A DRAFT Statement of Work for

State of South Carolina - Division of State Information Technology

B&CB
SC Budget and Control Board

DIVISION OF STATE
INFORMATION TECHNOLOGY

Enterprise Information Security Program Assistance

5 November 2012

Engagement: 330012768

Gartner.

Gartner, Inc.
10 Glenlake Parkway, Suite 390
Atlanta, Georgia 30328
Telephone: +1 770-913-2376
Facsimile: +1 770-913-2310
gartner.com

Gartner®

5 November 2012

Jimmy Earley
Chief Information Officer
State of South Carolina - Division of State Information Technology
SC Budget and Control Board
DSIT
4430 Broad River Rd
Columbia, SC 29210

Telephone: +1 803-896-0222
Facsimile: +1 CCfax
Email: jearley@cio.sc.gov

Engagement: 330012768
Re: Statement of Work for Enterprise Information Security Program Assistance

Dear Mr. Earley:

Gartner, Inc. (Gartner) is pleased to provide the State of South Carolina - Division of State Information Technology (DSIT) with this Statement of Work for Enterprise Security Program Assistance.

The program we have outlined in this SOW brings senior, highly skilled, and government industry experienced support to DSIT from Gartner experts in the field of information security and risk management. Our program support is designed to empower your organization as DSIT brings leadership to security and risk management statewide for the State of South Carolina.

Our programmatic approach focuses on understanding the current information security environment from strategic enterprise perspective and developing a plan for improving the information security capabilities within the State of South Carolina, including initiation of governance council, defining a statewide information security framework, and developing a roadmap for improving the State's ability to secure and protect its information assets over the next few years; providing a mechanism for rapidly conducting agency security and risk management assessments in a consistent, coordinated, and quality manner; establishing a statewide security and risk management program office and reporting mechanism based on agency-level assessments; and providing ongoing security and risk management decision support for DIST, Inspector General, and the information security governing council.

Gartner recognizes that DSIT is looking for a partner to help build a holistic enterprise security program; a program that can satisfy the State's responsibilities to protect sensitive information, including citizen, financial, health, and other sensitive personal information.

Gartner is in a unique position to partner with DSIT. For this engagement, both our advisory and research based expertise will be engaged to provide independent and objective program support and assessments. Gartner has no vendor or technology bias and does not stand to benefit from any subsequent implementation work that may result from the agency assessments. Our goal is to partner with DSIT to startup and operate the Enterprise Security Program, to conduct security and risk management assessments, facilitate statewide reporting, and to provide decision support and research – a proven approach which we are using with another large state at this very time. We have a proven methodology, based on our leading practice Reference Architecture, used with other states in similar situations which will help DSIT achieve its long term goals, improve statewide standards, and establish some quick wins.

Our offer is valid for 30 days from the submission date of this Statement of Work.

If this Statement of Work represents your requirements, please sign the Authorization Page and return the entire Statement of Work to Jeff Perkins via email to Jeff.Perkins@gartner.com or fax to +1 770-913-2310.

Please contact me at +1 770-913-2376 or via e-mail at Jeff.Perkins@gartner.com if you have any questions regarding this Statement of Work. Thank you for this opportunity. We look forward to assisting DSIT with this key initiative.

Sincerely,

Jeff Perkins
Managing Partner, State of Local Government, Gartner Consulting

cc: Jim Phillips, Senior Account Executive

Attachment

Table of Contents

1.0 The Gartner Advantage 2
1.1 Executive Overview 2
1.2 Our Understanding and Business Context 3
1.3 Project Scope and Objectives 3
1.3.1 Project Scope 3
1.3.2 Objectives 4
1.4 Gartner Approach 5
1.4.1 Program Schedule and Timeline 8
1.5 Why Gartner? 10
1.6 Unique Gartner Qualifications 10
1.6.1 Gartner Value 10
1.6.2 Corporate Experience and Past Performance 12
1.6.3 Relevant Research Notes 13
2.0 Statement of Work 15
2.1 Project Tasks 15
2.1.1 Detailed Approach 15
2.1.2 Base Period Project Schedule 34
2.2 Gartner Project Team 35
2.2.1 Proposed Project Team 35
2.3 Gartner Project Management Life Cycle 36
2.4 Assumptions 37
2.5 Pricing and Invoicing 38
2.5.1 Base Period (Years 1 and 2) Pricing and Invoicing 38
2.5.2 Extension Options Pricing for Years 3, 4 and 5 40
2.5.3 Validity Period 41
2.5.4 Period Of Performance 42
2.5.5 Changes to Scope 42
2.5.6 Authorization 43
2.5.7 Further Assurances 44
3.0 Attachments 46
Project Team Biographies 46

The Gartner Advantage

1.0 The Gartner Advantage

1.1 Executive Overview

Gartner is pleased to submit this Statement of Work to State of South Carolina - Division of State Information Technology (DSIT) to provide critical Enterprise Information Security Program Assistance. This SOW outlines the ongoing decision support and guidance services that Gartner will provide to DSIT related to information security and risk management by leveraging Gartner's world class advisory and research services.

The goal of this SOW is to outline Gartner's approach for assisting DSIT and the State of South Carolina in understanding and defining what is needed to improve the State's ability to secure and protect its information assets. This includes defining what information security means at the enterprise and at the department / agency level; identifying how information security will be governed in the future; and developing a program plan for improving the State's ability to secure information. The also SOW describes Gartner's proposed support for DSIT and the Office of the Inspector General, in developing these key concepts and program plan as noted above.

The SOW proposes to immediately perform comprehensive risk assessments, resulting in improvement roadmaps, for two organizations, DSIT and the Department of Revenue (DOR). The DSIT assessment is important to understand how enterprise information technology services and its related security posture fits with other department and agencies. The DOR assessment is important because it complements the immediate and tactical security review that Mandiant is providing as a result of the October 2012 security breach at DOR. The DOR security assessment and roadmap is different than what we understand the tactical and forensic assistance provided by Mandiant, in that the Gartner independent and objective assessment will look strategically and comprehensively across all relevant people, process, and technology issues related to information security and risk to better understand the security posture at DOR, the subsequent risks DOR faces, and the practical steps DOR can take to minimize risks given their constraints.

In addition, the SOW provides a mechanism for departments and agencies to engage Gartner to perform information security and risk assessments for each requesting department or agency, which will result in an improvement roadmap for each participating department or agency. Gartner assumes that a minimum of fifteen (15) such assessments will be performed over a two-year period or sooner. The SOW also proposes to provide assistance in initiating and operating an enterprise program management office to oversee and report on the effect that the individual assessments have on the statewide security posture (without attribution to specific departments or agencies) and to build enterprise security capabilities within DSIT. Finally, to support all of the activities above, the SOW proposes to provide access to Gartner Research for key State participants for access to existing guidance through written research, advice from Gartner's leading research analyst team, training and webinars to help bring awareness and educate State employees, department leaders, information technology leaders, and security professionals on information security topics.

In summary, the SOW outlines a practical and proven approach for improving the information security capabilities at the enterprise and department and agency levels, which when properly executed will result in significantly lower security risks for the State of South Carolina. We will provide immediate and expert support for DSIT and the Inspector General as they develop a plan t improve information security capabilities for the State. Gartner's thought-leading information security research and reference architecture will be a foundational element to our holistic approach. In addition to our expertise in information security, Gartner brings unparalleled independence and objectivity which means Gartner will provide practical advice that departments, agencies, and the administration can trust – we do not sell information security solutions nor provide implementation services for these solutions. Our proven approach ensures information security is addressed in a coordinated, consistent, and quality manner across the State, resulting in a much improved security posture for the State of South Carolina.

1.2 Our Understanding and Business Context

In recent months the State of South Carolina, like many governmental and commercial organizations, has experienced security incidents involving the exposure of sensitive and confidential data. These security incidents have lead to the loss or exposure of sensitive and confidential data, places the State at risk, and calls into question the policies, procedures, technologies and awareness of information technology security statewide.

As legislated, DSIT is the State's central authority on statewide information technology matters and, in part, is responsible for the leadership, policies, and procedures for information technology security statewide as is required in S.C. Code Ann. Section 1-11-435 (Critical Information Technology Infrastructure Protection Plan), which directs DSIT to develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of critical data.

Toward this end, DSIT is seeking assistance in establishing an enterprise security program aimed at strengthening security statewide by defining a statewide plan for improving information security, providing mechanisms for assessing security and risk management at the agency level, and providing statewide and agency security and risk management decision support. Gartner proposes to support DSIT in the following areas:

- Establishing an Enterprise Security Program and Program Plan,
- Conducting agency-level security and risk management assessments,
- Providing ongoing security and risk management decision support; and,
- Initiating and operating an enterprise security and risk management program office and reporting framework to enable the State to measure and track the improvements in the security posture of the State of South Carolina overall.

