoma (hereafter referred to as the State). The Policy, as well as the procedures, guidelines and best practices apply to all state agencies. As such, they apply equally to all State employees, contractors or any entity that deals with State information.

The Office of Management and Enterprise Services Information Services (OMES IS) will communicate the Policy, procedures, guidelines and best practices to all state agencies. In turn, all agencies are required to review the Policy and make all staff members aware of their responsibility in protecting the information assets of the State. Those agencies that require additional controls should expand on the content included in this document, but not compromise the standards set forth.

The Policy and those procedures prefaced by "must" are mandatory as the system involved will be classified as insecure without adherence. Guidelines and best practices are generally prefaced with "should" and are considered as mandatory unless limited by functional or environmental considerations.

It is recognized that some agencies have their own proprietary systems that may not conform to the Policy, procedures, guidelines and best practices indicated in this document. ~~A plan for resolution of these system limitations should be created. Any exceptions are to be documented and be available on request.~~ Other non-system related standards that do not require system modification should be instituted as soon as possible.

Revisions to this document are maintained collectively in Appendix E: Revisions, which includes a "Revision Table" describing each addition, change or deletion and the date it was implemented. All revisions are referenced using this procedure. The original document will remain intact.

STATE OF OKLAHOMA

INFORMATION SECURITY POLICY

Information is a critical State asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets, the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss or misuse can be costly, if not illegal. The intent of this Security Policy is to protect the information assets of the State.

This Security Policy governs all aspects of hardware, software, communications and information. It covers all State Agencies as well as contractors or other entities who may be given permission to log in, view or access State information.

Definitions:

- *Information includes any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.*
- *The Owner of the information is the State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.*
- *The Hosting State Agency has physical and operational control of the hardware, software, communications and data bases (files) of the owning Agency. The Hosting Agency can also be an Owner.*

The confidentiality of all information created or hosted by a State Agency is the responsibility of that State Agency. Disclosure is governed by legislation, regulatory protections and rules as well as policies and procedures of the owning State Agency. The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

All information content is owned by the State Agency responsible for collecting and maintaining the authenticity, integrity and accuracy of the information. The objective of the owning State Agency is to protect the information from inadvertent or intentional damage, unauthorized disclosure or use according to the owning Agency's defined classification standards and procedural guidelines.

Information access is subject to legal restrictions and to the appropriate approval processes of the owning State Agency. The owning State Agency is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the State Agency hosting the information. The hosting State Agency has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning State Agencies in a timely manner.

Information security – The State Agency Director, whose Agency collects and maintains (owns) the information, is responsible for interpreting confidentiality restrictions imposed by

laws and statutes, establishing information classification and approving information access. The hosting State Agency will staff a security function whose responsibility will be operational control and timely implementation of access privileges. This will include access authorization, termination of access privileges, monitoring of usage and audit of incidents. The State Agencies that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

Information availability is the responsibility of the hosting State Agency. Access to information will be granted as needed to all State Agencies to support their required processes, functions and timelines. Proven backup and recovery procedures for all data elements to cover the possible loss or corruption of system information are the responsibility of the hosting State Agency.

The hosting State Agency is responsible for securing strategic and operational control of its hardware, software and telecommunication facilities. Included in this mandate is the implementation of effective safeguards and firewalls to prevent unauthorized access to system processes and computing / telecommunication operational centers. Recovery plans are mandatory and will be periodically tested to ensure the continued availability of services in the event of loss to any of the facilities.

Development, control and communication of Information Security Policy, Procedures and Guidelines for the State of Oklahoma are the responsibility of OMES IS. This Policy represents the minimum requirements for information security at all State Agencies. Individual agency standards for information security may be more specific than these state-wide requirements but shall in no case be less than the minimum requirements.

1.0 INTRODUCTION

1. This document states the Policy and outlines procedures, guidelines and best practices required for creating and maintaining a secure environment for the storage and dissemination of information.

2. It is critical that all agencies and their staff are fully aware of the Policy, procedures, guidelines and best practices and commit to protecting the information of the State. Common sense and high ethical standards are required to complement the security guidelines.

3. The Policy, procedures, guidelines and best practices outlined represent the minimum security levels required and must be used as a guide in developing a detailed security plan and additional policies (if required).

1.1 BACKGROUND

1. The information Policy, procedures, guidelines and best practices apply to all agencies and are inclusive of their hardware facilities, software installations, communication networks / facilities as well as information.

1.2 POLICY, PROCEDURES, GUIDELINES

1. OMES IS has, among other responsibilities, the mandate to establish minimum mandatory standards for information security and internal controls as well as contingency planning and disaster recovery (reference: Oklahoma Statute, Title 62. Section 34.12(A)(3) Duties of Information Services).

2. In reference to the responsibilities stated above, the Statute reads as follows:
"Such standards shall, upon adoption, be the minimum requirements applicable to all agencies. These standards shall be compatible with the standards established for the Oklahoma Government Telecommunications Network. Individual agency standards may be more specific than statewide requirements but shall in no case be less than the minimum mandatory standards. Where standards required of an individual agency of the state by agencies of the federal government are stricter than the state minimum standards, such federal requirements shall be applicable."

1.3 AUDIENCE

1. The Policy, procedures, guidelines and best practices are for distribution to all State agencies through their respective Security Representative who will then be responsible for communicating the details to State employees as well as contractors or other entities whose position responsibilities include the creation, maintenance, or access of State information residing on any computer system or platform. Appendix C assigns the primary responsibility of the procedures, guidelines and best practices to the User, Owning Agency, or Hosting Agency.

2.0 INFORMATION

1. Management of information requires a working set of procedures, guidelines and best practices that provide guidance and direction with regards to security. The primary focus is on the confidentiality and integrity of the information required for delivering information throughout the State.

2.1 INFORMATION CONFIDENTIALITY

1. The overriding premise is that all information hosted or created by a State Agency is property of the State. As such, this information will be used solely for performance of position related duties. Any transfers or disclosures are governed by this rule.

2. The confidentiality of all information created or hosted by a State Agency is the responsibility of all State Agencies. *Disclosure is governed by legislation, regulatory protections, rules as well as policies and procedures of the State and of the owning State Agency.* The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

3. *Release of information is strictly for job related functions. Confidentiality is compromised when knowingly or inadvertently, information crosses the boundaries of job related activities.*

4. Users must be required to follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thereby establish access rights to information processing facilities or services. All agency staff must be advised to:
   (A) keep passwords confidential,
   (B) avoid keeping a paper record of passwords, unless this can be stored securely,
   (C) change passwords whenever there is any indication of possible system or password compromise,
   (D) select quality passwords with a minimum length of eight characters which are:
      (i) easy to remember,
      (ii) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.,
      (iii) free of consecutive identical characters or all-numeric or all alphabetical groups,
   (E) change passwords at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords),
   (F) avoid reusing or cycling old passwords,
   (G) change temporary passwords at the first log-on,
   (H) not include passwords in any automated log-on process, e.g. stored in a

macro or function key, and
(I) not share individual user passwords.

2.2 INFORMATION CONTENT

1. All information content hosted by a state agency is owned by and is the primary responsibility of the Agency responsible for collecting and maintaining the authenticity, integrity and accuracy of information. The objective of the owning State Agency is to protect the information from inadvertent or intentional damage as well as unauthorized disclosure or use according to the classification standards and procedural guidelines of the owning State Agency.

2. The following procedures must be followed by all State Agencies:
   (A) All information content must reflect the actual state of affairs of the respective Agency.
   (B) Changes in the status of personnel who have system access are entered in the system immediately and the appropriate authorization / change form sent to the hosting agency's Security Administration.
   (C) In the event of a dismissal, the respective Agency is to call and notify the hosting agency's Security Administration immediately.

2.3 INFORMATION ACCESS

1. Information access is subject to legal restrictions and to the appropriate approval processes of the owning State Agency. The owning State Agency is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the State Agency hosting the information.

2. All agencies must designate a security representative whose role includes: (A) communicating the information security Policy to all their respective agency's employees,
   (B) communicating the appropriate procedures, guidelines and best practices to the responsible user, owner, or people directly responsible for hosting activities as indicated in Attachment C,
   (C) granting, on behalf of their agency, user access to system functions, and (D) reporting all deviations to the Policy, procedures, guidelines and best practices.

3. Procedures for the Security Administration function at the Hosting Agency are: (A) Confirm set up to the Agency Director and the individual concerned via email when the set-up is complete for the role of Security Representative. (B) Confirm set up to the Security Representative and the individual concerned when the set-up is complete for the use roles assigned. The email confirmation will include access rights assigned in the system.
   (C) A daily report will be run by the hosting agency to list terminations. Security Administration at the hosting agency will lock the access privileges

at the end of day on the effective date. This does not preclude the responsibility of all agencies to notify the hosting agency of terminations using agreed upon formal notice or by the phone and/or email in the case of dismissals.

(D) The hosting agency will run a weekly report of transfers and follow up with the agencies concerned if a change notification is not received.

(E) Users not using the system for 60 days will be automatically deactivated. Security Administration at the hosting agency will notify the respective user agency and will require an email or new activation form from the user agency's security representative to reactivate the individual.

4. The hosting State Agency has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning State Agencies in a timely manner.

2.4 INFORMATION SECURITY

1. The State Agency Director whose Agency collects and maintains (owns) the information is responsible for interpreting all confidentiality restrictions imposed by laws and statutes as well as establishing information classification and approving information access. The hosting State Agency will staff a Security Administration function whose responsibility will be operational control and timely implementation of access privileges.

2. System limitations may prevent all of the following procedures to be implemented, however, when possible, these rules apply:
   (A) Passwords will be required to be a minimum of 8 characters long, containing at least one (1) numeric character.
   (B) Passwords will expire in a maximum of 90 days.
   (C) Passwords will be deactivated if not used for a period of 60 days. (D) Passwords for a given user should not be reused in a 12 month period.

3. The State Agencies that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

2.5 INFORMATION AVAILABILITY

1. Information availability is the responsibility of the hosting State Agency. Access to information will be granted as needed to all State Agencies to support their required processes, functions and timelines. Proven backup and recovery procedures for all information elements to cover the possible loss or corruption of system data are the responsibility of the hosting State Agency.

2. Required availability will vary with normal cycles of use (i.e. information is used constantly throughout the day, but is only periodically accessed during the evening by a backup process, becomes archival after the backup is complete). The following asset availability definitions should include a statement detailing over what time period the definition is accurate for (i.e. Constant during business

hours, archival after year-end, etc.):

Availability	**Frequency of Use**	**Loss / Absence Impact**
Constant	*Accessed at all times*	*Immediate cessation of supported business functions*
Regular	*Accessed intermittently by* 1 *individual but constantly by all users as a group (i.e. email)*	*Interruption or degradation, but not cessation, of supported business functions*
Periodic	*Accessed intermittently, or on* 1 *a schedule (i.e. year-end records)*	*Delay of supported business functions*
Archival	*Not normally accessible*	*Disruption of business support objectives*

3. The hosting State Agency will be responsible for:

(A) publishing a Service Level Agreement for all users of the system including response time, hours of availability and all other services contracted,
(B) ensuring all backups are current, secure and accessible,
(C) ensuring information facilities and data can be recovered, and
(D) ensuring adequate technical support for systems, data base access and operating systems.

3.0 SECURITY PROGRAM MANAGEMENT

1. Managing information security within the State can be layered into three components:
2. Central organization (OMES IS) is responsible for direction and leadership in all aspects of information security.
3. Agencies that host data services are responsible for creating system specific policies and guidelines *to complement, but not contradict* those issued by the central organization.
4. All agencies are required to develop procedures specific to their information and process flows to protect the integrity of information and guard against misuse or loss. This is not limited to, but includes computer based information systems.

3.1 CENTRAL SECURITY PROGRAM

1. In regards to information services, OMES IS will develop, maintain and communicate polices and guidelines for the protection of information assets including but not limited to hardware, software, information and

communications. The Policy, Procedures, Guidelines and Best Practices will be mandatory for all agencies and represent the minimum standards that all agencies will adopt.

2. Minimum standards will be issued for:
   (A) systems planning,
   (B) systems development methodology,
   (C) documentation,
   (D) hardware requirements and compatibility,
   (E) operating systems compatibility,
   (F) software and hardware acquisition,
   (G) information security and internal controls,
   (H) data base compatibility, and
   (I) contingency planning and disaster recovery.

3.2 HOSTING AGENCY SECURITY

1. Under the boundaries established by the minimum mandatory standards issued by the OMES IS, agencies hosting information and systems for their own use or for the use of other agencies will further develop, maintain and communicate polices and guidelines for the protection of information assets including but not limited to hardware, software, information and communications.