1.3 Project Scope and Objectives

1.3.1 Project Scope

The Project Scope of this engagement includes:

- Strategic assessment of information security and risk management practices currently in place from a statewide perspective, including people, process, and technology considerations (i.e., organizational authority, policy, governance, security framework, etc.)
- Definition of the to-be state enterprise information security program, including strategic context and drivers, program vision and objectives, stakeholders, governance mechanisms, program scope, security framework, program approach and key tasks, timeline, required resources, and risks
- Two (2) comprehensive information security and risk management assessments for the Division of State Information Technology (DSIT) organization and Department of

Revenue, which will assess the effectiveness of the people, processes and technologies currently in place

- Fifteen (15) information security and risk management assessments for Executive Branch departments (a comprehensive assessment is already being conducted with the Department of Health and Human Services)
- Ongoing guidance, insight, decision support and leading practices for DSIT and State agencies related to information security and risk management from technical architectural and governance standpoints
- Assistance in initiating and operating a program management office to manage and track statewide progress toward the enterprise information security program plan and objectives
- Optional additional standard information security and risk management assessments for State departments as requested (priced per assessment)

1.3.2 Objectives

Under DSIT's governance and oversight, Gartner will accomplish the following objectives for this engagement:

- Assess the current enterprise information security capabilities (people, process, and technology) and support DSIT and the Inspector General in developing an enterprise information security program plan to improve the information security capabilities across the State
- Conduct comprehensive information security and risk management assessments for the Division of State Information Technology (DSIT) organization and Department of Revenue by:
  - ❑ Document the current-state baseline IT environment as it relates to security and information protection, including the people, processes, and technologies
  - ❑ Identify the business drivers and future-state requirements for ensuring the security of the sensitive information environment and processes, and that define the desired, future-state information protection posture
  - ❑ Identify the relevant vulnerabilities and opportunities for improvement by conducting gap and maturity analyses between the identified current-state security environment and industry leading practices as defined by Gartner Research and the Gartner Reference Architecture; risks will be defined in context of the Department-specific business drivers and requirements identified as part of the baseline security environment
  - ❑ Define the recommendations, including options and alternatives, for improving program maturity and addressing the identified vulnerabilities as defined by the gaps; recommendations will be based on industry leading practices, industry trends, and what other similar organizations are doing to deploy similar risk mitigations; recommendations will be developed using the Gartner Reference Architecture and related Gartner research
  - ❑ Develop a strategic deployment roadmap depicting the sequence and dependencies of actions required for achieving the desired information protection posture
- Conduct fifteen (15) information security and risk management assessments for Executive Branch departments in a quality, consistent, and coordinated manner

  - ❑ Follows same approach as with the comprehensive assessment, although is based on smaller set of mandatory assessment items (versus an expanded set of assessment items which is used for departments that have experienced a significant security incident as is the case with Department of Revenue incident report on October 26, 2012)

- Provide ongoing guidance, insight, decision support and best practices for DSIT and State agencies related to information security and risk management in form of written research-based guidance, access to information security and risk management experts, and planned communication and training events for leadership and staff through webinars and focused expert presentations

- Initiate and operate an Enterprise Security Program Management Office (ESPMO) to oversee security and risk management assessment activities, coordinate all events and activities of Gartner resources (advisors, consultants, analyst visits, webinars, conference calls, etc.), coordinate and facilitate assessment initiation and communication, and be the single point of contact for ongoing reporting related to enterprise security and risk management (reporting will be done from a statewide perspective, without attribution to specific departments or agencies)

- Optionally, as requested, conduct additional standard information security and risk management assessments for departments and agencies in a quality, consistent, and coordinated manner. Day-to-day management of assessments including schedule definition, timelines, deliverables, governance, priorities, and project status communications will be provided by the individual Gartner Consulting assessment teams in conjunction with the individual department points-of-contact

- Develop Statewide Enterprise Security and Risk Management Report in order to describe the program achievements on a quarterly basis (reporting will be done from a statewide perspective, without attribution to specific departments or agencies)

1.4 Gartner Approach

The Gartner approach to accomplishing the objectives outlined in this SOW is divided into three distinct segments of work:

- **Work Segment 1 (Program Support Services)** – Assist in defining the enterprise approach and plan for improving information security and risk management capabilities statewide, which includes defining enterprise information security and risk management governance. Establish and operate an Enterprise Security Program Management Office (ESPMO), including developing and facilitating a statewide security and risk management reporting process

- **Work Segment 2 (Security and Risk Management Assessments)** – Conduct two (2) comprehensive security and risk management assessments, one for Division of State information Technology and one for Department of Revenue. Conduct an additional fifteen (15) standard information security and risk management assessments for Executive Branch departments over two-year period or less. Optionally conduct additional standard information security and risk management assessments for departments as requested.

- **Work Segment 3 (Enterprise Security and Risk Management Decision Support Services)** – Provide ongoing DSIT and agency guidance and decision support services related to security and risk management using Gartner's research and analyst support capabilities.

For Work Segment 1 –Program Support Services, Gartner proposes to support DSIT and the Inspector General, in defining the enterprise approach and plan for improving information security and risk management capabilities for the State of South Carolina. This segment will begin by looking strategically at the information security and risk management practices currently in place from a statewide perspective, including people, process, and technology by reviewing the existing concepts such as organizational authority, policy, governance, and the existing security framework. Taking into account the findings from the current environment review, Gartner will help define the "to be" state enterprise information security program, including strategic context and drivers, program vision and objectives, stakeholders, governance mechanisms, program scope, security framework and architecture, program approach and key tasks, timeline, required resources, and risks.

Also, in Work Segment 1, Gartner will facilitate and coordinate the creation and operation of an IT Security Advisory Council chaired by a designated enterprise security leader Under this leader's direction and oversight, the council will be a place for agencies to have input into the creation of statewide security governance, as well as enterprise security and risk management processes and policies. It is expected that the council will have representation from State agencies. Having an IT Security Advisory Council will provide a forum to facilitate baseline security education and awareness to security, IT, management and audit personnel.

Gartner will work with the security leader and the IT Security Advisory Council to establish processes that IT security officials must own including:

- security governance
- policy management
- awareness and education
- identity and access management
- vulnerability management
- threat management
- incident response
- disaster recovery and business continuity

Work Segment 1 also includes the initiation and operation of Enterprise Security Program Management Office (ESPMO). The ESPMO will coordinate the activities and responsibilities of Gartner employees related to enterprise security, coordinate and facilitate assessment initiation and communication, provide information security and risk management decision support, and facilitate the recurring statewide enterprise reporting methodology. Gartner will assign a program management team or individual to help oversee and contribute to the responsibilities of the ESPMO. Day-to-day management of assessments including schedule definition, timelines, deliverables, governance, priorities, and project status communications will be provided by the individual Gartner Consulting assessment teams in conjunction with the individual department points-of-contact.

For Work Segment 2 - Security and Risk Management Assessments, Gartner will conduct agency-level information security and risk management assessments by leveraging Gartner's extensive Reference Architecture, frameworks, models and tools in the information security and risk management and identify and access management areas. Agency assessments are available in two primary forms: a standard assessment and a more in-depth comprehensive assessment. The comprehensive assessment is designed for the DSIT organization and any organization that has had a recent security incident such as in the Department of Revenue incident reported on October 26, 2012).

The Gartner Comprehensive Security Assessment encompasses a “deep dive” analysis of the current environment and supporting program to identify the major threats and vulnerabilities facing the client. Approximately 1,200 individual items are included in this assessment of the client’s environment, and typically requires ten-to-fourteen (10 to 14) weeks to complete. Through the Gartner Standard Security Assessments, Gartner performs a “health check” of the agency or department’s information protection environment and supporting security program against a set of industry-leading-practice requirements, evaluating the current state and level of maturity of the security architecture. Approximately 150 elements are evaluated as part of the “health check” of the client environment. A Gartner Standard Security Assessment typically requires approximately six (6) weeks to complete.

Work Segment 2 within this SOW includes two separate comprehensive assessments, one for DSIT and one for Department of Revenue. Also for Work Segment 2, each participating State agency will individually undergo a standard security and risk management assessment that covers a broad range of people, process and technology issues related to security and risk.

The people and process areas to be addressed by both the comprehensive and standard assessments include:

- Understand organizational IT security governance including (but not limited to) structure, information ownership and classification, training and awareness, incident response, disaster recovery/contingency planning, levels of authority and influence, and regulatory (State, Federal, local, and industry) compliance requirements
- Understand how the organization operates and what makes it succeed or fail in terms of security
- Identify key threats, vulnerabilities, and consequences associated with information and information technologies deployed in the department
- Understand where the business value lies and the impacts of information corruption, loss of availability, loss of control, and leakage involving different elements of IT systems and infrastructure
- Understand the components, technologies and operational methodologies comprising the information systems and their operation within the organization

The technical areas to be addressed by the assessments include:

- *Application Security* – What frameworks and approaches are used to ensure security protections in software applications?
- *Availability of Information* – What approaches should the department use to protect the availability of electronic information in the resource layer as part of overall disaster recovery and business continuity?
- *Change Management with Assurance:* How should the department control changes in their hardware, software, and supporting infrastructure while maintaining suitable and appropriate information assurance?
- *Confidentiality of Information:* What technical approaches should the department use to protect the confidentiality of electronic information in the resource layer?
- *Endpoint Admission:* What approaches should the department use to control how client endpoints gain admission to zones and connect to resources?

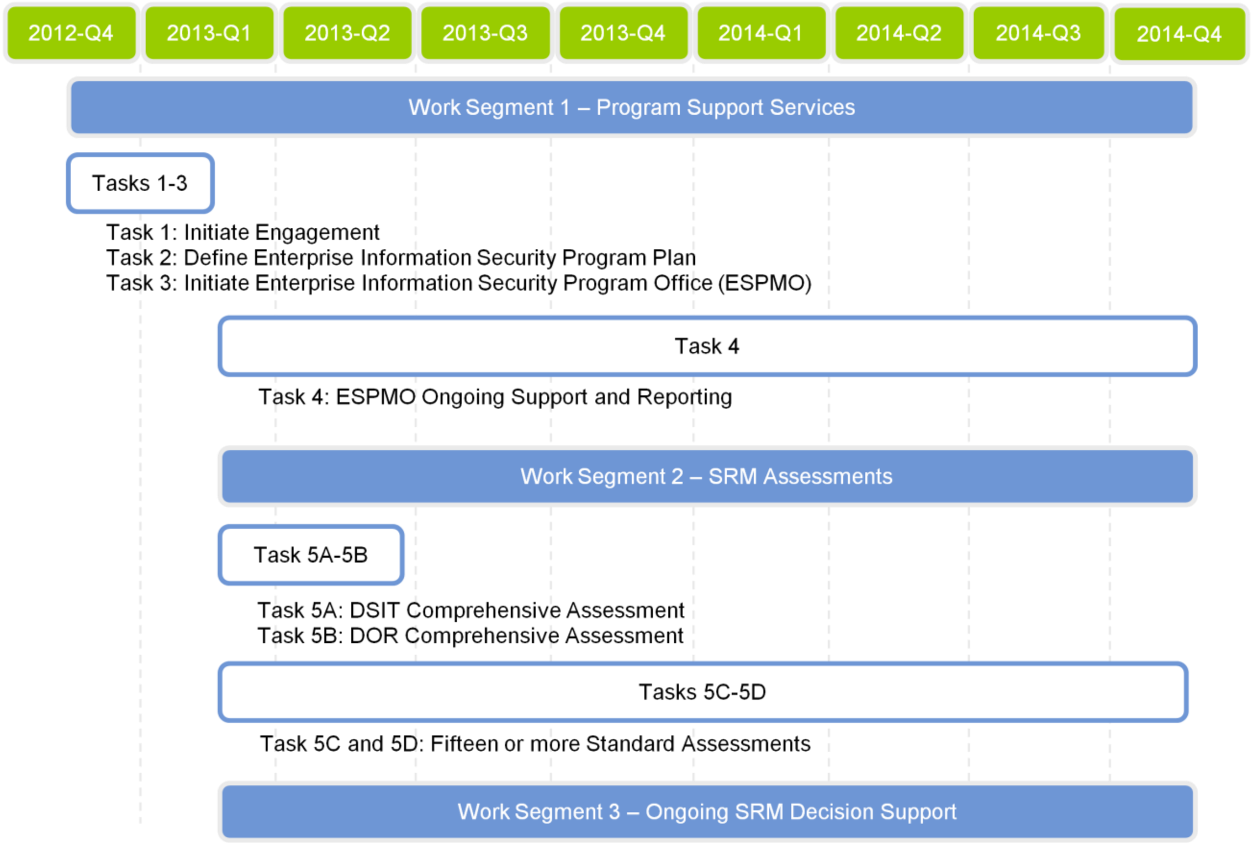
- *Governance*: How is the department IT security function organized and governed, and what is the scope of the IT security program?
- *Host & Mobile System Security Choices:* What management and protection postures should the department take with regard to host system and mobile device security?
- *Identity and Access Management (IAM):* What approaches (including directory services, provisioning, authentication and authorization, etc.) are used by the department to enable the management of identities and control the access of users and services to IT and information resources?
- *Integrity of Information:* What technical approaches should the department use to protect the integrity of electronic information in the resource layer?
- *Malicious Software:* What mechanisms and approaches should the department use to mitigate malicious software (e.g., unwanted viruses, spyware, and Trojan horses)?
- *Monitoring and Intrusion Detection:* How should the department detect and respond to security incidents on their network?
- *Network Perimeters:* What network perimeter mechanisms should be used by the department to enforce zone boundaries and protect sites, systems, and users across a distributed infrastructure?
- *Network Zones:* What zones of trust should the department establish to protect their information technology (IT) resources on communications networks?
- *Physical Security*: What processes and approaches should be used to protect information and the physical assets related to the organization's IT capabilities?
- *Public Key Infrastructure (PKI) and Encryption*: When should encryption mechanisms be used to protect information, and, when necessary, how should the department plan and deploy tiered public key infrastructure systems to support security?
- *System Placement:* How should the department place systems in security zones?
- *Vulnerability Management:* How should the department manage and remediate data, software and configuration vulnerabilities of the resource layer?

For Work Segment 3 –Security and Risk Management Decision Support Services, Gartner will provide DSIT and State agencies with a unique and robust set of research and analyst based services that provide select agency leadership and staff (as identified by DSIT, agency leadership, and the IT Security Advisory Council) direct access to Gartner's published research, leading practices, analysts, and supporting programs to raise awareness of security and risk management, provide models for establishing controls, and gaining insight and information into best practices and lessons learned. At DSIT's discretion, Gartner will provide a number of workshops, webinars and conference calls to help establish baseline knowledge of security and risk management practices for state agencies.

1.4.1 Program Schedule and Timeline

The schedule in Figure 1 below reflects a high-level time line for the Enterprise Information Security Program Assistance services from Gartner. The proposed services with run over a period of 24 months and can be extended per the SOW options reflected in this SOW. In addition to the base program services outlined in Segments 1, 2 and 3, Gartner has also estimated three one year extension options that, if exercised, will extend the program support that Gartner provides to DSIT.

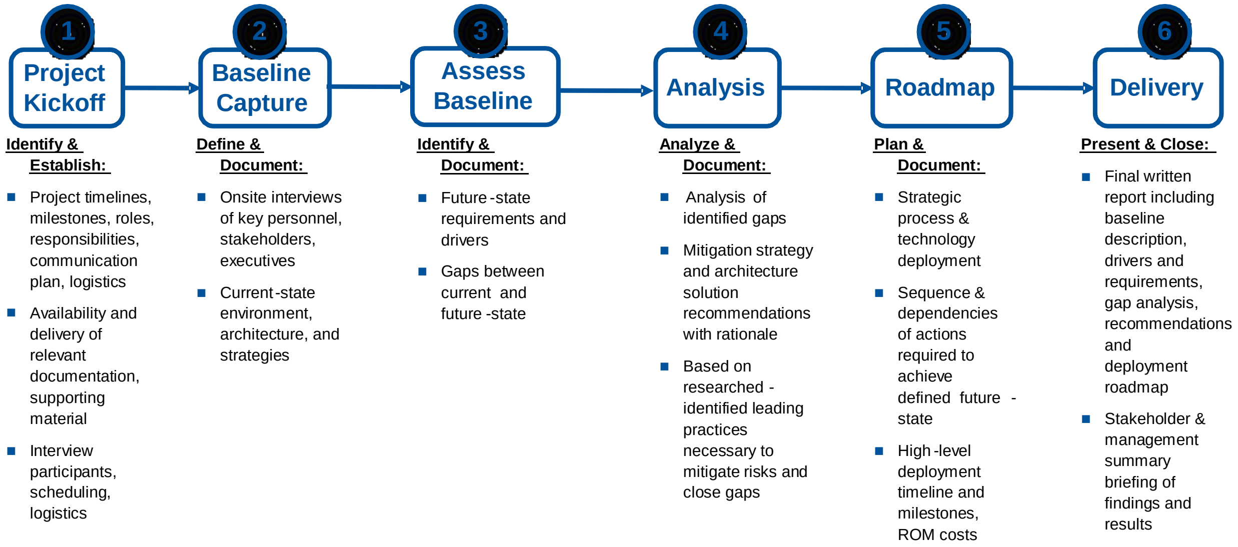
Figure 1. Gartner Proposed Calendar Year Timeline


2012-Q4
2013-Q1
2013-Q2
2013-Q3
2013-Q4
2014-Q1
2014-Q2
2014-Q3
2014-Q4
Work Segment 1 – Program Support Services
Tasks 1-3
Task 1: Initiate Engagement
Task 2: Define Enterprise Information Security Program Plan
Task 3: Initiate Enterprise Information Security Program Office (ESPMO)
Task 4
Task 4: ESPMO Ongoing Support and Reporting
Work Segment 2 – SRM Assessments
Task 5A-5B
Task 5A: DSIT Comprehensive Assessment
Task 5B: DOR Comprehensive Assessment
Tasks 5C-5D
Task 5C and 5D: Fifteen or more Standard Assessments
Work Segment 3 – Ongoing SRM Decision Support

1.4.2 Agency Assessment Approach

As described in Work Segment 2 and further detailed in Figure 2 below, Gartner will conduct work activities and tasks with participating State agencies and provide them with an individual security and risk management assessment, recommendations, and roadmap. The results of these agency assessments will be appropriately leveraged to facilitate an overall standardized statewide reporting mechanism on Enterprise Security and Risk Management. Regardless of the type of assessment (Comprehensive or Standard), Gartner uses the same high-level approach that includes the following tasks and activities:

Figure 2. Process for Conducting Individual State Agency Security & Risk Management Assessments in Segment 2



1 **Project Kickoff**

Identify & Establish:

- Project timelines, milestones, roles, responsibilities, communication plan, logistics
- Availability and delivery of relevant documentation, supporting material
- Interview participants, scheduling, logistics

2 **Baseline Capture**

Define & Document:

- Onsite interviews of key personnel, stakeholders, executives
- Current-state environment, architecture, and strategies

3 **Assess Baseline**

Identify & Document:

- Future-state requirements and drivers
- Gaps between current and future-state

4 **Analysis**

Analyze & Document:

- Analysis of identified gaps
- Mitigation strategy and architecture solution recommendations with rationale
- Based on researched-identified leading practices necessary to mitigate risks and close gaps

5 **Roadmap**

Plan & Document:

- Strategic process & technology deployment
- Sequence & dependencies of actions required to achieve defined future-state
- High-level deployment timeline and milestones, ROM costs

6 **Delivery**

Present & Close:

- Final written report including baseline description, drivers and requirements, gap analysis, recommendations and deployment roadmap
- Stakeholder & management summary briefing of findings and results

1.5 Why Gartner?

The cornerstone of the Gartner Approach is that our solutions are research-based, industry-focused and benchmark-enabled, and our advisory engagements deliver a comprehensive, consistent, and quality perspective that takes into account agency requirements, alignment, maturity and investment. Existing Gartner research and benchmark material, combined with the unique Gartner Security and Risk Management Reference Architecture, which is highlighted below, will be the foundation upon which the content for the Enterprise Information Security Program Assistance engagement will be delivered.

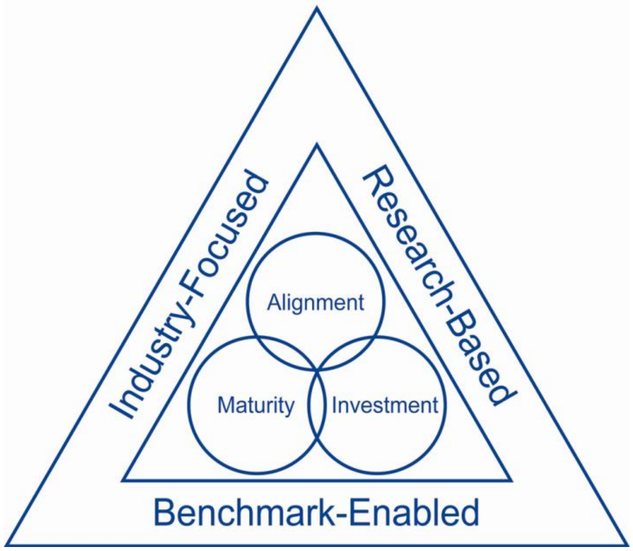
Gartner's Security and Risk Management Reference Architecture is an industry leading set of best practices that assist organizations with identifying and capitalizing on improvement opportunities related to security and risk management. The Decision Points that comprise the Reference Architecture identify the set of typical requirements encountered for an enterprise IT security architecture, future considerations, etc., and recommend tuned, architectural approaches to satisfy the set of requirements. The Reference Architecture is designed to provide proven architectural approaches given any number of organization considerations and constraints.

1.6 Unique Gartner Qualifications

1.6.1 Gartner Value

There is a reason that Gartner is quoted an average of 70 times per week in more than 30 leading business publications. There is a reason that more than 70% of the *Fortune* 1000 and 75% of the Global 500 support their key technology decisions with Gartner insight. And, there is a reason that our clients in more than 12,400 distinct organizations worldwide trust their organizations to Gartner. The reason is simple: Gartner delivers value to our clients every day. As shown in Figure 3 below, the cornerstone of the Gartner Value is that our solutions are research-based, industry-focused and benchmark-enabled, and our Consulting engagements deliver a comprehensive view that takes into account alignment, maturity and investment.

Figure 3. Gartner's Unique Value



Gartner will deliver value for DSIT, as demonstrated by the proof points in the following table.

Table 1. Gartner Value Proof Points

Gartner Value for DSIT	Proof Points
Gartner Consulting Is Based On Gartner Research Gartner created the IT Research industry 33 years ago, and our reputation speaks for itself. Gartner Research is the only IT research informed by both the technology end user and provider's perspectives. We use our research as the basis for our Consulting solutions, methodologies and tools; and, we leverage our research and our industry leading analysts, as needed, throughout our Consulting engagements. So, when our clients buy Gartner Consulting, they are buying Gartner Research.	■ Gartner Research has more than 810 analysts, including 20 analysts relevant to this engagement. ■ Our analysts are dedicated to conducting and reporting on research, which is what gives them the availability to conduct more than 290,000 one-to-one client interactions per year. ■ Security is a focus of Gartner Research, with more than 100 relevant notes published in the previous year alone. ■
Gartner Consulting Solutions Are Enabled By World-Class Benchmark Databases Our support leads to defensible business decisions because it is driven by our industry-leading benchmark data. We are the pioneers in IT benchmarking, and our database is the broadest, deepest and most up-to-date in the industry. With our benchmark data, we drive quantitative, measurable savings. Use of our benchmarking database and approach typically identifies more than double the savings identified through less rigorous methodologies.	■ Clients improve business performance by benchmarking their spending and best practices against our IT performance repository, the largest in the industry, drawing on 5,500 IT benchmarks a year. ■ Gartner has provided IT benchmarking services for more than 33 years, longer than any of our competitors. We are the founder of benchmark industry standards such as Total Cost of Ownership.
Gartner Consulting Support Is Industry Focused and Client Specific	■ Gartner has a dedicated Consulting organization for the SLG market

Gartner Value for DSIT	Proof Points
State and Local Government (SLG) is one of our focus areas of investment for Research and Consulting. We understand the business context and therefore the key IT enablers. Our analysts and consultants in more than 85 countries understand the industry trends and best practices, as well as local regulatory and environmental challenges, and we apply this knowledge to our Consulting support. Gartner will also apply the lessons learned from our experience supporting DSIT.	■ This Consulting organization focuses on specific IT-related issues that affect the state and local government entity's information services effectiveness.
Gartner Consulting Looks At The Entire Business Problem We understand that every successful strategic decision must encompass three key areas: ■ Alignment with Priorities, Benefits and Objectives ■ Investment, including Cost/Income Ratios, Divesting in Poor Performing Areas, and Investing to Maximize Results ■ Maturity of Process, Governance, Sourcing These three cornerstones are the basis of our approach to every Gartner Consulting engagement in order to ensure a balanced, comprehensive view of the business problem at hand.	■ Gartner's vast knowledge of the entire SLG landscape assists customers in formulating strategies that are balanced with appropriate investment and effectiveness.
Gartner Is Independent and Objective Our advice is trustworthy and credible because we maintain strict objectivity and independence. Our strategic recommendations are driven by what is best for our clients, and not what is best for Gartner or any other company.	■ We have no preferred hardware or software vendors. ■ We do not perform implementation work so we are not concerned with downstream opportunities.

1.6.2 Corporate Experience and Past Performance

Overview of Corporate Experience

Gartner has conducted more than 1,000 relevant engagements worldwide. The following descriptions represent but a small sample of this experience:

- Conducted statewide and agency specific comprehensive security assessments at the State of Oregon, State of Texas, State of Michigan and State of California, among others.
- Developed the security and access management architecture for the DOE/National Nuclear Security Administration (NNSA). Design included identification of authoritative sources of user security clearance data, directory integration, web access management, federation with collaborative laboratories and sites and Kerberos authentication integration. Also provided vendor recommendations, staffing recommendations, procurement and deployment cost estimates and project phasing recommendations.
- Designed state government electronic signature solution for the State of Alaska Revenue Board for citizenry tax and permanent fund dividend submission, including

participation in drafting new state statute in support of federal E-Sign and state UETA digital/electronic signature technology.

- Designed high-level security and access management architecture for a large public utility organization (natural gas, electric and raw materials mining). Design included potential vendors, cost estimates and recommended phasing. Further assisted in vendor evaluations and recommendations and was primary contributor to detailed design consisting of data mappings, flows, workflows and user management, delegated administration and self-service.
- Conducted the detailed design of a global directory services infrastructure for a large, multi-national automaker conducting business on two continents. Design included support for employees, contractors, dealers, suppliers and customers. Provided in-depth requirements gathering for directory schema and managed schema design for entire project.
- Developed Draft Department of Treasury Public Key Infrastructure (PKI) Architecture, Certificate Policy (CP), Certificate Practice Statements (CPS), and working documents analyzing the Federal PKI (FPKI) Bridge CA architecture as well revocation and trust domain architecture alternatives.
- Designed directory services architecture to support a global PKI implementation for a large, multi-national credit card company. Design included publishing certificates and CRLs to an existing LDAP directory infrastructure as well as to new certificate repositories for use by end users, servers and network devices.