2. All hosting agencies will:
   (A) follow a systems development methodology,
   (B) create and maintain adequate documentation,
   (C) develop hardware requirements and compatibility for review by the Office of State Finance,
   (D) ensure operating systems compatibility,
   (E) expand and apply information security and internal controls,
   (F) ensure data base compatibility, and
   (G) develop and test contingency planning and disaster recovery.

3.3 AGENCY SECURITY

1. All agencies have the responsibility of protecting their information assets from disclosure, loss or misuse. As such all agencies are required to adhere to and have documented procedures for:

   (A) security of information flow within their area of control,
   (B) information retention,
   (C) information disposal (including shredding and deletion of electronic information), and
   (D) communication of information security Policy, procedures, guidelines and best practices monitoring adherence with polices.

3.4 INCIDENT MANAGEMENT

1. Incident management responsibilities and procedures must be established by the hosting agency to ensure a quick, effective and orderly response to security

incidents. Procedures must be established to cover all potential types of security incidents, including:
(A) information system failures and loss of service,
(B) denial of service,
(C) errors resulting from incomplete or inaccurate business information, and (D) breaches of confidentiality.

2. In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures must also cover:
   (A) analysis and identification of the cause of the incident,
   (B) planning and implementation of remedies to prevent recurrence, if necessary,
   (C) collection of audit trails and similar evidence,
   (D) communication with those affected by or involved with recovery from the incident, and
   (E) reporting the action to the security administration function at the hosting agency.

3. Audit trails and similar evidence must be collected and secured as appropriate, for:
   (A) internal problem analysis,
   (B) use as evidence in relation to a potential breach of contracts, policies, or regulatory requirements,
   (C) use in the event of civil or criminal proceedings, e.g. under computer misuse or information protection, and
   (D) use in negotiating for compensation from software and service suppliers.

4. Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures must ensure that:
   (A) only clearly identified and authorized staff are allowed access to live systems and information,
   (B) all emergency actions taken are documented in detail,
   (C) emergency action is reported to management and reviewed in an orderly manner, and
   (D) the integrity of business systems and controls is confirmed with minimal delay.

3.5 EVENT LOGGING AND MONITORING

1. Audit logs recording exceptions and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should include:
   (A) user IDs,
   (B) dates and times for log-on and log-off,

(C) terminal identity or location if possible,
(D) records of successful and rejected system access attempts, and
(E) records of successful and rejected data and other resource access attempts.

2. Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

3. Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:
   (A) Authorized access, including detail such as:
      (i) the user ID,
      (ii) the date and time of key events,
      (iii) the types of events,
      (iv) the files accessed, and
      (v) the program/utilities used.
   (B) All privileged operations, such as:
      (i) use of supervisor account,
      (ii) system start-up and stop, and
      (iii) I/O device attachment/detachment.
   (C) Unauthorized access attempts, such as:
      (i) failed attempts,
      (ii) access procedure violations and notifications for network gateways and firewalls, and
      (iii) alerts from proprietary intrusion detection systems.
   (D) System alerts or failures such as:
      (i) console alerts or messages,
      (ii) system log exceptions, and
      (iii) network management alarms.

4.0 RISK MANAGEMENT

1. Risk management encompasses risk assessment, risk mitigation as well as evaluation and assessment. The risk assessment process includes identification and evaluation of risks and risk impacts and recommendation of risk-reducing measures. Risk mitigation refers to prioritizing, implementing and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Through a continual evaluation process, the hosting agency is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk.

4.1 RISK ASSESSMENT

1. The hosting agency will be responsible for determining the likelihood of an adverse event, the threats to system resources, the vulnerability of the system and the impact such an adverse event may have.

2. To determine the likelihood of an adverse event, consider:
   (A) Motivation
   (B) Nature of the vulnerability
   (C) Current controls

3. A threat needs, and cannot exist without a vulnerability. A vulnerability is a weakness that can be intentionally or accidentally triggered. Threats can be posed from a lot of sources, some of which are:
   (A) System Intruders (hackers)
   (B) Criminals
   (C) Terrorists
   (D) Espionage
   (E) Insiders which could be malicious or a result of poor training

4. In identifying the vulnerabilities, consideration must be given to:
   (A) Hardware
   (B) Software
   (C) Network
   (D) System Interfaces
   (E) Data and information
   (F) People who support and use the system
   (G) Information sensitivity
5. The impact of an adverse event is the:
   (A) Loss of Integrity
   (B) Loss of Availability
   (C) Loss of Confidentiality

4.2 RISK MITIGATION

1. All hosting agencies are responsible for reducing risk to all information assets. The following are options provided in analyzing the alternatives.
   (A) Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
   (B) Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
   (C) Risk Limitation. To limit the risk by implementing controls that minimizes the adverse impact of a threat exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
   (D) Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements and maintains controls.
   (E) Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
   (F) Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

5.0 PERSONNEL/USER ISSUES

1. Personnel awareness of the information security Policy, procedures, guidelines and best practices is the responsibility of all agencies. Adherence to the Policy, procedures, guidelines and best practices is the responsibility of all state agencies on behalf of their employees.

2. Information security must be adopted at all levels as a "norm" of job performance. Information systems and data are vulnerable. With constant re-enforcement and monitoring, individuals will accept their responsibility to protect the information assets of the State and relate their performance in this area to standards of performance.

3. The IT staff must be alert and trained in offensive and defensive methods to protect the State information assets. Adequate staffing and key position backup are essential to run and maintain a secure environment.

5.1 STAFFING

1. Adequate staffing, training and backup are the responsibility of all hosting agencies. Each agency will be responsible for:
   (A) ensuring qualifications meet position requirements,
   (B) identifying roles that will impact operations when not filled, i.e. if the incumbent leaves or cannot perform the function,
   (C) ensuring training is in place to keep key individuals current with the technology available in the marketplace (this is particularly important with regards to the Internet and data base controls), and
   (D) documenting contingency plans if critical functions are not

available. **5.2 AWARENESS/TRAINING**

1. Awareness is not training. The purpose of awareness presentations are simply to focus attention on security and are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences, whereas training is more formal, having a goal of building knowledge and skills to facilitate job performance.

2. Effective IT security awareness presentations must be designed. Awareness presentations must be on-going, creative and motivational, with the objective of focusing attention so that the learning will be incorporated into conscious decision making.

3. The OMES IS will be responsible for:
   (A) communicating the minimum standards for all related policies and procedures,
   (B) providing recommendations for best practices in selected areas related to information security, and
   (C) providing all necessary information for the development of an

awareness
program by the agencies.

4. All state agencies will:
   (A) create and present security awareness sessions for their staff members, and
   (B) ensure all staff members have attended an awareness session.

5. All current employees as well as new employees or contractors when hired that have access to any information assets must be briefed by the hiring or contracting agency as follows:
   (A) the access requirements of their position or contract,
   (B) their responsibilities for safeguarding sensitive information and assets,
   (C) all information security policies, procedures, guidelines and best practices, and
   (D) a written document outlining the contents of the briefing and the date, which should be signed by the individual briefed acknowledging receipt of its contents.

5.3 PERSONAL COMPUTER USAGE 1. The agency computers of the State are provided for job related activities. To this end, the hosting agency provides support in networking and information resources for its computing community. 2. All users are given access to computers for job related duties and this usage must remain in compliance with State and agency policies as well as all state and federal laws governing usage and communication of information. Failure to comply will result in the denial of access privileges and may for employees lead to disciplinary action up to and including dismissal. For contractors, it may lead to the cancellation of the contractual agreement. Litigation may ensue. 3. In the effort to protect the integrity of the statewide network and its systems, any proof of unauthorized or illegal use of any agency computer and/or its accounts will warrant the immediate access to these files, accounts and/or systems by the hosting agency's security and information systems staff and appropriate action will be taken. 4. Information Security Policy for computer usage prohibits the use of its resources to: (A) Send email using someone else's identity (Email forgery). (B) Take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and/or access to external networks. (C) Install any system or software on the network without prior approval. (D) Install any software systems or hardware that will knowingly install a virus, Trojan horse, worm or any other known or unknown destructive mechanism. (E) Attempt IP spoofing. (F) Attempt the unauthorized downloading, posting or dissemination of

copyrighted materials. (G) Attempt any unauthorized downloading of software from the Internet. (H) Transmit personal comments or statements in a manner that may be mistaken as the position of the State.

(I) Access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

5. Furthermore, it is the State's position that all messages sent and received, including

~~personal messages and all information stored on the agency's electronic mail system, voicemail system or computer systems are State property regardless of the content. As such, the hosting agency reserves the right to access, inspect and monitor the usage of all of its technology resources including any files or messages stored on those resources at any time, in its sole discretion, in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information or for any other business purpose.~~

5.4 EMAIL USAGE

1. Electronic mail (email) is a highly efficient form of modern communication media. Used appropriately, email provides people with a means to communicate thereby facilitating business contact. However, this convenience also tempts users to experiment or take advantage of this media, resulting in email of unwelcome types (collectively known along with other unwelcome activity as Net Abuse). The improper use of this email technology may jeopardize systems integrity, security and service levels. Access to email is provided to users to assist them to perform their work and their use of email must not jeopardize operation of the system or the reputation and/or integrity of the State.

2. Email accounts are made available to all agency staff that require the service for the performance of job related functions. The following statements apply: (A) All email and associated system resources are the property of the State. Email is subject to the same restrictions on its use and the same review process as is any other government furnished resource provided for the use of employees. Its use and content may be monitored.
   (B) Email usage must be able to withstand public scrutiny. Users must comply with all applicable legislation, regulations, policies and standards. This includes complying with copyright and license provisions with respect to both programs and data.
   (C) While email is provided as a business tool to users, its reasonable, incidental use for personal purposes is acceptable. This use must not, however, detrimentally affect employee productivity, disrupt the system and/or harm the government's reputation.
3. Users may not:
   (A) use email for commercial solicitation or for conducting or pursuing their own business interests or those of another organization,

   (B) use email to distribute hoaxes, chain letters or advertisements and/or send rude, obscene, threatening or harassing messages,
   (C) use email to distribute pornographic material or hate literature,
   (D) use email to harass other staff members,
   (E) use email to send executable programs or games,
   (F) use email to send potentially offensive material, and
   (G) propagate viruses knowingly or maliciously.
4. Users must not send, forward and/or reply to large distribution lists concerning non-government business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists.
5. Email is a record and therefore management of email must comply with

existing legislation, regulations, policies and standards.

6. Alleged inappropriate use of the email technology will be reviewed by the agency involved as well as the hosting agency on a case by case basis and may lead to disciplinary action up to and including dismissal. In respect to contractors, it may lead to cancellation of the contractual arrangement. In any of the cases, it may lead to litigation.

5.5 INTERNET/INTRANET SECURITY

1. The World Wide Web (WWW) is a system for exchanging information over the Internet. An Intranet is a proprietary network that is specific for an entity, such as the State.

2. At the most basic level, the Web can be divided in two principal components: Web servers, which are applications that make information available over the Internet (in essence publish information) and Web browsers (clients), which are used to access and display the information stored on the Web servers. The Web server is the most targeted and attacked host on most organizations' network. As a result, it is essential to secure Web servers and the network infrastructure that supports them.

3. The specific security threats to Web servers generally fall into one of the following categories:
   (A) Malicious entities may exploit software bugs in the Web server, underlying operating system or active content to gain unauthorized access to the Web server. Examples of unauthorized access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the Web server.
   (B) Denial of Service attacks may be directed to the Web server denying valid users an ability to use the Web server for the duration of the attack.
   (C) Sensitive information on the Web server may be distributed to unauthorized individuals.
   (D) Sensitive information that is not encrypted when transmitted between the Web server and the browser may be intercepted.
   (E) Information on the Web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.

   (F) Malicious entities may gain unauthorized access to resources elsewhere in the organization's computer network via a successful attack on the Web server.
   (G) Malicious entities may attack external organizations from a compromised Web server, concealing their actual identities and perhaps making the organization from which the attack was launched liable for damages.
   (H) The server may be used as a distribution point for illegal copies software attack tools, or pornography, perhaps making the organization liable for damages.

4. The hosting agency is responsible for the Web server. Some examples of controls to protect from unauthorized access or modification are:

(A) install or enable only necessary services,
(B) install Web content on a dedicated hard drive or logical partition, (C) limit uploads to directories that are not readable by the Web server, (D) define a single directory for all external scripts or programs executed as part of Web content,
(E) disable the use of hard or symbolic links,
(F) define a complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted and which are accessible (and by whom), and
(G) use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

5. Maintaining a secure Web server is the responsibility of the hosting agency and involves the following steps:
(A) configuring, protecting and analyzing log files,
(B) backing up critical information frequently,
(C) maintaining a protected authoritative copy of the organization's Web content,
(D) establishing and following procedures for recovering from compromise, (E) testing and applying patches in a timely manner, and
(F) testing security periodically.

6. A firewall environment must be employed to perform the following general functions:
(A) filter packets and protocols,
(B) perform inspection of connections,
(C) perform proxy operations or selected applications,
(D) monitor traffic allowed or denied by the firewall, and
(E) provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed.

7. The hosting agency responsible for Internet security will:
(A) Keep operational systems and applications software up to date. Because software systems are so complex, it is common for security related problems to be discovered only after the software has been in widespread use. Although most vendors try to address known security

flaws in a timely manner, there is normally a gap from the time the problem is publicly known, the time the vendor requires to prepare corrections and the time you install the update. This gap gives potential intruders an opportunity to take advantage of this flow and mount an attack on computers and networks. To keep this time interval as short as possible, it is required to stay aware of:
(i) announcements of security-related problems that may apply, (ii) immediate actions to reduce exposure to the vulnerability, such as disabling the affected software and
(iii) permanent fixes from vendors.
(B) Restrict only essential network services and operating system on the host server.

(i) Ensure that only the required set of services and applications are installed on the host server. Either do not install unnecessary services or turn the services off and remove the corresponding files (and any other unnecessary files) from the host.

(C) Configure computers for file backup.

(D) Protect computers from viruses and programmed threats. (E) Allow only appropriate physical access to computers.

(F) Design, implement and monitor an effective firewall system.

6.0 HELP DESK MANAGEMENT

1. A world class Help Desk is characterized by responsiveness, knowledge, feedback and improvement. The speed at which issues are resolved, the

number of requests handled by the first level in support, the follow-up with the user community on status, security and the monitoring of performance with the goal of continuous improvement are the characteristics that separate a progressive, secure, mission critical operation from the ordinary, reactive operation.

2. The mandate of the help desk function should include:
   (A) Adherence to all policies and procedures as published.
   (B) Recommendation of new and/or changes to policies and procedures. (C) Ownership of all the calls until reassigned or routed.
   (D) Performance of all front line tasks such as password resets, printer resets, etc.
   (E) Routing of system or technical queries to the knowledge expert responsible. (F) Reporting on and monitor calls.
   (G) Reporting and escalation of all incidents of suspicious activity or violations of security.

3. The following is a list of suggested reports required for managing the Help Desk.

   (A) Incident Report - Content: all known information, status. Schedule: Immediately. Distribution: Security Administration at hosting Agency.
   (B) Call Activity - Content: calls by type agency, severity average resolution time. Schedule: Monthly. Distribution: Management.
   (C) Open Calls - Content: calls by user agency, severity, ranked by oldest time open. Schedule: Weekly. Distribution: Help Desk, Knowledge Experts.
   (D) Daily Activity - Content: calls received by time of day. Schedule: Daily. Distribution: Help Desk.
   (E) Repeat Calls - Content: number of calls ranked by user (over 3) showing Agency, type. Schedule: Monthly. Distribution: Knowledge Expert and Director of the agency generating the calls.

6.1 SUPPORT CALLS

1. Call handling and routing is the responsibility of the hosting agency's help desk function. This function should present a standard front to all users of their services including telephone calls, emails and voice mails. Information on all calls will be logged and violations in security or suspicious activity will be reported immediately to the appropriate designated authority. The help desk function will verify the identity of the caller by:
   (A) Obtaining their name.

   (B) Verifying a question and answer submitted on a Systems Access Authorization Request.
   (C) Requesting additional information, such as:
      (i) User ID *(interchangeable with Log-on ID)*
      (ii) Agency

(iii) Phone number

6.2 PASSWORD RESETS

1. Password resets are the responsibility of the hosting state agency's help desk function. Identities of requestors will be verified by the help desk, logged and confirmed back to the user at the respective State Agency.

2. It is the responsibility of the requestor from all State Agencies, in requesting a password reset, to confirm their identity. This may be accomplished by: (A) Providing their name.
   (B) Answering a unique question and answer submitted on sign up, such as: place of birth, mother's maiden name, etc.).
   (C) Providing additional information as may be requested, such as:
      (i) Agency
      (ii) Phone number

3. The responsibility of the host agency's Help Desk is to:
   (A) Confirm the identity of the requestor.
   (B) Report all suspicious activity to the security Administrator immediately. Discrepancies in answers, inability to provide the correct User ID, frequent requests for changes to the same User ID, or obvious password sharing constitute security breaches and will be reported.
   (C) Reset the password.
   (D) Log details of the call.
   (E) Confirm the password reset to the user registered to the User ID via email. (F) Report activity monthly to each State Agency involved.

6.3 VOICE MAIL SECURITY

1. The voice mail feature of many PBXs can be a particularly vulnerable feature. This is because voice mail is typically used to let someone store voice messages at a central location by calling in from any inside or outside line and then retrieve the messages from any inside or outside line. It also grants the general public access to the PBX system.

2. In retrieving messages, the target extension and a password are usually required to gain access to the messages. Since the target extension is usually easy to determine, the only significant restriction to an adversary is the password. Once an adversary determines a target user's password all messages left for the target user are accessible to the adversary. The adversary could also delete

messages from the target user's mailbox to prevent an important message from getting to the target user. Some guidelines to secure the contents of voice mail include the following:
(A) Default and obvious passwords must be changed at initial log-in. The target user's extension is easily known. Default passwords established at system initialization time may never have been changed. Fixed

length passwords are more vulnerable than variable length passwords. Variable length passwords can be terminated by a special key such as the # or * key. If not, the passwords would probably be of fixed length and it reduces the number of random combinations that may be tried before a correct password is found.

(B) Non-terminated password entry should be avoided. Some systems accept a continuous string of digits, granting entry when the correct password sequence is entered. By not requiring a password entry to be terminated, the length of the average sequence needed to guess a four digit password is reduced by a factor of five.

(C) A complete password must be entered before an incorrect password is rejected. If it is rejected on the first incorrect digit, sequential guessing becomes much more practical. For example, on such a system that has a fixed password length of four and uses the digits 0-9, it would take at most 40 sequential attempts to guess a password. On a system that required all four digits to be entered at most 10,000 guesses would be required. (D) Disallow access to external lines via the Voice Mail system.

7.0 PHYSICAL AND ENVIRONMENTAL SECURITY

1. The hosting agency has the responsibility for documentation, execution, monitoring and testing of a physical security plan for both computer and telecommunication assets. This physical security plan would evaluate the risks from potential losses due to:

(A) physical destruction or theft of physical assets,
(B) loss or destruction of information and program files,
(C) theft of information,
(D) theft of indirect assets, and
(E) delay or prevention of computer processing.

2. Included in the plan would be measures for reducing the possibility of a loss and must address:
(A) changes in the environment to reduce exposure,
(B) measures to reduce the effect of a threat,
(C) improved control procedures,
(D) early detection, and
(E) contingency plans.

7.1 OPERATIONS CENTER

1. The following are guidelines of the action items for establishing, implementing and maintaining a physical security program at the hosting agency:
(A) conduct a risk analysis (refer to section 4),
(B) determine local natural disaster probabilities,
(C) protect supporting utilities
(D) ensure computer reliability,
(E) provide physical protection
(F) implement procedural security,
(G) plan for contingencies,
(H) develop security awareness, and
(I) validate the program.

7.2 OPERATIONS MONITORING

1. Hosting agencies can monitor security effectiveness by comparing performance to the metrics in a service level agreement and incidents that occur in violation of security policies, procedures, guidelines and best practices.

2. Guidelines for hosting agencies in establishing a service level agreement are: (A) hours of system availability,
(B) hours of application system support,
(C) hours of technical support,
(D) off hours support,
(E) average system response time, and
(F) other metrics as suitable for agency specific applications.

3. Hosting agencies should have a goal of achieving 99.9%+ of the metrics established in the service level agreement. Failure to achieve these targets could be an indication of security breaches.

4. Insofar as incidents are concerned, both offensive and defensive actions to

protect the security of physical assets should be considered routine. Examples of offensive actions include:
(A) routine changes of passwords,
(B) develop an escalation procedure of incidents,
(C) routine changes of locks or combinations to the facilities,
(D) have more than one person knowledgeable for critical functions,
(E) rotate shifts or people between functions,
(F) monitor all incursion attempts,
(G) install latest versions of firewall software,
(H) maintain 24x7 vendor contact list,
(I) routine backups,
(J) off-site storage of system information and programs,
(K) redundant components, lines for critical systems, and
(L) testing of recovery procedures.

5. Examples of defensive actions include:
(A) report and action all deviations to security policies, procedures, guidelines and best practices,
(B) shut down any infected machine immediately,
(C) disconnect any problem areas from the network,
(D) revoke privileges of users violating policies,
(E) assign severity to an issue and escalate, and
(F) acquire knowledgeable resources.

7.3 BACK-UP OF INFORMATION

1. Back-up copies of essential business information and software must be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. The following controls must be considered:
(A) A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, should be stored in a remote location at a sufficient distance to escape any damage from a disaster at the main site. ~~At least three generations or cycles of~~ back-up information should be retained ~~for important business applications~~as commercially and technically feasible as per Agency's business application requirements.
(B) Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.
(C) Back-up media should be regularly tested, where practicable, to ensure that

they can be relied upon for emergency use when necessary.
(D) Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

(E) The retention period for essential business information and also any requirement for archive copies to be permanently retained should be determined.

7.4 ACCESS CONTROL

1. Logical and physical access controls are required to ensure the integrity of the information and physical assets.

2. The following guidelines for controlling logical access should be implemented by all state hosting agencies:
   (A) document and adhere to procedures for granting, modifying and revoking access,
   (B) ensure segregation of duties for access
   (C) install detection mechanisms for unauthorized access attempts,
   (D) timeout a session after reasonably acceptable period~~15 minutes~~ of inactivity, and
   (E) revoke access after ~~an inactivity period of~~ 60 days upon employee termination.

3. Physical access control guidelines for all agencies include:
   (A) all telecommunication and computer related equipment are to be in a secured, locked environment,
   (B) access codes for secure environments must be changed at least every 60 days or in the event of an individual departing that previously had access,
   (C) account for all keys issued for those facilities using this method and replace locking mechanism when a key is missing,
   (D) when the system permits, log all accesses and retain, and
   (E) secure all peripherals such as air conditioning, generators, etc.
   (F) segregation of duties must be implemented to prevent unauthorized access to systems or data

7.5 NETWORK

1. Unsecured connections to network services can affect the whole organization. Users must only have direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.
2. Procedures concerning the use of networks and network services should cover: (A) the networks and network services which are allowed to be accessed, (B) authorization procedures for determining who is allowed to access which networks and networked services, and
   (C) management controls and procedures to protect the access to

network connections and network services.

3. The path from the user terminal to the computer service must be controlled.

Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to business applications, or unauthorized use of information facilities. Incorporating controls that restrict the route between a user terminal and the computer services its user is authorized to access, e.g. creating an enforced path can reduce such risks. The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorized to access. This usually requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices.

4. ~~The following methods should be implemented to limit the path to a service: (A) allocating dedicated lines or telephone numbers, (B) automatically connecting ports to specified application systems or security gateways, (C) limiting menu and submenu options for individual users, (D) preventing unlimited network roaming, (E) enforcing the use of specified application systems and/or security gateways for external network users, (F) actively controlling allowed source to destination communications via security gateways, e.g. firewalls, and (G) restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organization.~~

5. External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. Therefore, access by remote users must be subject to authentication. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.
   (A) Authentication of remote users should be achieved using one of the following techniques:
   (B) a cryptographic based technique,
   (C) hardware tokens,
   (D) a challenge/response protocol,
   (E) dedicated private lines or a network user address checking,
   and (F) call-back procedures.

6. Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's

network from remote locations. When using this control an organization should not use network services which include call forwarding or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. It is also important that the call back process includes ensuring that an actual disconnection on the organization's side

occurs. Otherwise, the remote user could hold the line open pretending that call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

7. A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems must therefore be authenticated. This is especially important if the connection uses a network that is outside the control of the organization's security management. Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility.

8. Access to diagnostic ports must be securely controlled. Many computers and communication systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. They should therefore be protected by an appropriate security mechanism, e.g. a key lock and a procedure to ensure that they are only accessible by arrangement.

9. Networks are increasingly being extended beyond traditional organizational boundaries as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions will increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, controls must be introduced in networks to segregate groups of information services, users and information systems.

10. The security of large networks should be controlled by dividing them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter should be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains and to block unauthorized access in accordance with the organization's access control procedures. An example of this type of gateway is what is commonly referred to as a firewall. The criteria for segregation of networks into domains should be based on the access control procedures and access requirements and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

11. The connection capability of users must be restricted in shared networks, in accordance with the access control procedures.