Client Reference Details Provided Upon Request

1. State of Oregon, Department of Administration & Information Services
2. National Nuclear Security Administration
3. State of Texas, Department of Information Resources

1.6.3 Relevant Research Notes

We will also leverage Gartner Research, as needed, throughout the engagement. Following is a small sample of recent research that is relevant to this initiative.

Table 2. Relevant Research Notes Summary

- Decision Point for Encryption; written by Ramon Krikken and Dan Blum; 2012
- Information Security Architecture Model; written by Eric Maiwald; 2012
- Network Intrusion Detection & Response; written by Trent Henry; 2012
- The Shared Responsibility of Data Governance, Information Protection, and Controlling Sprawl; written by Trent Henry and Ian Glazer; 2012
- Risk Assessment Methodologies: A Comparison; written by Trent Henry and Mario de Boer; 2012
- *A Systematic, Comprehensive Approach to Information Security, written by Blum, 2010*
- *Security Governance for the Enterprise, written by L. Cohen, 2009*
- *An Objectives-based Assessment Framework for Security Solutions, written by Maiwald, 2010*

Statement of Work

2.0 Statement of Work

2.1 Project Tasks

2.1.1 Detailed Approach

The following Gartner Task Descriptions table provides a detailed description of all tasks and steps of the engagement with its associated deliverables.

The base period of services for years 1 and 2 are reflected in Work Segments 1, 2 and 3 in the table below. The tasks described in the sections below are designed to accomplish the objectives as stated in the Scope and Objectives section of this proposal. The individual steps described within Work Segment 2 - Task 4: Conduct Assessments, are meant to show the repeatable steps that will be executed during each agency's standard SRM assessment.

Also detailed below are the tasks and deliverables for each of three one-year extension options for DSIT. The extension options are designed to continue the Enterprise Security Program with DSIT progressively assuming more responsibilities for the tasks and deliverables to complete the remaining South Carolina state agencies. With the exception of decision support services, these extensions assume a progressive reduction in Gartner support for the Program Management and Security Assessment Support with Gartner serving in a supporting advisor role commencing in year 3.

Table 3. Gartner Task Descriptions

Work Segment 1. Program Support Services	
Task 1. Initiate Engagement	***Deliverable(s) and Time Frame***
Objective: ■ Work closely with DSIT to set the foundation for a successful engagement that is delivered on time, within budget and meets DSIT's objectives. ■ Introduce the overall Program to key stakeholders from both DSIT and agencies across the State that will benefit from this Program ■ Define objectives and expectations of the Program and begin to enhance DSIT's position in the State around security initiatives and programs. ■ Introduce approach, communication and high level schedule of Program **Activities performed by Gartner:** ■ Prepare Program approach and overview materials ■ Work with DSIT in preparing Kickoff materials ■ Gartner will hold a kickoff meeting with DSIT to ensure understanding of the project objectives, scope, milestones, roles, responsibilities and required resources for Gartner and DSIT. Gartner will also discuss anticipated risks and mitigation plans, based on lessons learned from past experiences. Gartner will also	**Deliverable(s):** ■ Program Kickoff & Kickoff Materials **Time frame:** ■ Week 1

begin to gather any relevant background material from DSIT. **DSIT responsibilities:** ■ Assign senior resources to the Program Office to actively participate in all communication, scheduling and presentation efforts ■ Work with Gartner in preparation of Program Kickoff materials ■ Prepare and introduce communication plan to the agencies ■ Ensure attendance at kickoff meeting by Project Sponsor, Project Manager and other key stakeholders, as determined prior to kickoff.	
Task 2. Define Enterprise Information Security Program Plan	***Deliverable(s) and Time Frame***
Objective: ■ Assess strategic context and current environment with respect to enterprise information security within the State ■ Develop holistic program plan for improving information security capabilities statewide, including strategic context and drivers, program vision and objectives, stakeholders, program scope, security framework, program approach and key tasks, timeline, required resources, and risks ■ Define initial mechanisms for governing information security across the State **Activities performed by Gartner:** ■ Review current materials and environment for enterprise information security ■ Interview key stakeholders for context and explanation of current environment ■ Work with preliminary governance body to provide guidance on desired enterprise future state posture for information security ■ Support DSIT and the Inspector General in defining program plan for improving enterprise information security capabilities ■ Document strategic context and drivers, program vision and objectives, stakeholders, program scope, security framework, program approach and key tasks, timeline, required resources, and risks as part of program plan ■ Share industry leading practices for enterprise information security governance ■ Define what decisions must be made and identify plan for establishing decision authority for information security	**Deliverable(s):** ■ Strategic Enterprise Current State Assessment ■ Enterprise Program Plan ■ Program Governance Definition **Time frame:** Weeks 1 through 8

DSIT responsibilities: ■ Provide materials and access to interviewees to facilitate current state review ■ Identify and ensure participation from governing body for program plan definition ■ Participate in development of program plan and initial enterprise governance definition ■ Approve program plan and initial enterprise governance definition	
Task 3. Initiate Enterprise Security Program Management Office	***Deliverable(s) and Time Frame***
Objective: ■ To develop the ESPMO charter and baseline parameters for execution and ongoing management ■ Establish agency grouping and prioritization ■ Develop preliminary program schedule and establish methods to manage assessment efforts ■ Develop format and content of Statewide Security & Risk Management Reporting and Decision Support - to be informed by individual agency assessments and reflect an overall State of South Carolina Security Posture ■ Establish repeatable processes to manage the overall program and projects for timeliness, reporting, outcomes and results. **Activities performed by Gartner:** ■ Interview key stakeholders, including DSIT leaders to help define the ESPMO Charter ■ Analysis to align expectations, needs and gaps to Program outcomes and results ■ Establish communication plan requirements – internal to DSIT and to other agencies ■ Develop status reporting methods and templates ■ Develop statewide SRM reporting format, requirements and measurements ■ Develop program management work-plan and resource plan ■ Prepare schedule of assessments by agency or grouping and prioritization ■ Determine and initiate scheduling of resources to perform assessments **DSIT responsibilities:** ■ Validate communication plan for each agency to prepare them for assessments ■ Identify and select state agencies that will receive SRM assessments under this SOW and develop a list of	**Deliverable(s):** ■ ESPMO Charter ■ Agency Assessment Groupings & Organization ■ Program Management Work-plan ■ Program Governance ■ Baseline Program Plan and schedule ■ Enterprise Statewide SRM Reporting and Decision Support Framework ■ Program Communications Plan **Time frame:** Weeks 6 through 10

participating South Carolina agencies with contact names, addresses and key agency information ■ Actively participate in Program Office for coordination, scheduling and execution of assessments	
Task 4. Provide Ongoing Enterprise Security Program Management Office Support And Reporting	***Deliverable(s) and Time Frame***
Objective: ■ Support day-to-day the Enterprise Security Program Management office functions ■ Central role to provide leadership support and to coordinate program management efforts of Gartner, including the agency SRM assessments, Gartner Research Analyst scheduling, workshops, web seminars, etc. ■ Coordination and communication amongst all agencies engaged in security assessments ■ Communication and scheduling of assessments ■ Single point of contact for questions/clarifications on the overall Program ■ Facilitation and support in developing the State of South Carolina statewide enterprise reporting on security and risk management ■ Consolidated view of the overall Program for updates, status reporting and progress **Activities performed by Gartner:** ■ Manage the resourcing, scheduling and work activities of the agency SRM assessments ■ Work alongside DSIT in producing the Statewide Enterprise Report, updated quarterly, on SRM and reflecting the “state of the state” ■ Facilitate quarterly workshop with DSIT leadership to provide status of program and discuss “State Security Report Card” ■ Communication with State stakeholders on status, progress and updates on findings **DSIT responsibilities:** ■ Timely review of status reports in order to help closely manage expectations and schedules of the Program. ■ DSIT will retain fiduciary responsibilities related to management and decision making ■ Work alongside Gartner in producing the Statewide Enterprise Report, updated quarterly ■ Participate in quarterly workshops to provide feedback and support to the program	**Deliverable(s):** ■ Decision support on Security and Risk Management ■ Bi-weekly status reports ■ Statewide Enterprise Security Reporting (updated quarterly) ■ Final Statewide Enterprise Security Report Card reflecting a view on the “South Carolina Security Posture” (at conclusion of Program) ■ Coordinate web seminars, workshops and/or analyst calls **Time frame:** 21.5 months (duration of the Program)