12. ~~Such controls should be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be~~

based on the access procedures and requirements of the business applications and should be maintained and updated accordingly. Examples of applications to which restrictions should be applied are: (A) electronic mail, (B) one-way file transfer, (C) both-ways file transfer, (D) interactive access, and (E) network access linked to time of day or date.

13. Shared networks must have routing controls to ensure that computer connections and information flows do not breach the access control procedures of business applications. This control is essential for networks shared with third party (non organization) users.

14. Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware. Implementers should be aware of the strength of any mechanisms deployed. A wide range of public or private network services is available, some of which offer value added services. Network services may have unique or complex security characteristics.

15. A clear description of the security attributes of all network services used by the organization must be provided.

7.6 ELECTRONIC COMMERCE SECURITY

1. Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information and must be protected. The following issues must be resolved:

(A) Authentication. What level of confidence should the customer and trader require in each other's claimed identity?
(B) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?
(C) Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of dispatch and receipt of key documents and the non-repudiation of contracts?

(D) Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?
(E) Order transactions. How is the confidentiality and integrity of order, payment and delivery address details and confirmation of receipt, provided?
(F) Vetting. What degree of vetting is appropriate to check payment information supplied by the customer?
(G) Settlement. What is the most appropriate form of payment to guard against fraud?

(H) Ordering. What protection is required to maintain the confidentiality and integrity of order information and to avoid the loss or duplication of transactions?
(I) Liability. Who carries the risk for any fraudulent transactions?

2. Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization. Other agreements with information service and value added network providers may be necessary.

3. Consideration should be given to the resilience to attack of the host used for electronic commerce and the security implications of any network interconnection required for its implementation.

7.7 MOBILE COMPUTING

1. Formal procedures must be in place and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. For example such procedures should include the requirements for:
   (A) physical protection,
   (B) access controls,
   (C) cryptographic techniques,
   (D) back-ups, and
   (E) virus protection.

2. Procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

3. Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

4. It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against

malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

5. Suitable protection should be given to the use of mobile facilities connected to networks.

6. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and

authentication and with suitable access control mechanisms in place

7. Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

7.8 REMOTE COMPUTING

1. Remote computing uses communications technology to enable staff or agencies to work remotely from a fixed location outside of their organization. Suitable protection of the remote computing site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working.

2. Procedures must be developed from best practices to authorize and control remote computing activities. Agencies should only authorize remote computing activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the agency's security procedures. The following should be considered:
   (A) the existing physical security of the remote computing site, taking into account the physical security of the building and the local environment, (B) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system, and
   (C) the threat of unauthorized access to information or resources from other people using the accommodation.

3. The controls and arrangements to be considered include:
   (A) the provision of suitable equipment and storage furniture for the remote computing activities,
   (B) a definition of the work permitted, the hours of work, the

classification of information that may be held and the internal systems and services that the user is authorized to access,
(C) the provision of suitable communication equipment, including methods for securing remote access,
(D) physical security,
(E) the provision of hardware and software support and maintenance, (F) the procedures for back-up and business continuity, and
(G) audit and security monitoring.

7.9 EXTERNAL FACILITIES

1. The use of an external contractor to manage information processing or communication facilities may introduce potential security exposures, such as the possibility of compromise, damage or loss of data at the contractor's site.

2. Prior to using external facilities, the risks must be identified and appropriate controls agreed with the contractor and incorporated into the contract. Particular issues that should be addressed include:
   (A) identifying sensitive or critical applications better retained in-house, (B) obtaining the approval of business application owners,
   (C) implications for business continuity plans,
   (D) security standards to be specified and the process for measuring compliance,
   (E) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
   (F) responsibilities and procedures for reporting and handling security

incidents. **7.10 ENCRYPTION**

1. Encryption should be applied to protect the confidentiality of sensitive or critical information.

2. Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

3. Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

4. Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

5. When developing procedures the following should be considered: (A) the management guidelines on the use of cryptographic controls across the organization,
   (B) including the general principles under which business information should be protected,
   (C) the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys,
   (D) roles and responsibilities, e.g. who is responsible for: the implementation of the procedures; the key management,

(E) how the appropriate level of cryptographic protection is to be determined, and
(F) the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).

8.0 BUSINESS CONTINUITY

Agency's BCM program proactively develops capabilities and procedures that enable Agency to avoid business interruptions where possible, and to efficiently, effectively, and safely resume critical business operations and services following a business disruption. Business continuity system is focused on the following:

- **Prevention, identification and elimination of existing and future threats to Agency's business;**

- **Proactive approach to minimize impact of incidents;**
- **Effectiveness of actions taken in the events which might lead to business interruption;**
- **Minimizing the periods and consequences of downtime during incidents.**

IT Disaster Recovery addresses the technology planning and systems necessary to recover critical applications, services and technology infrastructure required to support critical business functions and services following a disruption to normal technology operations..

1~~. Information Technology facilities and systems are vulnerable to a variety of disruptions, some of which are short term (measured in minutes and hours) and others lasting for a day or longer. The intent of Business Continuity Planning is to be alert and ready to sustain an organization's processes during and following a significant unforeseen disruption in services caused by disasters and security failures. 2. Business continuity should begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of magnitude and recovery time frame). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes, and is not limited to the information processing facilities. 3. A strategy plan, based on appropriate risk assessment, must be developed for the overall approach to business continuity. 4. All hosting State Agencies will develop contingency plans for each major application or general support system to meet the needs of critical IT operations in the event of a disruption extending beyond a given time period. The length of the time period may vary with the system or facility involved. The procedures for execution of such a capability will be documented in a formal contingency plan, be reviewed annually and updated as necessary by the hosting agency. The procedures must account for differential daily backups and complete weekly backups to be conducted and sent to a designated off-site facility. As well, the plans should assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential IT functions. Designated personnel will be trained to execute contingency procedures. An annual test of the recovery procedures will be conducted. 5. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. **8.1 CONTINGENCY PLAN** 1. A contingency plan provides the documented organizational plan to mitigate risks of business interruption and minimize the impact of any disruption of service. It must maintain instructions for achieving a full or minimally acceptable set of business objectives in the absence of assets, through cost-effective strategies to provide replacements for assets as they become unavailable. The Plan must involve advance planning and preparations to respond to external circumstances as determined by a risk assessment and continue to provide a pre-determined acceptable level of business functionality. Procedures and guidelines must be defined, implemented, tested and maintained to ensure continuity of organizational services in the event of a disruption. Each contingency plan is~~ ~~unique and must be tailored to organization's requirements; it must be flexible enough to allow additions, modifications and maintenance. The plan should minimize dependency on individuals for interpretation and implementation – in the event of emergency, key personnel may not be available. It must ensure completeness and establish critical decisions. Always make sure that the plan remains current. The following questions must be answered: (A) What risks the organization is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes? (B) How long can the enterprise operate without this asset? (C) What is the impact interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents, as~~

well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities? (D) What is the maximum acceptable delay before which temporary systems must be made available? (E) What is the minimum time in which temporary systems may be expected to become available? (F) At what minimally acceptable level of functionality can the enterprise operate? (G) How long can the enterprise operate at a minimally acceptable level of performance? (H) At what point can the enterprise begin to resume normal operations? (I) At what point must the enterprise begin to resume normal operations? 2. A Contingency Plan should contain the roles, responsibilities and procedures for restoring a system or facility following a major disruption. The following guidelines represent the stages to be followed in preparing and executing a Contingency Plan: (A) Documentation - A plan must be documented, tested and communicated. Included in the plan should be a mission, a scope of what is included and not included assumptions, requirements, staffing and responsibilities. (B) Notification/Activation - Internally within IT, the notification, timing and paths should be documented. There should only be one voice talking for the recovery team for communication and escalation outside the boundaries of IT. Immediately following damage assessment, the plan is activated. (C) Recovery - The sequence of recovery activities should be documented in procedures. These activities are to restore operations which may be in temporary locations or with incomplete data. (D) Reconstitution - Restoring facilities and systems to the "norm" will include testing and proof of operations viability. (E) What equipment / facilities are expected to be unavailable? (F) What is the timing of the disruption? (G) What records, files and materials may / may not be expected to be protected from destruction? (H) What resources are available or required following the event? (i) Applications / Processes (ii) Functionality / Capacity (iii) Equipment / Infrastructure (iv) Staff /Skills (v) Connectivity / Network (vi) Data Sources (vii) Facilities / Services / Physical Premises (viii) Transportation (ix) Documentation / Reference material (x) Security Policies and Procedures (xi) Specific Policies and Procedures (xii) Authorization 3. Following is a list of considerations that, at a minimum, must be addressed in creating contingency plans: (A) What additional security measures are required to protect assets in the planning, execution and maintenance of procedures to assure business continuity? (B) What degree of functionality is still available at the main facility, if any? (C) Availability of staff to perform critical functions defined within the plan. (D) Ability of staff to be notified and report to the backup site(s) to execute contingency plans. (E) Backup files and recovery methods. (F) Off-site storage facilities and materials availability. (G) Disaster recovery plan. (H) Suitability of subsets of the overall plan, to be used to recover from minor interruptions. (I) Availability of an alternate facility. (J) Off-site availability of critical forms and supplies, either at an alternate facility or off-site storage. (K) Existence of a backup site for processing the organization's work. (L) Availability of long distance and local communications lines. (M) Quality of surface transportation in from local to remote sites. (N) Ability of vendors to perform according to their general commitments to support the organization in a disaster. (O) Provisions for staff while at off-site location (food, water, telephones, beds, etc.) This list of considerations is not all inclusive and must be added to as appropriate. 4. General requirements of contingency plans must include: (A) Definitions of conditions under which the Business Recovery Strategy must be implemented. (B) Recovery point objective stages. (C) Recovery time objective stages. (D) Security preservation checklist. (E) Task Assignments. (F) Post-event Recovery Analysis. (G) Required resources, by priority. (H) Required recovery time / levels of availability of resources. (I) Documentation of normal and response procedures. 5. Refer to the considerations outlined in Appendix D. **8.2 DISASTER RECOVERY PLAN**

1. A Disaster Recovery Plan is intended to maintain critical business processes in the event of the loss of any of the following areas for an extended period of time: (A) desktop computers and portable systems,
(B) servers,
(C) Web sites,
(D) local area networks,
(E) wide area networks,
(F) distributed systems, and
(G) mainframe systems.

2. Teams should be formed to address each of the areas indicated consisting of a team lead and designate as well as key knowledge personnel required for that particular area. All contact information must be available for IT management, team members, all IT personnel and designated business unit management. When available, this information should include:
(A) work telephone number,
(B) pager number,
(C) home telephone number,
(D) cellular telephone number,
(E) work email address,
(F) home email address, and
(G) home address.

3. Upon receiving the information of a serious incident any member of management can invoke the Plan. Depending on the nature of the incident a command center will be established and appropriate teams mobilized. Management and the team leads are responsible for contacting all required personnel. Appendix B represents a sample crisis team organization and roles corresponding with potential disaster situations. All roles would have designates in the event one or more individuals are unavailable.

4. Communications to the IT department is the responsibility of Management and the Team Lead. In respect to external communications, it is extremely important that there is a single point of disclosure in order to ensure accurate and timely updates. The following roles and individuals must be determined and documented:
(A) Upwards, within the affected agency's organization.
(B) Outwards to affected agencies.
(C) Outwards to the public.

5. Hard copies of the Plan must be:
(A) stored off site at a secure location,
(B) stored at the personal residence of the team leads,
(C) stored at the personal residence of all IT managers and directors,
and (D) stored on a secure internet site.

6. As soon as an emergency is detected:
(A) Identify the problem and,

(i) Notify emergency services in cases of physical threats to personnel or facilities,
(ii) Notify the IT Director and his alternate.
(iii) Notify the appropriate team leads. In the event of a mainframe disaster, notify all team leads.
(iv) Notify vendors and business partners.

(B) Evacuate the premises if there are concerns of personal safety. All personnel should:
(i) be aware of evacuation routes and
(ii) have in possession or be aware of notification numbers.

(C) Reduce any exposure:
(i) In the event of air conditioning failure *(this usually involves powering down the systems at a temperature determined by the tolerances set by the manufacturer),*
(ii) In the event of fire *(this usually involves the automatic releasing of fire retardant, cutting of power, notification to emergency services and evacuation),*
(iii) In the event of electrical failure *(If a UPS and generator are available, usually the only action is to monitor fuel levels of the generator. If a UPS only is available, shut down procedures should begin and be terminated with at least 20% of rated capacity left),*
(iv) In the event of flood, water or wind damage *(this usually involves the normal powering down all systems if possible. If not, the immediate cut off of power is required, followed by notification to emergency services and evacuation),*
(v) In the event of malicious intrusion *(this usually involves the immediate isolation of affected hardware from all networks and connectivity. Usually the extent of exposure and damage is not immediately known so the immediate isolation of all network links is recommended and processing on affected facilities halted pending analysis by crisis teams).*

(D) Initiate backup site procedures:
(i) The Plan Coordinator establishes a command and control center *(usually an onsite and offsite center have been previously identified and the necessary computer and communication links are readily available).*
(ii) The Plan Coordinator ensures all team leaders are notified *(usually it is the responsibility of the Team Lead to get in touch with all team members).*
(iii) The Plan Coordinator notifies the off-site storage facility that a contingency event has occurred and to ship the necessary materials as determined in the damage assessment to the alternate site.
(iv) The Plan Coordinator notifies the alternate site that a contingency event has occurred and to prepare the facility for the organization's

 arrival.
(v) Both upward and outward communication on status is the responsibility of the Plan Coordinator *(usually set times are pre established such as: immediate after 1 hour, after 3 hours, etc. or at*

major milestones such as problem determination, resolution plan, when planned resumption of services is known and start-up of services is accomplished).

(vi) The Plan Coordinator is responsible for managing expectations.

(E) Initiate recovery at the alternate site:

(i) Contingency plan is followed using documented recovery points and defined priorities.

(ii) The Plan Coordinator reviews responsibilities with all team members and establishes recovery logs.

(iii) Recovery goals and procedures are established and prioritized by the Plan Coordinator.

7. The Disaster Plan appendices should include:

(A) Personnel Contact List

(B) Vendor Contact List

(C) Equipment and Specifications.

(D) Service Level Agreements.

(E) Related Contracts.

(F) Standard Operating Procedures.

8.3 BUSINESS RECOVER STRATEGY

1. A Business Recovery Strategy provides the documented organizational plan to restore full business functionality as quickly and as cost-effectively as possible. The Business Recovery Strategy is initiated as soon as the enterprise is deemed able to resume normal operations following a disaster.

2. The Business Recovery Strategy must involve advance planning and preparations to recover from external circumstances. Recovery strategies must be created, implemented, tested and maintained to ensure restoration of organizational services in the event of an interruption.

3. A "worst case scenario" must be the basis for developing the plan, where the worst case scenario is the destruction of the main or primary facility. Because the plan is written based on this premise, less critical situations can be handled by using subsets of the plan, with minor (if any) alterations required. Recovery from, or mitigation of a scenario should not be considered an all-or-nothing proposition. Many stages may be required, each with its own success conditions, before a 'final' state of continuity or recovery is reached.

4. Specific goals of the Business Recovery Strategy must include:

(A) Complete service functionality recovery objectives, in stages, by delay, duration and degree.

(B) Details of processes already in place to recover from an incident.

 (C) Details of what degree of business functionality they may be expected to restore.

(D) In what length of time existing process may be expected to restore service. (E) Requirements to bridge from existing processes to sufficient processes. (F) Lead time to secure additional resources.

5. The Business Recovery Strategy must include detailed, step-by-step instructions for how to replace / restore the following, in appropriate sequence: (A) Applications / Processes
(B) Functionality / Capacity
(C) Equipment / Infrastructure
(D) Staff /Skills
(E) Execution Duration / Delay
(F) Connectivity / Network
(G) Data Sources
(H) Facilities / Services / Physical Premises
(I) Transportation
(J) Documentation / Reference material

9.0 DATA CENTER MANAGEMENT

1. Related specifically to security of information and data center management, the pace of change, the reality of the World Wide Web and the increasing numbers of internal and external portals demand constant monitoring with both offensive

and defensive strategies.

9.1 OPERATING PROCEDURES

1. The operating procedures identified by security procedures should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.

2. The procedures should specify the instructions for the detailed execution of each job including the following:
   (A) processing and handling of information,
   (B) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times,
   (C) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities,
   (D) support and owner contacts in the event of unexpected operational or technical difficulties,
   (E) special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs, and
   (F) system restart and recovery procedures for use in the event of system failure.

3. Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

9.2 OPERATIONAL CHANGE CONTROL

1. Changes to information processing facilities and systems must be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

2. Operational programs should be subject to strict change control. When programs are changed an audit log containing all relevant information should be retained. Changes to the operational environment can impact applications. Wherever practicable, operational and application change control procedures should be integrated.

3. In particular, the following controls must be implemented:
   (A) identification and recording of significant changes,
   (B) assessment of the potential impact of such changes,
   (C) formal approval procedure for proposed changes,
   (D) communication of change details to all relevant persons, and

(E) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

9.3 SEGREGATION OF DUTIES

1. Duties and areas of responsibility must be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.

2. Small agencies may find this method of control difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent.

3. Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.

4. The following controls must be implemented:
   (A) It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received.
   (B) If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.
   (C) Separation of duties of both physical and logical access controls must be implemented to separate the access and functions of:
   (i) information systems and infrastructure administration to include configuration;
   (ii) security, audit, and accountability functions;
   (iii) privileged users and power user functions;
   (iv) data analysis and report generation functions;
   (v) general user functionality and associated access must be segregation between user and administrative functions and access must be maintained.

9.4 SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES

1. Development and testing facilities must be separated from operational facilities. Rules for the transfer of software from development to operational status should be defined and documented.

2. Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems should be considered. A similar separation should also be implemented between development and test

functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

3. Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational information. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems.

4. Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business information.

5. The following controls should be considered:
   (A) Development and operational software should, where possible, run on different computer processors, or in different domains or directories.
   (B) Development and testing activities should be separated the best way possible.
   (C) Compilers, editors and other system utilities should not be accessible from operational systems.
   (D) Different log-on procedures should be used for operational and test systems, to reduce the risk of error. Users should be encouraged to use different passwords for these systems and menus should display appropriate identification messages.
   (E) Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

9.5 SYSTEMS PLANNING AND ACCEPTANCE

1. To minimize the risk of systems failure:
   (A) Advance planning and preparation are required to ensure the availability of adequate capacity and resources.
   (B) Projections of future capacity requirements should be made, to reduce the risk of system overload.
   (C) The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

9.6 CAPACITY PLANNING

1. Capacity demands must be monitored and projections of future capacity

requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization's information processing.

2. ~~Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Operations managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.~~

3. ~~These managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services and plan appropriate remedial action.~~

9.7 SYESTEMS ACCEPTANCE

1. Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance. Operations managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented and tested.

2. The following controls should be considered:
   (A) performance and computer capacity requirements,
   (B) error recovery and restart procedures and contingency plans,
   (C) preparation and testing of routine operating procedures to defined standards,
   (D) agreed set of security controls in place,
   (E) effective manual procedures,
   (F) business continuity arrangements as required,
   (G) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end,
   (H) evidence that consideration has been given to the effect the new system has on the overall security of the organization, and
   (I) training in the operation or use of new systems.

3. For major new developments, the operations function and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

9.8 OPERATIONS AND FAULT LOGGING

1. Operational staff must maintain a log of their activities. Logs should include as

appropriate:
(A) system starting and finishing times,
(B) system errors and corrective action taken,
(C) confirmation of the correct handling of data files and computer output, and (D) the name of the person making the log entry.

2. Faults must be reported and corrective action taken. Faults reported by users regarding problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:
(A) review of fault logs to ensure that faults have been satisfactorily resolved, and
(B) review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized.

9.9 MANAGEMENT OF REMOVABLE COMPUTER MEDIA

1. Appropriate operating procedures must be established to protect documents, computer media (tapes, disks, cassettes, etc.), input/output data, and system documentation from damage, theft and unauthorized access. The following procedures should be followed:
(A) If no longer required, the previous contents of any re-usable media that are to be removed from the organization should be erased.
(B) Authorization should be required for all media removed from the organization and a record of all such removals maintained.
(C) All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.
(D) All procedures and authorization levels should be clearly

documented. **9.10 DISPOSAL OF MEDIA**

1. Formal procedures for the secure disposal of media should be established to minimize this risk. The following controls should be considered:
(A) Media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding or emptied of information for use by another application within the organization.
(B) The following list identifies items that might require secure disposal: (i) paper documents,
(ii) voice or other recordings,
(iii) output reports,
(iv) one-time-use printer ribbons,
(v) magnetic tapes,
(vi) removable disks or cassettes,

(vii) optical storage media (all forms and including all manufacturer software distribution media),
(viii) program listings,
(ix) test information, and

(x) system documentation.

(C) It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.

(D) Disposal of sensitive items should be logged where possible in order to ~~maintain an audit trail.~~

~~(E) Disposal of certain hardware must conform to the current EPA requirements or other relevant legislation in effect.~~

9.11 EXCHANGES OF INFORMATION AND SOFTWARE

1. Exchanges of information and software between organizations should be controlled and should be compliant with any relevant legislation.

2. Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit must be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

3. Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should include:
   (A) responsibilities for controlling and notifying transmission, dispatch and receipt,
   (B) procedures for notifying sender, transmission, dispatch and receipt, (C) minimum technical standards for packaging and transmission,
   (D) courier identification standards,
   (E) responsibilities and liabilities in the event of loss of information,
   (F) information and software ownership and responsibilities for information protection, software copyright compliance and similar considerations,
   (G) technical standards for recording and reading information and software, and (H) any special controls that may be required to protect sensitive items, such as cryptographic.

4. Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. As such, media being transported must be protected from unauthorized access, misuse or corruption.

9.12 PUBLICLY AVAILABLE SYSTEMS

1. Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations

in the jurisdiction in which the system is located or where trade is taking place. There must be a formal authorization process before information is made publicly available and the integrity of such information must be protected to prevent unauthorized modification.

2. Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures. Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:
   (A) information is obtained in compliance with any information protection legislation,
   (B) information input to and processed by, the publishing system will be processed completely and accurately in a timely manner,
   (C) sensitive information will be protected during the collection process and when stored, and
   (D) access to the publishing system does not allow unintended access to networks to which it is connected.

9.13 USE OF SYSTEM UTILITIES

1. Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Use of these system utility programs must be restricted and tightly controlled. The following controls should be considered:
   (A) use of authentication procedures for system utilities,
   (B) segregation of system utilities from applications software,
   (C) limitation of the use of system utilities to the minimum practical number of trusted authorized users,
   (D) authorization for ad hoc use of systems utilities,
   (E) limitation of the availability of system utilities, e.g. for the duration of an authorized change,
   (F) logging of all use of system utilities,
   (G) defining and documenting of authorization levels for system utilities,
   and 2. removal of all unnecessary software based utilities and system software.

9.14 MONITORING SYSTEMS ACCESS AND USE

1. Systems should be monitored to detect deviation from access control procedures and record system events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked.

2. Audit logs recording exceptions and other security-relevant events must be produced and kept for a period defined by the agency and within the mandate of

both federal and State legislation to assist in future investigations and access control monitoring. Audit logs should also include:
(A) user IDs,
(B) dates and times for log-on and log-off,
(C) terminal identity or location if possible,
(D) records of successful and rejected system access attempts, and
(E) records of successful and rejected data and other resource access attempts.

3. Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

4. Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be included are:
   (A) authorized access, including detail such as:
      (i) the user ID,
      (ii) the date and time of key events,
      (iii) the types of events,
      (iv) the files accessed, and
      (v) the program/utilities used.
   (B) all privileged operations, such as:
      (i) use of supervisor account,
      (ii) system start-up and stop, and
      (iii) I/O device attachment/detachment.
   (C) unauthorized access attempts, such as:
      (i) failed attempts,
      (ii) access procedure violations and notifications for network gateways and firewalls, and
      (iii) alerts from proprietary intrusion detection systems.
   (D) system alerts or failures such as:
      (i) console alerts or messages,
      (ii) system log exceptions, and
      (iii) network management alarms.

5. The result of the monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:
   (A) the criticality of the application processes,
   (B) the value, sensitivity or criticality of the information involved, (C) the past experience of system infiltration and misuse and
   (D) the extent of system interconnection (particularly public networks).

6. A log review involves understanding the threats faced by the system and the manner in which these may arise. System logs often contain a large volume of

information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

7. Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorized changes and operational problems including: (A) the logging facility being de-activated,
(B) alterations to the message types that are recorded,
(C) log files being edited or deleted, and
(D) log file media becoming exhausted and either failing to record events or overwriting itself.

9.15 CONTROL OF OPERATIONAL SOFTWARE

1. Control must be applied to the implementation of software on operational systems. To minimize the risk of corruption of operational systems, the following controls should be considered:
(A) The updating of the operational program libraries should only be performed by the nominated librarian upon appropriate management authorization.
(B) Operational systems should only hold executable code.
(C) Executable code should not be implemented on an operational system until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated.
(D) An audit log should be maintained of all updates to operational program libraries.
(E) Previous versions of software should be retained as a contingency measure.

2. Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Any decision to upgrade to a new release should take into account the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

9.16 ACCESS CONTROL TO SOURCE LIBRARY

1. In order to reduce the potential for corruption of computer programs, strict control must be maintained over access to program source libraries.
(A) Program source libraries should not be held in operational systems. (B) A program librarian should be nominated for each application.