■ Actively participate in reviewing "State Security Posture" documentation ■ Actively assist in the coordination of Gartner events (non-assessment related) ■ Shared program management responsibility with Gartner throughout the duration of the Program	
Segment 2. Security and Risk Management (SRM) Assessments	
Task 5. Conduct Agency Security and Risk Management Assessments	***Deliverable(s) and Time Frame***
Objective: ■ Gartner will perform comprehensive assessment each for Division of State Information Technology and Department of Revenue ■ Gartner will perform standard assessments for 15 (fifteen) Executive Branch departments ■ Optionally Gartner will perform standard assessments for other departments as requested **Activities performed by Gartner:** ■ Steps 1 – 6 as defined below for each Agency **DSIT/Agency responsibilities:** ■ Communicate schedule for execution of assessments with individual agencies ■ Agencies' active involvement during the assessment of their particular environment	**Deliverable(s):** ■ Defined for each Step of the assessment **Time frame:** ■ Ten to Fourteen (10 – 14) weeks per comprehensive assessment ■ Six to ten (6 – 10) weeks per standard assessment
Step 1: Individual Assessment Kickoff	*Deliverable(s) and Time Frame*
Objective: ■ Work closely with each agency/department to set the foundation for a successful engagement that is delivered on time, within budget, and meets each agency/department's objectives. ■ Refine the project schedule and expectations from those established in this Statement of Work (SOW). **Activities performed by Gartner:** ■ Conduct a kickoff meeting via teleconference with each agency/department to establish and ensure understanding of the project objectives, scope, schedule and milestones, roles, responsibilities, communication plan, and required resources for Gartner and each agency/department. ❑ Additional conference calls may be used to supplement the kickoff meeting as necessary to complete the necessary communication and information transfer.	**Deliverable(s):** ■ Agency specific kickoff meeting materials ■ Agency draft project schedule ■ Agency draft project plan ■ Communications Plan ■ Interview questions, participant list, schedule, and related travel logistics information ■ Pre-interview survey **Time frame:** ■ One (1) week **Relevant Information and Supporting Material (not all of these may exist):** ■ Existing information regarding strategies, governance, architecture,

■ Discuss anticipated risks and mitigation plans, based on lessons learned from past experience. ■ Gartner will gather any relevant background material from each agency/department, as well as logistics for onsite project activities including the information gathering interviews. **Agency/Department responsibilities:** ■ Ensure attendance at kickoff meeting by Project Sponsor, Project Manager and other key stakeholders, as determined prior to kickoff. ■ Identify relevant information necessary for the project, identify personnel required for participation in the defined tasks of the project, and establish timeframes and logistics for on-site interviews and activities. ■ Establish an agency/department “Core Team” (as necessary) to support and participate in the activities of the engagement. A list of the typical roles represented for this effort are (1) project manager (2) line-of-business (3) enterprise architect (4) security architect (5) security domain expert ■ Assign a project team leader who will effectively manage the execution of the assessment, including ❑ Communicate factors (as soon as they are known) that could affect the assessment’s schedule or the cost, quality, or delivery of Gartner’s consulting services ❑ Inform Gartner of the assessment’s status so that Gartner can quickly address issues associated with direction and scope ❑ Provide timely feedback on questions and information requests submitted by Gartner	infrastructure components, and related in-flight projects ■ Documented business and use cases ■ Functional requirements and specifications documents including infrastructure, process, data flow, and architecture diagrams ■ Other documentation such as existing policies, procedures, and audit and incident reports
Step 2: Baseline Environment Information Gathering	*Deliverable(s) and Time Frame*
Objective: ■ Ensure that both Gartner and each agency/department are working from the same baseline understanding of the environment including the current-state of the infrastructure, the business drivers, and the strategic future-state requirements. ■ This task is comprised of two primary subtasks ❑ Document review ❑ Sponsor and stakeholder interviews. **Activities performed by Gartner:** ■ Review the documentation provided during kickoff. Through the review, acquire a sufficient overview of and background on each agency/department environment, the target processes and supporting infrastructure, and potential constraints and impacts. This will enable the consulting team to appropriately focus the follow-on	**Deliverable(s):** ■ Up to ten (10) interviews conducted over consecutive working days (2 days for standard assessments; 3 days for comprehensive assessments); used to capture the necessary information. ■ All interviews will be conducted onsite at the agency-selected location determined in advance. **Time frame:** ■ One (1) week: ❑ Documentation review ❑ Interviews (1 - 3 days) **Stakeholder Interview Topics:** ■ The interviews will lead the core team and stakeholders through detailed

interviews and information gathering activities. ■ Conduct a series of interviews with key personnel, functional organizations, sponsors, stakeholders, and executives. These interviews will allow stakeholders and impacted organizations to describe their existing responsibilities and technologies. Interviews may be with individuals, or with small groups in the same department or who perform similar functions or have similar subject matter expertise across departments. These interviews will focus on enterprise and business unit-specific requirements and explore a mix of business and technology perspectives. ❑ These interviews will be used by Gartner to (1) further identify business challenges that are expected to be addressed by the initiative (2) discuss perceived issues, pain points and critical success factors (3) understand the perspectives regarding current and future capabilities. ❑ Typically, these interviews include individuals and management from both IT and business organizations that are drawn from cross-functional groups. These groups may include (but are not limited to) IT architecture, application development, IT Engineering, IT/Data Center Operations including networks and system administration, IT Service Management, IT Security, Risk or Compliance management, directory services, Human Resources, Physical Security, Internal Audit, functional business units/end-users, and other representatives that can be supported by the results of this project. **Agency/Department responsibilities:** ■ Provide Gartner team members with access to appropriate facilities (e.g., buildings, labs, conference rooms, offices), and a suitable work area and resources (e.g., desk, phone, Internet, printer, fax) for when working on-site. ■ Present applicable agency-related IT initiatives, requirements, constraints, and a description of the current environment ■ Select participants and coordinating meetings involving agency/department personnel. Note: the participation of appropriate agency/department personnel will be the responsibility of each agency/department, and the lack of participation of appropriate personnel may impact the quality and depth of the results ■ Provide timely feedback on questions and information requests submitted by Gartner.	discussion and information sharing in order to gain an understanding of the following topics: ❑ The nature of the business, the scope of the enterprise, the structure of the organization, the interaction and dependencies of the business units, and the identification of the end-user population including internal (e.g., employees, contractors) and external (e.g., customers, consumers, suppliers, partners) users. ❑ How the agency and its information technology operate and what makes it succeed or fail in terms of security. ❑ What is the organizational governance including (but not limited to) structure, IT and information ownership and classification, training and awareness, incident response, disaster recovery/contingency planning, levels of authority and influence, and regulatory compliance requirements. ❑ Where the business value lies and the impacts of corruption, loss of availability, loss of control, and data leakage involving different elements of information systems and infrastructure. ❑ The end-user environment and devices and the nature of their interaction with the infrastructure, from both inside the enterprise and outside. ❑ The components and operational methodologies comprising the information and identity systems, and their operation within the enterprise, including (but not limited to) directory services, network operations, collaboration and content management including database and document repositories, identity lifecycle management including ERP systems, access control, monitoring and audit, and PKI. ❑ The threats, vulnerabilities, and consequences associated with

	information, information technologies, identities, and related access control. ❑ Information on previously identified incidents and audit findings. ❑ Other discussions, observations, and assessments as identified during the interviews will be collected for subsequent analysis
Step 3: Baseline Environment Assessment: Business Drivers, Requirements, and Gap Identification	*Deliverable(s) and Time Frame*
Objective: ■ Ensure that both Gartner and each agency/department are working from the same baseline understanding of the environment including the current-state of the infrastructure, the business drivers, and the strategic future-state requirements. ■ This task is comprised of three primary subtasks ❑ Define security program drivers and requirements ❑ Identify gaps between current-state and future-state requirements; and between the current-state and industry leading practices ❑ Document the baseline environment. **Activities performed by Gartner:** ■ Review the information and documentation provided during the previous project kickoff and information gathering tasks. Through the review, acquire a sufficient overview of and background on the agency/department environment, the target processes and supporting infrastructure, and potential constraints and impacts. This will enable the consulting team to appropriately focus the follow-on requirements and gaps identification and definition activities. ■ Taking the input from the previous tasks ❑ Identify the high level drivers and related requirements of both the current-state of the environment and the desired future-state; ❑ Define the strategic gaps between the current-state and desired future-state requirements as well as between the desired future-state and industry leading practices. ■ Develop and deliver a report that summarizes and documents the information gathered through the interviews, the provided documentation, the drivers and requirements, and identified gaps. The information documented in this report will be used as the foundation for the follow-on gap analysis, and the development of the strategic recommendations and deployment roadmap.	**Deliverable(s):** ■ Baseline Environment portion of the Final Report ❑ An electronically delivered report that summarizes and documents the information gathered through the interviews, the provided documentation, and the survey responses. ❑ The agency/department will have the opportunity to review this document and provide consolidated feedback for one (1) revision cycle to ensure that the baseline has been accurately captured prior to finalizing the report. ❑ Unless otherwise indicated, report will be delivered in English, in MS-Word format. **Time frame:** ■ Two - Three (2 - 3) weeks: ❑ 1 week requirement and gap definition ❑ 1 week report development ❑ 1 week agency/department review and feedback of draft report; delivery of final report **Report Contents:** ■ The high-level Table Of Contents for the baseline portion of the final deliverable includes: ❑ Executive Summary ❑ Project Overview and Methodology ❑ Baseline Environment (i.e., Current State) including People,