(C) IT support staff should not have unrestricted access to program source libraries.
(D) Programs under development or maintenance should not be held in operational program source libraries.
(E) The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorization from the IT support manager for the application.
(F) Program listings should be held in a secure environment.
(G) An audit log should be maintained of all accesses to program source libraries.
(H) Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.
(I) Maintenance and copying of program source libraries should be subject to strict change control procedures.

9.17 CHANGE CONTROL PROCEDURES

1. The implementation of changes must be strictly controlled by the use of formal change control procedures to minimize the risk of system corruption. These formalized change controls must be enforced. They should ensure that security and control procedures are not compromised, that programmers are given access to only those units required for their work and that formal approvals are obtained. Changing application software can impact the operational environment. Whenever practical, application and operational change procedures should be integrated. These processes should include:
(A) maintaining a record of agreed authorization levels,
(B) ensuring changes are submitted by authorized personnel,
(C) reviewing controls and procedures to ensure they will not be compromised by the changes submitted,
(D) identifying all the software, databases and hardware that require change, (E) obtaining formal approval before work commences,
(F) ensuring the changes are carried out to minimize any possible disruptions, (G) ensuring the system documentation is current,
(H) maintaining version control on all updates,
(I) maintaining an audit trail of all change requests,
(J) ensuring that operational documentation and user procedures reflect the new environment, and
(K) ensuring that the changes are implemented without business disruption.

2. Test environments should be separated from development and production environments.

9.18 RESTRICTIONS ON CHANGES TO SOFTWARE

1. Modification to software packages must be discouraged and essential changes

controlled. Only when deemed essential, should the packages be modified. The following points should be considered:

(A) the possibility of controls and processes included in the base software being compromised,

(B) the necessity of obtaining the vendor's consent,

(C) the possibility of the vendor including the changes into the base offering, and

(D) the impact of incorporating these changes in future releases of the base software.

9.19 INTRUSION DETECTION SYSTEMS (IDS)

1. Network IDS utilize traffic analysis to compare session data against a known database of popular application attack signatures. On detection, the network IDS can react by logging the session alerting the administrator, terminating the session and even reconfiguring the firewall or router to block selected traffic

2. Host IDS compare application / internal service log events against a known database of security violations and custom policies. If a breach of policy occurs, the host IDS can react by logging the action alerting the administrator and in some cases stopping the action prior to execution.

3. Application-Level IDS rely upon custom applications to log unauthorized or suspect activity and / or produce an alert. An example of an Application-Level IDS would be a Web application which maintains its own internal user / password system. Attempts to circumvent this system would not be noticed by a Network IDS, or recorded by a Host IDS.

9.20 CONTROLS ON MALICIOUS SOFTWARE

1. Detection and prevention controls to protect against malicious software and appropriate user awareness procedures must be implemented. Protection against malicious software should be based on security awareness appropriate system access and change management controls. The following procedures should be implemented:

(A) compliance with software licenses and prohibiting the use of unauthorized software,

(B) protection against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken,

(C) installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis,

(D) regular reviews of the software and information content of systems supporting critical business processes—the presence of any unapproved files or unauthorized amendments should be formally investigated,

(E) verification of files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use,

(F) verification of any electronic mail attachments and downloads for malicious software before use—this check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization,

(G) assignment of responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks,

(H) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements,

(I) verification of all information relating to malicious software and ensure that warning bulletins are accurate and informative, and

(J) verification that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses.

2. Staff should be made aware of the problem of hoaxes and what to do on receipt of them. These controls are especially important for network file servers supporting large numbers of workstations.

9.21 FIREWALLS

1. Firewalls' functionality must be documented and detail how they manage security policy as applied to network traffic and how they maintain internal security.

2. System documentation must detail the following:
   (A) Purpose / Business rationale for the system
   (B) Services offered, including business rationale
   (C) Rationale for the choice of platform, operating system, components and configuration.
   (D) Adjacent or integrated systems.
   (E) Modifications to the default system software configuration
   (F) Installed software
   (G) Installed software configuration
   (H) Installed hardware
   (I) Installed hardware configuration
   (J) Support contracts
   (K) Software licenses
   (L) Hardware lease details
   (M) Procedures for shutdown, restart and recovery
   (N) System maintenance schedule

9.22 EXTERNAL FACILITIES MANAGEMENT

1. The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise,

damage, or loss of data at the contractor's site. Prior to using external facilities management services, the risks must be identified and appropriate controls agreed with the contractor, and incorporated into the contract.

2. Particular issues that should be addressed include:
   (A) identifying sensitive or critical applications better retained in-house, (B) obtaining the approval of business application owners,
   (C) implications for business continuity plans,
   (D) security standards to be specified, and the process for measuring compliance,
   (E) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
   (F) responsibilities and procedures for reporting and handling security incidents.

10.0 LEGAL REQUIREMENTS

1. All security related aspects of information processing may be subject to statutory or contractual security requirements. Each agency must be aware of their responsibilities as dictated by legislation and other legal commitments particularly as they apply to the information systems and practices required by the federal and state governments. All agencies should put in place the appropriate procedures to ensure compliance with legal considerations.

10.1 SOFTWARE COPYRIGHT

1. Proprietary software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be implemented: (A) publishing software copyright compliance procedures which define the legal use of software and information products,
   (B) maintaining awareness of the software copyright and acquisition procedures and giving notice of the intent to take disciplinary action against staff who breach them,
   (C) maintaining appropriate asset registers,
   (D) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.,
   (E) implementing controls to ensure that any maximum number of users permitted is not exceeded,
   (F) carrying out checks that only authorized software and licensed products are installed,
   (G) providing procedures for maintaining appropriate license conditions, and (H) providing procedures for disposing or transferring software to others.

10.2 PROTECTION OF INFORMATION

1. Important records of an organization must be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements as well as to support essential business activities. The time period and information content for retention may be set by federal and state laws or regulations.

2. Records should be categorized into record types, such as accounting records, database records, transaction logs audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures, should be kept securely and made available to authorized persons when needed.

3. Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with Manufacturer's recommendations.

4. Wherever electronic storage media are chosen, procedures to ensure the ability to access information (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

5. The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the organization.

6. To meet these obligations, the following steps should be taken within an organization:
   (A) Guidelines should be issued on the retention, storage, handling and disposal of records and information.
   (B) A retention schedule should be drawn up identifying essential record types and the period of time for which they should be retained.
   (C) An inventory of sources of key information should be maintained.
   (D) Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

10.3 PRIVACY OF PERSONAL INFORMATION

1. In many cases, legislation controls the processing and transmission of personal information (generally information on living individuals who can be identified from that information). Such controls impose responsibilities on those collecting, processing and disseminating personal information.

2. Controls must be applied to protect personal information in accordance with relevant legislation. Compliance with information protection legislation requires appropriate management structure and control. It is the responsibility of the owner of the information to ensure the information is protected and that there is awareness by all users of the information protection principles defined in the relevant legislation.

11.0 COMPLIANCE WITH SECURITY POLICY

1. Agencies must ensure that all security procedures within their area of responsibility are documented and carried out correctly. All areas within the organization may be subject to regular review to ensure compliance with security procedures and standards. These should include the following:
   (A) information systems,
   (B) systems providers,
   (C) owners of information and information assets,
   (D) hosting agencies of information and information assets, and
   (E) users.

2. Both the owning and hosting agencies should support regular reviews of the compliance of their systems with the appropriate security procedures, standards and any other security requirements. All variances must be documented.

APPENDIX A: GLOSSARY

Backup: A copy of files and programs made to facilitate recovery if necessary.

Business Continuity: The predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption of the normal business environment.

Business Recovery Strategy: The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption to the normal business environment has occurred.

Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures or disaster.

Critical Application: An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to, or modification of, the information in the application. A breach in a critical application might comprise many individual application programs and hardware, software and telecommunications components. Critical applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.

Disaster Recovery Plan: An information technology plan designed to restore operability of the target system, application, telecommunication, or computer facility after a major hardware or software failure or destruction of facilities.

Disruption: An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, equipment or facility damage or destruction, or corruption of files by accidental or malicious intent).

Distributed System: A distributed system is an interconnected set of multiple autonomous processing units, configured to exchange and process information to complete a single business function. To the user a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more accessible to users in different locations.

Environmental Considerations: Those physical or tangible factors that affect the performance of, or compliance with, a given procedure or process.

Facilities: Interconnected information resources that share common functionality. They

include hardware, software, information, information applications and communications.

Functional Considerations: Those process or procedure factors that affect

the performance of, or compliance with, a given function.

Hosting Agency: The Hosting State Agency has physical and operational control of the hardware, software, communications and data bases (files) of the owning Agency. The Hosting Agency can also be an Owner.

Hot Site: A fully operational off-site information processing facility equipped with hardware and system software to be used in the event of a disaster.

Incident: A malicious attack against an organization's IT systems. It is normally associated with cyber attacks but includes any unauthorized violation of policies and procedures.

Information: Any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

Intrusion Detection System: The function of an Intrusion Detection System (IDS) is to monitor and analyze captured activity data and issue alerts when unauthorized activity is detected. The functionality of the IDS must be documented as well as details on how the IDS discovers, filters and reports events based on guidelines set by security policy.

Local Area Network (LAN): A local area network (LAN) is a data communications network owned by a single organization. It can be as small as two PCs attached or can include hundreds of users and multiple servers.

Mainframe: A mainframe is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store most, if not all data in a central location rather than dispersing data among multiple machines as with distributed systems.

Owner: The Owner of the information is the State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

Risk Management: Risk management is the ongoing process of assessing, controlling and mitigating the risks to information systems and technologies. Risk management should prevent or reduce the likelihood of damage to its information resources through implementation of security controls to protect a system or technologies against natural, human and environmental threats. Risk management should encompass actions to reduce or limit the consequences of risks in the event they disrupt a system or technological component.

Security Representative: An individual designated by a state agency to approve user access, communicate security policies, procedures, guidelines and best practices to agency personnel, and report on all deviations to security policies, procedures, guidelines and best practices.

Server: A server is a computer that runs software to provide access to a resource or part of the network and network resources, such as disk storage, printers and network applications. A server can be any type of computer running a network operating system.

A server may be a standard PC or it can be a large computer containing multiple disk drives and a vast amount of memory that will allow the computer to process multiple, concurrent requests.

Service Level Agreement: A documented commitment on products, services or service levels to be provided. This must be agreed upon by the provider as well as the recipient and serves to manage expectations and monitor performance.

Shared Network: A network shared with third party or non-organizational users.

System: A generic term used for briefness to mean either a major application or a general support system.

Systems Access Authorization Request: Documented authorization for an individual's system access signed and approved by the requesting manager, the designated Security Representative and the Owner.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance and ultimately its disposal that instigates another system initiation.

Vetting: Verification of information or individuals associated with the process or task assigned.

Warm Site: An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

Web Site: A Web site is used for information dissemination on the Internet or an intranet. The Web site is created in Hypertext Markup Language (HTML) code that may be read by a Web browser on a client machine. A Web site is hosted on a computer (Web server) that serves Web pages to the requesting client browser. The Web server hosts the components of a Web site (e.g., pages, scripts, programs and multimedia files) and serves them using the Hypertext Transfer Protocol (HTTP). Web sites can present static or dynamic content. A Web site can be either internal to an organization (an intranet) or published to the public over the Internet.

Wide Area Network (WAN): A wide area network (WAN) is a data communications network that consists of two or more LANs that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable one LAN to interact with other LANs.

APPENDIX B: SAMPLE CRISIS TEAM ORGANIZATION

The following sample illustrates crisis team compositions insofar as skills mix required for the disaster recovery components. Alternates should be assigned for all critical

skills.

~~APPENDIX C: RESPONSIBILITY GRID~~

~~The following grid outlines the primary responsibilities **(in bold)** for all the security considerations listed in the Policy, Procedures, and Guidelines document. In addition,~~

~~the considerations are applied to the major components listed under disaster recovery. This does not preclude the fact that all State employees and agencies share in all responsibilities pertaining to information security.~~

~~Security Considerations~~	**Users**	**Own Agcy**	**Host Agcy**	Desktops	Servers	Web Sites	LAN	WAN	Dist. Sys.	Mainframe
~~Information Confidentiality~~	**x**	**x**	**x**	x	x	x	x	x	x	x
~~Information Content~~		**x**		x	x	x			x	x
~~Information Access~~		**x**	**x**	x	x	x				x
		x		x	x	x			x	x
~~Information Security~~			**x**	x	x	x	x	x	x	x
			x	x	x	x	x	x	x	x
~~Information Availability~~	**x**	**x**	**x**	x	x	x	x	x	x	x
~~Hosting Agency Security~~		**x**	**x**	x	x	x	x	x	x	
			x		x	x	x	x	x	x
~~Agency Security~~			**x**	x	x	x	x	x	x	x
			x	x	x	x	x	x	x	x
~~Incident Management~~			**x**		x	x	x	x	x	x
~~Event Logging and Monitoring~~		**x**	**x**	x	x	x	x	x	x	x
~~Risk Assessment~~	**x**	**x**		x						
	x	**x**	**x**	x			x	x		x
~~Risk Mitigation~~			**x**		x	x				x
			x		x	x	x	x	x	x
~~Staffing~~		**x**			x				x	
~~Awareness/Training~~		**x**	**x**					x		
			x	x	x	x	x	x		
			x		x	x	x	x	x	

	x		**x**	x	x				x	
~~Personal Computer Usage~~			**x**	x	x	x	x	x	x	
			x				x	x	x	
~~Email Usage~~			**x**		x		x	x	x	
	x		**x**	x					x	
~~Internet/Intranet Security~~			**x**	x	x	x		x	x	
			x	x	x	x	x	x	x	
~~Support Calls~~			**x**	x	x	x	x	x	x	
		x		x	x		x	x	x	
~~Password Resets~~		**x**	**x**		x	x	x	x	x	
		x	**x**		x	x	x	x	x	
~~Voice Mail Security~~		**x**	**x**		x	x	x	x	x	
		x	**x**		x	x	x	x	x	
~~Operations Center~~										
~~Operations Monitoring~~										
~~Back Up of Information~~										
~~Access Control~~										
~~Network~~										
~~Electronic Commerce Security~~										
~~Mobile Computing~~										
~~Remote Computing~~										
~~External Facilities~~										
~~Encryption~~										

~~Contingency Plan~~ ~~Disaster Recovery Plan~~ ~~Business Recovery Strategy~~										

Information Security Policies, Procedures, Guidelines

Security Considerations	**Users**	**Own Agcy**	**Host Agcy x**	Desktops	Servers x	Web Sites x	LAN x	WAN x	Dist. Sys. x	Mainframe x
~~Operating Procedures~~ ~~Operational Change Control~~ ~~Segregation of Duties~~ ~~Separation of Development & Operational Facilities~~ ~~Systems Planning & Acceptance~~ ~~Capacity Planning~~ ~~Systems Acceptance~~ ~~Fault Logging~~ ~~Management of Removable Computer Media~~ ~~Disposal of Media~~ ~~Exchanges of Information & Software~~ ~~Publicly Available Systems~~ ~~Use of System Utilities~~ ~~Monitoring Systems Access & Use~~ ~~Control of Operational Software~~ ~~Access Control to Source Library~~ ~~Change Control Procedures~~ ~~Restrictions on Changes to Software~~ ~~Intrusion Detection Systems (IDS)~~ ~~Controls on Malicious Software~~ ~~Firewalls~~ ~~External Facilities Management~~ ~~Software Copyright~~ ~~Protection of Information~~ ~~Privacy of Personal Information~~ ~~Compliance with Security Policy~~			**x**		x	x	x	x	x	x
			x		x				x	x
			x		x				x	x
			x		x				x	x
			x	x	x		x	x	x	x
			x		x	x	x	x	x	x
			x		x				x	x
		x	**x**		x				x	x
	x	**x**	**x**	x	x				x	x
		x	**x**		x		x	x	x	x
		x			x	x				x
			x		x				x	x

		x	**x**	x	x	x	x	x	x	x
			x		x				x	x
			x		x					x
			x		x				x	x
			x		x				x	
			x		x				x	
			x		x				x	
			x		x				x	
		x	**x**	x	x				x	
			x	x	x	x	x	x	x	
	x	**x**	**x**	x	x				x	
	x	**x**	**x**	x	x	x	x	x	x	
	x	**x**	**x**	x	x				x	
	x	**x**	**x**	x	x	x	x	x	x	

APPENDIX D: CONTINGENCY PLAN CONSIDERATIONS

Considerations	**Portables**	**Servers**	**Web Sites**	**LAN**	**WAN**	**Dist. Sys**	**Mainframe**
Maintain an up to date inventory of hardware and ~~software.~~ Standardize hardware, software, and peripherals. Coordinate with security policies and procedures. Backup and storage of critical information offsite.	x	x				x	x
Ensure interoperability among system components. Implement redundancy in critical system components. Use uninterruptible power supplies.	x	x				x	x
Document system and application configurations Document environmental	x	x	x	x	x	x	x
	x	x				x	x

requirements.	x	x				x	x
Backup and storage of information and applications ~~offsite.~~	x	x		x	x	x	x
Implement fault tolerance in critical system components. Replicate information.	x	x		x	x	x	x
Document Web site.	x	x		x	x	x	x
Code and program the Web site uniformly.	x	x	x	x	x	x	x
Consider contingencies of supporting infrastructure. Implement load balancing.		x		x	x	x	
Coordinate with incident response procedures. Document the network.	x	x				x	x
Coordinate with vendors.		x				x	x
Identify single points of failure.		x				x	
Monitor the network.							x
Institute service level agreements			x				
Consider a hot site or reciprocal agreement.			x				x
			x			x	x
			x				
			x			x	
				x	x		
		x		x	x	x	
		x		x	x		
				x	x		
		x		x	x		
		x			x	x	

APPENDIX E: PROCEDURES AND ACCEPTABLE USE

APPENDIX E, SECTION 1. COMPUTER (CYBER) INCIDENT REPORTING PROCEDURES

Purpose: The purpose of this procedure is to provide a computer incident reporting and

response process that the State of Oklahoma will employ in the event of an intrusion to or an attack on government computer systems. This reporting and response process provides a coordinated approach to handling incidents across all levels of government. The intention of this coordinated process is to minimize or eliminate the propagation of an event to other computers and networks. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. Centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions.

Scope: This procedure applies to all agency, authority, board, department, division, commission, institution, institution of higher education, bureau, or like government entity of the executive branch of the state government.

Definitions: A computer or cyber incident is an event violating an explicit or implied computer security policy. The following types of events or activities are widely recognized as being in violation of a typical security policy. These activities include but are not necessarily limited to:

- Attempts or activities interpreted by the agency as legitimate attempts to gain unauthorized access to a system or its data;
- Unwanted disruption or denial of service;
- Unauthorized use of a system for the transmission, processing or storage of data;
- Storage and/or distribution of child pornography;
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent; and
- Cyber-terrorism is the unlawful and deliberate use, modification, disruption or destruction of computing resources to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

The Oklahoma CyberCommand maintains partnerships of federal, state, and local law enforcement agencies within the state of Oklahoma to aggressively address cyber threats and crime in a coordinated manner.

Procedures: It is the responsibility of all state employees to report suspected computer incidents as quickly as possible. The ultimate goals, regardless of incident, are the protection of assets, containment of damage, and restoration of service.

The reported cyber incident will be coordinated by the Oklahoma CyberCommand with the Oklahoma Office of Homeland Security, Information Analysis/Infrastructure Protection Division (OHS IA/IPD) and the Oklahoma State Bureau of Investigation (OSBI).

Primary support for an incident response will be at the request of the OHS IA/IPD and OSBI and be provided by the Oklahoma CyberCommand.

NOTIFICATION

- Initial notification of a cyber incident should be made to the Lead Technology Position (Chief Information Officer, IT Director, Manager or Administrator) of the affected state agency or office. The affected state agency or office will make the appropriate cyber incident notification to the Oklahoma CyberCommand and law enforcement.
- Initial Notification of this cyber incident should be made through the OMES IS Service Desk at 405-521-2444 or toll free at 1-866-521-2444. Additional details will be provided via email to joe.mcintosh@omes.ok.gov, michael.toland@omes.ok.gov, and jason.lawson@omes.ok.gov. The Oklahoma CyberCommand will provide all necessary notification and coordination to the Supervisory Special Agent of the Computer Intrusion Squad at the Federal Bureau of Investigation (FBI) and the Electronic Crimes Special Agent at the United States Secret Service.

RESPONSE ACTIONS

- Once an incident has been reported, the incident specifics such as time, date, location, affected systems, and the nature and consequence of the incident will be obtained.
- An initial response team and the affected agency will respond to the incident. ■ The focus will be on identifying the origins of the incident and apprehending those responsible. If the initial response team suspects the incident to be a cyber terrorism incident, the FBI Joint Terrorism Task Force (JTTF), and Oklahoma Office of Homeland Security will be notified. Based on continuing analysis and assessments, the initial response team will focus on remediation of mission critical information and telecommunications systems, as well as those systems whose loss would constitute an immediate threat to public health or safety.
- The Oklahoma CyberCommand shall apprise the State Chief Information Officer, and the person(s) responsible for Information Technology at the agency, affected by the computer incident of the progress of the investigation to the extent possible.

AGENCY RESPONSIBILITIES

Employee:

- To adhere to this procedure and any other state or agency security policies and procedures.
- To report all actual computer incidents to their supervisors and to the appropriate business or technical area manager who in turn will notify the Oklahoma CyberCommand through the OMES IS Service Desk at 405-521-2444. This number is monitored 24 x 7 x 365.
- To fully cooperate with any subsequent investigation of a computer incident by sharing a report with relevant information to comply with applicable laws and regulations.

Agency:

- To communicate this procedure to all employees.
- To provide periodic security awareness training to agency employees. ■ To implement procedures to ensure compliance with the initial notification procedures described in this policy.

It is the responsibility of each agency to identify procedures, whereby its IT staff will determine if a computer or cyber incident has taken place and if it should be reported using this process.

The Incident Reporting Form used by Gartner shall include at a minimum:

1. Facts of the Incident, such as date, time, description, how the security incident was detected;
2. Impact to services provided to the client and/or Client data affected;
3. Root cause of the incident (when known); and
4. Description of any actions taken by Gartner or any actions Gartner will take to minimize the likelihood of recurrence.

~~The Incident Reporting Form is attached.~~ ~~INCIDENT REPORTING FORM~~

~~Note: This form is required for all suspected or actual privacy or security breaches. This form will be sent in confidence to the state Incident Response Center.~~

~~Type of Incident (Privacy, Security, Virus, etc)~~		~~Incident Date~~
~~Individuals Providing Report (Full Name)~~		~~Report Date~~
~~Phone Division~~		~~Supervisor/ Manager~~

~~**Incident Description**~~ ~~*Complete all information known at the time of the report preparation. Supervisors and investigators will complete other items on the report as results become available.*~~	
~~Incident Description~~	
~~Information Compromised (or at risk)~~	
~~Information Systems Compromised (Hardware, software, sites): include host name(s), host IP address(es), & primary purpose of host machine(s)~~	

~~Location of the Incident or Systems: include street, city, state, zip~~	
~~Other affected hosts/sites / information (include 3rd parties, local public health, other state agencies, etc.)~~	
~~Damage or observations resulting from attack (Impact on Operations to include downtime, costs, other damages)~~	
~~Summary of Incident Investigation Results~~ ~~(i.e., number of hosts attacked, how access was obtained, how was attack identified, was an incident response organization contacted prior to submission of this report, etc.)~~	
~~Identify the agency or agencies which received a report concerning this incident.~~	

~~Report Completed by: Information Reviewed by:~~

~~Date: Date:~~

APPENDIX E, SECTION 2. INCIDENT MANAGEMENT

PROCEDURE OVERVIEW

The Office of Management and Enterprise Services Information Services (OMES IS) monitors the State of Oklahoma network backbone, primarily focusing on the segments used by OMES IS and by the agencies to which OMES IS provides services. When abnormal and excessive traffic are revealed, further investigation is conducted. OMES IS will notify the agencies involved when events are observed and recorded that clearly indicate questionable activities. Examples of such activity include events indicating the possible presence of computers compromised by unknown attackers or computers actively being used to scan and perhaps exploit other cyber assets belonging to State or other entities. These activities are indicative of a serious and potentially critical intrusion and as such are considered a possible criminal act. The agency will be given a period of

time to evaluate their environment and report the results of their evaluation. T he confirmed security ~~suspected~~ incident involving OMES IS data is ~~not~~ reported within 24hours upon discovery of the incident ~~and depending on the suspected severity of the observed activity, OMES IS can submit a report on behalf of the agency, after notifying the agency Director. Agencies can submit, update and modify reports for their agency, regardless of who submits them.~~
These procedures will be used together with the Computer (Cyber) Incident Reporting Procedures contained in Appendix E, Section 1. In this section, a computer or cyber incident is defined as "an event violating an explicit or implied computer security policy". The goal of these procedures is to define the process for reporting and responding to "significant" incidents, whether they originate externally or internally.

When any intrusion occurs, it is the responsibility of the agency to analyze and validate each incident, documenting each step taken. When the agency believes that an incident has occurred, they shall perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the agency to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. The agency shall assume the worst until thorough analysis concludes the root cause(s) of the incident and steps have been taken to mitigate or remediate the vulnerabilities and the results of any exploit(s).

Below is the list of recommended actions for the agency to follow.

Recommended Actions:

1. Report this incident to the Oklahoma CyberCommand, following the procedures in Appendix E: Section 1. Computer (Cyber) Incident Reporting Procedures of the statewide Information Security Policy, Procedures, and Guidelines document.
2. The initial incident response activities are the responsibility of the agency experiencing the event. Whenever possible, it is imperative to preserve evidence in case of a criminal investigation. This means avoiding actions that would alter

or destroy physical evidence that resides in memory and/or on the disk drives of suspected host computers.

3. The first priority must always be to protect state assets and ensure the continuity of critical services. So the statements in #2 above must be weighed in light of the criticality, urgency and perceived risk(s) to the state. If the impact and/or risk to the state are significant, then those factors override the importance of preserving data. If the agency is able to make this decision, it must be based on the results gathered during steps #4 and #5 below. 4. Analyze the computer(s) in question to determine if any sensitive data may have been exposed, lost or damaged. Oklahoma statute (74 O.S. 3113.1) defines sensitive data to include "personal information", consisting of the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: a) social security number; b) driver license number; or c) account number, credit or debit card number, in combination with any required security

code, access code, or password that would permit access to the financial account of an individual. This statute also specifies that if such information is reasonably believed to have been, acquired by an unauthorized person, then disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

5. Conduct an analysis of the network traffic flows between the compromised computers) and other inbound and/or outbound computer(s), including all known assets that communicate with the primary suspect devices involved in questionable activities; also, do not initiate communication with unknown assets or IP addresses of any kind, including use of the "ping command" — such activity will alert the intruder that we are aware of their presence, which may produce undesired results. If the agency is not able to perform this analysis, please notify OMES IS for assistance.
6. The Oklahoma CyberCommand will evaluate the reported incident and determine if a criminal investigation is needed. If not, the incident will be turned over to the agency and/or OMES IS to continue the response activities.
7. The remaining actions will depend on the decisions made by the agency based on the results of the analysis above that set the expectations for the overall impact of the event on critical agency assets and services.

The following describes the computer incident response team organization and roles. These procedures define the agency's roles and the roles of the state and/or other agencies where appropriate.

INCIDENT RESPONSE TEAM ORGANIZATION

Response to significant cyber incidents is guided by the agency's Incident Response Team **(IRT).** Although first responders may be general IS or IT staff and can include other agency staff with prior approval, the IRT provides overall response guidance. This team's

first effort during an incident is to take control of the situation with the intent of mitigating potential damage to the agency or its customers.

It is the IRT's responsibility to:

- Manage the incident response process
- Defend against attacks and prevent further damage from occurring when an incident does occur
- Implement improvements that prevent attacks from reoccurring
- Report the outcome of any security incidents to the Information Security Officer or Cyber Security Representative, who will report the incident using established state procedures

The agency will appoint a qualified IRT with current members listed in the following table, if available.

IRT Groups IRT Functional	Members* IRT Member Roles	
State Agency Agency Director Decisions related to assets & services		
	IT/IS Director	Technology decisions & alternatives
	Security Manager/Admin	Response coordinator & documentation
	Network Manager/Admin	Address network related questions/issues
	Server Manager/Admin	Address server questions/issues
	Workstation Manager/Admin	Address workstation questions/issues
	Operations Manager/Admin	Address operational questions/issues
	Applications Manager/Admin	Address application questions/issues
Office of Management and Enterprise Services	**IS Director**	Notify Agency Director if issues are identified Coordinate with OKOHS & OSBI to enforce the statewide minimum information security and internal control standards
	Information Security Officer	Coordinate IRT activities with agency & OCCA Coordinate IRT support for agencies requesting or requiring assistance

Information Security Policies, Procedures, Guidelines events Coordinate/support non-criminal IRT activities with agency & other group team members

Information Security Admin Document & clarify monitored

	Network Manager/Admin	Coordinate/support OMES IS customer equipment

Oklahoma Office of Homeland Security	**(OKOHS) Agency Director**	Enforce the statewide minimum information security and internal control standards

IRT Groups IRT Functional	Members* IRT Member Roles	
	Information Analysis / Infrastructure Protection	Enforce the statewide minimum information security and internal control standards
Oklahoma State Bureau of Investigation	**(OSBI) Division Director**	Enforce the statewide minimum information security and internal control standards
	Computer Crimes Unit	Enforce the statewide minimum information security and internal control standards
Oklahoma Cyber Crime Alliance Partners (OCCA)	**Office of Homeland Security**	Assess incident reports for prosecutable value and investigate and gather evidence when necessary
	OSBI	Assess incident reports for prosecutable value and investigate and gather evidence when necessary
	FBI	Coordinate resources & investigations
	OMES IS	Maintain incident reporting system

***Note**: It is recognized that multiple functions may be handled by the same incident response team member(s), depending on how each agency is organized. If the agency uses a third party to perform any of these functions, then that group will be responsible for providing the support necessary to identify and address the requirements or issues involved.

INCIDENT RESPONSE PROCEDURES

Each agency will develop an IRT Plan based on the FBI's National Infrastructure Protection Center guidelines, which are now part of the Office of Domestic Preparedness/Department of Homeland Security and US-CERT (United States Computer Emergency Readiness Team). These guidelines are segmented into three phases:

Triage
Information Security Policies,
Procedures, Guidelines

Phase I: Detection, Assessment and

Phase II: Containment, Evidence Collection, Analysis and Investigation, and

Mitigation Phase III: Remediation, Recovery and Post-Mortem

Checklists for agency incident response are provided in the following tables. The original checklists have been updated to reflect statewide policy and statute requirements.

The IRT or other staff will generally respond to incidents by following these steps in the order given. Every step, however, may not apply to each incident, and the IRT shall use discretion and experience when applying these steps to actual incidents. The checklist steps below are initiated at the point in time when a potential incident is detected and declared.

Phase I activities are designed to control risk and damage and are particularly critical to the successful response. These Phase I tasks shall be conducted by technical staff or by the IRT.

Phase I **Detection, Assessment and Triage**	
Step I -1	**Document all aspects of the incident.** Documentation is one of the most critical success factors for incident response. Documentation is electronic or handwritten and need not be well-organized initially. The purpose of this step is to capture everything that occurs in detail, especially names, times and events as they actually occurred. For the initial incident handler, a notebook and pen may be adequate. Screen shots and digital pictures are used when possible to capture information completely and unambiguously. Detailed documentation continues by the IRT throughout the response.
Step I -2	**Notify the IRT leader and, on a need-to-know basis only, other relevant entities.** In this step all appropriate contacts and only appropriate contacts shall be made. Incidents may have legal, human resources and public relations implications and shall not be disclosed to anyone without a specific need-to-know. Care shall be taken not to communicate at any time using potentially compromised data or voice systems.

Step I -3	**Protect evidence.** During this step, evidence is not collected but care is taken to preserve the integrity of potential evidence by guarding against: (a) destruction of evidence through established processes like re-use of backup media, system use or hard-disk wiping; and (b) destruction or tainting of evidence through incident handling actions (logging onto affected systems, etc). If deliberate destruction is considered likely (e.g., by a suspect or attacker), then more aggressive actions may be required to preserve evidence (i.e., removing systems from the network, placing evidence in safe storage, etc.)

Step I -4 **Determine if an actual incident has occurred.** Based on available data, establish whether or not an incident has occurred. This action shall consider the previous steps so that actions such as logging on to affected systems, sending out broadcast e-mails and other similar activities shall be avoided. An event is verified by reaching one of three conclusion-action pairs:

1. verified and proceed
2. undetermined and proceed
3. refuted and terminate (this conclusion must be fully documented and verified)

Phase I
Detection, Assessment and Triage

Step I -5	**Notify Appropriate Personnel.** Once the incident is validated (or undetermined), the appropriate internal and external personnel shall be notified immediately. These contacts follow the communication plan established by the IRT and shall include technical and management staff, human resource, public relations, legal, as well as appropriate external contacts, including the OCCA if they have not been already.
Step I -6	**Determine Incident Status.** This step determines whether the attack / incident remains active or has ceased; and if it has ceased, if it likely to resume. If this step will cause only minimal delay to communications in Step I-5, then activities in Step I-6 may actually occur prior to Step I-5.
Step I -7	**Assess Scope.** Activities in this step determine which and how many systems and data are potentially affected, including whether or not compromised system(s) are the end target or part of a more distributed attack on other systems.
Step I -8	**Assess Risk.** This activity determines agency risk based on the incident activity, scope assessment and potential impact.

Step I -9	**Establish Goals.** This step determines appropriate business goals to guide the response. For instance, the agency may determine that the incident has potential regulatory impact which may guide response activities. The agency realizes that accommodating all business goals may be impossible (i.e., protecting confidential data and maintaining resource availability may conflict).
Step I -10	**Evaluate response options.** Based on information gained in the previous steps, this activity identifies and evaluates appropriate options to meet the goals determined in Step I-9.
Step I -11	**Implement Triage.** Implement the agreed to strategy and option(s) identified in the previous step.
Step I -12	**Escalation and handoff.** At this point, evidence is preserved, appropriate communications made, containment activities executed, and goals identified as possible. If the IRT has not been handling the incident directly, at this point, primary incident response is transferred to the IRT.

Phase II activities are intended to: address containment; stabilization of the environment; evidence collection and analysis; evaluate impact to operations; and determine if interim mitigation actions are available and need to be implemented. These Phase II tasks shall be conducted by the OCCA, where deemed appropriate, by technical staff and/or by the IRT.

Phase II

Containment, Evidence Collection, Analysis and Investigation and Mitigation

(Note: The OCCA must be contacted and participate, if criminal activity is suspected.)

Step II - 1	**Containment.** Since triage actions are often executed in a crisis environment, the first step in Phase II is to validate that the containment and related triage activities are effective.

Step II - 2	**Re-assess.** Once a relatively stable state is established, the scope, risk assessment and response goals are re-analyzed and re-validated. The following questions are generally addressed during this step: • How did the incident happen? When? What is the verified scope or depth of the incident? • Was there any activity after the initial incident? • Who was the source of the attack? • What are the immediate and future recommendations for response? Reestablishing the specific goals of the investigation may alter the response approach (i.e., trap and trace, disconnect systems, active or passive searching, etc.)
Step II - 3	**Collect evidence.** Evidence collection involves the identification and capture of data relevant to an incident investigation. Evidence is collected in a way that the integrity of the evidence is ensured and a solid chain of custody is maintained. All evidence relevant to the investigation is captured and may include evidence from systems not actually affected by the incident (e.g., firewall logs, IDS logs, DHCP logs, mail servers, physical access logs, etc.). It's possible some evidence collection activities may involve outside entities (e.g., ISPs web hosting services, etc), legal, human resource and other agency resources are recruited as necessary to ensure proper processes are followed.
Step II - 4	**Analyze Evidence.** If the OCCA determines that criminal prosecution is appropriate, the appropriate law enforcement agency will conduct a criminal investigation.
Step II - 5	**Develop Hypotheses and Verify.** Previous activities formulate hypothetical answers to questions identified in Step II-2. Each hypothesis is substantiated by evidence, but answers are often not absolute requiring qualitative interpretation with reasoned conclusions. It may be necessary to collect additional evidence to support a given conclusion.

EXECUTION VERSION SW1026 Gartner (002)

Final Audit Report 2024-06-03

Created:	2024-06-03
By:	Courtney Templeton (courtney.templeton@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAzj0T04NEkrD0-0GsQb9wn-5rXZiVzgk6

"EXECUTION VERSION SW1026 Gartner (002)" History

Document created by Courtney Templeton (courtney.templeton@omes.ok.gov)
2024-06-03 - 7:13:27 PM GMT

Document emailed to kristin.ghanem@gartner.com for signature
2024-06-03 - 7:16:00 PM GMT

Email viewed by kristin.ghanem@gartner.com
2024-06-03 - 8:17:55 PM GMT

Signer kristin.ghanem@gartner.com entered name at signing as Kristin Ghanem
2024-06-03 - 8:30:44 PM GMT

Document e-signed by Kristin Ghanem (kristin.ghanem@gartner.com)
Signature Date: 2024-06-03 - 8:30:46 PM GMT - Time Source: server

Document emailed to Joe McIntosh (joe.mcintosh@omes.ok.gov) for signature
2024-06-03 - 8:30:51 PM GMT

Email viewed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
2024-06-03 - 10:03:29 PM GMT

Document e-signed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
Signature Date: 2024-06-03 - 10:04:28 PM GMT - Time Source: server

Agreement completed.
2024-06-03 - 10:04:28 PM GMT