DSIT responsibilities: ■ Provide timely feedback on deliverables (draft and final), information requests, and project questions submitted by Gartner.	Process, Technology, and Existing related initiatives □ Drivers including Increasing Value, Containing Costs, Improving Compliance, and Reducing Risk □ Requirements (i.e., desired Future State) including constraints, assumptions, dependencies □ Gaps between current-state and desired future-state requirements □ Vulnerabilities between current-state and industry-leading practices
Step 4: Analysis and Recommendation Development: Gaps, Risks and Mitigations	*Deliverable(s) and Time Frame*
Objective: ■ Develop and document the strategic architecture recommendations that will address the gaps and vulnerabilities identified in the current-state environment, and are required to securely and effectively support the current and future business drivers, requirements, and initiatives of the agency or department. ■ The mitigation strategy and architecture will be developed using the established Gartner Reference Architecture, a mature and proven decision framework and methodology. ■ This task is comprised of four primary subtasks □ Gap analysis and vulnerability assessment □ Map requirements and gaps/risks to the Gartner Reference Architecture □ Integrate the Reference Architecture into a strategic solution architecture □ Document the recommended architecture and strategy. **Activities performed by Gartner:** ■ Taking the input from the previous tasks, conduct a high level gap analysis of the current state and future state requirements, as well as between the desired future state and industry best practices. □ The gap analysis will include an assessment of the level of security risk associated with the gaps in the context of the agency-specific environment, drivers, and requirements. ■ Integrate and map the high-level, generic Reference Architecture to develop the recommended strategy, related architecture, and solution alternatives for addressing the gaps, and achieving the goals of the strategy.	**Deliverable(s):** ■ Recommendations portion of the final Report □ An electronically delivered report that summarizes and documents the detailed analysis of the findings and recommendations. □ DSIT will have the opportunity to review this document and provide consolidated feedback for one (1) revision cycle prior to finalizing the report. □ Unless otherwise indicated, report will be delivered in English, in MS-Word format. **Time frame:** ■ Two - Three (2 - 3) weeks □ 1 week gap and mitigation analysis, report development □ 1 week DSIT review and feedback of draft report; delivery of final report **Topics Assessed:** ■ Security topics that will be addressed as part of the assessment: 1. Application Security 2. Availability of Information 3. Change Management with Assurance 4. Confidentiality of Information 5. Encryption 6. Endpoint Admission

❑ Solution and provider candidate recommendations will leverage Gartner's extensive research and advisory service as well as our understanding of what other like-industry institutions are doing to meet similar requirements. ❑ Gartner will consider and rationalize any existing agency, department or DSIT security principles, policies, position statements and templates as the recommended strategy is developed. As appropriate, relevant pre-existing materials shall be incorporated into the strategy (with any necessary refinements) in lieu of building them from scratch. ❑ Note that the precise contents of the strategy as documented in the final report will depend on the analysis work performed during the engagement. It may also be necessary to develop multiple permutations to satisfy options permitted by agency (or DSIT) principles, whichever apply. ■ Develop and deliver a report that describes and documents the results of the gap analysis as well as the strategy and architecture recommendations. **DSIT responsibilities:** ■ As necessary, provide applicable and relevant input in the resulting strategy and architecture. ■ Provide timely feedback on deliverables (draft and final), information requests, and project questions submitted by Gartner.	7. Governance 8. Host and Mobile System Security 9. Identity and Access Management (IAM) 10. Integrity of Information 11. Malicious Software 12. Network Intrusion Detection and Response 13. Network Perimeter 14. Network Zones 15. Physical Security 16. System Placement 17. Vulnerability Management **Report Contents:** ■ The high-level Table Of Contents for the recommendations portion of the final deliverable includes: ❑ Executive Summary ❑ Project Overview, Scope, Objectives, and Methodology ❑ Baseline Environment Summary Review ❑ Findings including Gap Analysis Results ❑ Strategy and Architecture Recommendations and Conclusions
Step 5: Deployment Roadmap Planning	*Deliverable(s) and Time Frame*
Objective: ■ Establish the high-level plan and strategy that is required to effectively and efficiently migrate from the current-state environment to the future-state environment in accordance with the agency/department business drivers, requirements, gaps, vulnerabilities, and constraints as identified during the previous activities. ■ The agency or department-specific deployment roadmap will include phased implementation objectives: ❑ Short-term: Immediate to 6-months ❑ Short-term: 6 to 24-months ❑ Mid-Term: 24 – 42-months ❑ Long-term: 42 to <60 months **Activities performed by Gartner:** ■ Organize the solution recommendations identified during the previous task into a high-level deployment roadmap depicting the sequence and dependencies of actions required for achieving the desired strategy and	**Deliverable(s):** ■ Final report including all of the previously documented elements (baseline environment and recommendations) plus the Strategic Deployment Roadmap report ❑ An electronically delivered report that will include milestones and estimated costs, specific deployment considerations, and best practices tailored specifically for the agency or department. ❑ It must be noted that Gartner considers the deployment roadmap as a "living" plan that should be altered in accordance with decisions made by the appropriate governance board(s) or the business owners of the project.

architecture. □ The process for developing the high-level deployment plan and strategy necessary for achieving the desired results will leverage the use of professional project management practices, Gartner’s extensive research and advisory service, as well as our understanding of what other like-industry institutions are doing to deploy similar capabilities and technologies. □ Gartner typically recommends a *phased* migration and deployment strategy in order to minimize disruption to the production environment(s), as well as to optimize investments in the recommended solutions moving forward. □ As part of the overall plan, Gartner also typically recommends an initial phase that is intended to incorporate all aspects of the implementation in order to meet all the phases of the project. This initial phase encompasses prerequisite tasks such as detailed project planning, staffing, acquisition and procurement, detailed design, governance, and process changes, most of which need to be completed prior to embarking on the other phases of the deployment plan. Planning for all the phases of the project at this first stage will create a solid direction going forward and will help uncover challenges and obstacles that may require additional internal or professional services support. □ The planning of the deployment phases is designed to deliver a modular, appropriately encompassing architecture implemented over an achievable, phased timeline. □ Each phase maximizes re-use and does not result in redundant, additional dollars despite the phased approach to deployment. □ The recommended deployment plan is intended to be consistent with the agency or department short and long-term drivers and requirements as defined during the baseline activity of this project. **DSIT responsibilities:** ■ As necessary, provide applicable and relevant input with regards to agency-specific considerations for technology and process deployment and migration approaches ■ Provide timely feedback on deliverables (draft and final), information requests and project questions submitted by Gartner.	□ DSIT will have the opportunity to review this document and provide consolidated feedback for one (1) revision cycle prior to finalizing the report. □ Unless otherwise indicated, report will be delivered in English, in MS-Word format. **Time frame:** ■ One – Two (1 - 2) weeks □ 1 week deployment planning and report development □ 1 week agency or department review and feedback of draft report; delivery of final report **Report Contents:** ■ The high-level Table Of Contents for the recommendations deliverable includes: □ Executive Summary □ Project Scope and Objectives □ Summary of Findings, Requirements, and Recommendations □ Overview of Phased Deployment Plan Milestones and ROM Project Costs □ Details of Deployment Plan Phases
Step 6: Assessment Delivery and Results Closeout Presentation	*Deliverable(s) and Time Frame*
Objective:	**Deliverable(s):**

■ Present an overview of the project and a summary of the results to an audience of agency or department senior management and the stakeholders for this initiative. ■ Obtain approval and signoff of the satisfactory completion of the engagement. **Activities performed by Gartner:** ■ Prepare and deliver in-person and onsite, a presentation summarizing the project results. **Agency/Department responsibilities:** ■ Provide Gartner team members with access to appropriate facilities and a suitable briefing area for the onsite presentation. ■ Select participants and coordinate the attendance of appropriate agency/department personnel. ■ Provide timely feedback on deliverables (draft and final), information requests, and project questions submitted by Gartner.	■ A two (2) hour presentation that represents the summary results of the engagement. ❑ Agency/department will have the opportunity to review the presentation deck and provide consolidated feedback for one (1) revision cycle to prior to the live presentation. ❑ Unless otherwise indicated, report will be delivered in English, in MS-PowerPoint format. **Time frame:** ■ One (1) week ❑ Presentation development ❑ Agency/department review and feedback ❑ Delivery of the on-site briefing **Presentation Contents:** ■ The high-level Table Of Contents for the management presentation deliverable includes: ❑ Project Overview ❑ Summary of current-state environment including business drivers and requirements, and gap analysis results ❑ Summary of the recommended strategic architecture ❑ Summary of the recommended strategic deployment roadmap ❑ Conclusion(s) and next steps
Segment 3. Ongoing SRM Decision Support Services	
Task 6. Provide Ongoing SRM Decision Support Services	***Deliverable(s) and Time Frame***
Objective: ■ Provide baseline education of security governance, practices, policies and architecture to an Advisory Council of State security practitioners, architects, IT managers and key executives ■ Provide the decision support framework and tools to develop a statewide security architecture ■ Provide frameworks that will give the state a security governance and operations models ■ Describe the functions of security and risk forums and	**Deliverable(s):** ■ One Enterprise IT Leaders Seat ■ Three Enterprise IT Leaders Role Based Workgroup Seats ■ Gartner for Technical Professionals Security & Risk Management and Identity & Access research for the DSIT organization. ■ Quarterly on-site Workshops covering topics such as:

committees ■ Assist in establishing processes that IT security officials must own ❑ Security Governance ❑ Policy Management ❑ Awareness and Education ❑ Identity and Access Management ❑ Vulnerability Management ❑ Threat Management ❑ Incident Response **Recommended Decision Support Seat Holders:** ■ The CISO or an alternate employee selected by DSIT will hold the Enterprise IT Leaders seat. ■ The three IT security personnel from DSIT will each hold Enterprise Work Group seats. ■ It is anticipated that ten IT personnel may work on sub-committees of the security council who may require additional access to research which is not currently part of this scope, but can be refined as more information is determined about security governance within the State.The sub-committees may focus on the following data types that require additional security precautions: ❑ Healthcare and other data covered by HIPAA ❑ Financial information and data covered by IRS regulations ❑ PCI compliance ❑ Law enforcement data ■ All DSIT users may leverage the Gartner for Technical Professionals Security & Risk Management and Identity & Access research ■	❑ Security Foundations ❑ Security Architecture ❑ How to Organize a Complex Security Structure ❑ Controlling Malicious Software (Specific workshop topics will be agreed upon by DSIT and Gartner and will align with assessment findings) ■ Monthly Webinars or Audio Teleconferences covering topics such as: ❑ Cloud Security ❑ Vulnerability Management ❑ Endpoint Admission Control ❑ User Provisioning ❑ Federated Identity (Specific Webinars and Audio Teleconferences will be agreed upon by DSIT and Gartner and will align with assessment findings) **Time frame:** ❑ Period of performance is November 2012 – October 2014.
Extension Option #1. Security Program Support Services (Year 3)	
Task 7. Program Office Support	***Deliverable(s) and Time Frame***
Objective: ■ Initiate transition of program management, coordination and communication to DSIT Program resources ■ Continue supporting overall Program objectives by assisting DSIT in the program management of security assessments of an additional 10 state agency assessments ■ Continue developing the State of South Carolina statewide enterprise reporting on security and risk management ■ Continue developing a consolidated view of the overall Program for updates, status reporting and progress **Activities performed by Gartner:** ■ Assist DSIT in the management of resources,	**Deliverable(s):** ■ Program Management Assistance to DSIT in conducting 10 agency assessments ■ Assist in decision support on Security and Risk Management efforts ■ Gartner monthly status reports ■ Support in developing Statewide Enterprise Security Reporting (updated quarterly) ■ Coordinate web seminars, workshops and/or analyst calls

scheduling and work activities of the agency SRM assessments ■ Assist DSIT in conducting agency assessments at up to 10 State agencies ■ Review findings from assessments in order to assist in the creation of the ongoing State-wide Security Scorecard ■ Provide support to DSIT in producing the Statewide Enterprise Report, updated quarterly, on SRM and reflecting the "state of the state" ■ Assist in preparations for quarterly workshop with DSIT leadership to provide status of program and discuss "State Security Report Card" ■ Provide assistance communicating with South Carolina stakeholders on status, progress and updates on findings ■ Provide an ongoing interface to Gartner analysts for scheduling of inquiry calls, workshops and webinars. **DSIT responsibilities:** ■ Creation of status reports in order to help closely manage expectations and schedules of the Program. ■ Lead the development of the Statewide Enterprise Report (State Security Report Card), updated quarterly ■ Lead the quarterly workshops in order to obtain feedback and support to the program ■ Work with Gartner to assist in the coordination of Gartner events (non-assessment related)	**Time frame:** ■ Year 3 of overall Program
Task 8. Security Assessment Support	***Deliverable(s) and Time Frame***
Objective: ■ Assist and support DSIT in finalizing a DSIT assessment tool to be used for ongoing DSIT lead security assessments, informed by Gartner tools and research ■ Assist DSIT in performing security assessments for the next 10 agencies, agencies to be defined and prioritized by DSIT – as defined in Task 4, Steps 1 - 6 ■ DSIT resources begin to take a more active role in the execution of these assessments with Gartner providing expert advisory assistance **Activities performed by Gartner:** ■ Provide assistance in the execution of the security assessments ■ Provide education and guidance to the DSIT assessment team ■ Participate in the creation of all deliverables and recommendations	**Deliverable(s):** ■ Gartner will assist in the development of all deliverables for the selected 10 agencies' as defined in Task 4, Steps 1-6 **Time frame:** ■ 12 months (year 3 of Security Program)

■ Support in the final presentation to the individual agencies **DSIT responsibilities:** ■ Responsible for leading the assessments ■ Lead in collection of information, evaluation and assessment of data points ■ Develop gap analysis based on findings with direct support from Gartner Subject Matter Experts ■ Develop recommendations and execution roadmap with direct support from Gartner Subject Matter Experts ■ Lead workshop/presentation of findings (final assessment deliverable) to the agency's leadership with counsel and guidance from Gartner	
Task 9. Ongoing Decision Support	***Deliverable(s) and Time Frame***
Objective: ■ Provide baseline education of security governance, practices, policies and architecture to an Advisory Council of State security practitioners, architects, IT managers and key executives ■ Provide the decision support framework and tools to develop a statewide security architecture ■ Provide frameworks that will give the state a security governance and operations models ■ Describe the functions of security and risk forums and committees ■ Assist in establishing processes that IT security officials must own ❑ Security Governance ❑ Policy Management ❑ Awareness and Education ❑ Identity and Access Management ❑ Vulnerability Management ❑ Threat Management ❑ Incident Response **Recommended Decision Support Framework:** ■ To be determined based upon the structure of the Security Advisory Council and its subcommittees at the time of extension.	**Deliverable(s):** To be determined based upon the configuration required at the time of extension. **Time frame:** ■ For a period of one year (year 3 of Program) ■ Pricing to be at the then prevailing DSIT price
Extension Option #2. Security Program Support Services (Year 4)	
Task 10. Program Office Support	***Deliverable(s) and Time Frame***
Objective: ■ Complete transition of program management coordination and communication to DSIT Program	**Deliverable(s):** ■ Assist in decision support on Security and Risk Management efforts

resources ■ Continue supporting overall Program objectives by completing security assessments of all remaining participating state agencies ■ Continue developing the State of South Carolina statewide enterprise reporting on security and risk management ■ Continue developing a consolidated view of the overall Program for updates, status reporting and progress **Activities performed by Gartner:** ■ Assist DSIT in the management, scheduling and work activities of Gartner resources for the agency SRM assessments ■ Review findings from assessments in order to assist in the creation of the ongoing State-wide Security Scorecard ■ Provide support to DSIT in producing the Statewide Enterprise Report, updated quarterly, on SRM and reflecting the “state of the state” ■ Assist in preparations for quarterly workshop with DSIT leadership to provide status of program and discuss “State Security Report Card” ■ Provide an ongoing interface to Gartner analysts for scheduling of inquiry calls, workshops and webinars. **DSIT responsibilities:** ■ Identify and select agencies for SRM assessments ■ Manage and schedule work activities of DSIT resources for performing SRM assessments ■ Review findings and final deliverables from each SRM assessment for completeness, conciseness and ability to execute the recommendations and roadmap ■ Create status reports in order to closely manage expectations and schedules of the Program. ■ Lead the development of the Statewide Enterprise Report (State Security Report Card), updated quarterly ■ Schedule, coordinate and lead the quarterly workshops in order to obtain feedback and support to the program ■ Work with Gartner to assist in the coordination of Gartner events (non-assessment related)	■ Gartner monthly status reports ■ Support in developing Statewide Enterprise Security Reporting (updated quarterly) ■ Coordinate web seminars, workshops and/or analyst calls **Time frame:** ■ Year 4 of overall Program
Task 11. Security Assessment Support	***Deliverable(s) and Time Frame***
Objective: ■ Perform security assessments for the next 10 agencies defined and prioritized by DSIT – as defined in Task 4, Steps 1 - 6 ■ DSIT resources will have leadership role in the execution of these assessments and Gartner will assist	**Deliverable(s):** ■ Gartner will review all deliverables, as defined in Task 4, Steps 1-6, for the selected agencies

Activities performed by Gartner: ■ Gartner will advise and assist with Subject Matter Expertise to support the DSIT team in conducting assessments ■ Provide education and guidance to the DSIT assessment team ■ Review all deliverables and recommendations ■ Support in the final presentation to the individual agencies **DSIT responsibilities:** ■ Responsible for leading the assessments ■ Lead in collection of information, evaluation and assessment of data points ■ Develop gap analysis based on findings ■ Develop recommendations and execution roadmap ■ Prepare and deliver a workshop/presentation of findings (final assessment deliverable) to the agency's leadership	**Time frame:** ■ 12 months (year 4 of Security Program)
Task 12. Ongoing Decision Support	***Deliverable(s) and Time Frame***
Objective: ■ Provide baseline education of security governance, practices, policies and architecture to an Advisory Council of State security practitioners, architects, IT managers and key executives ■ Provide the decision support framework and tools to develop a statewide security architecture ■ Provide frameworks that will give the state a security governance and operations models ■ Describe the functions of security and risk forums and committees ■ Assist in establishing processes that IT security officials must own ❑ Security Governance ❑ Policy Management ❑ Awareness and Education ❑ Identity and Access Management ❑ Vulnerability Management ❑ Threat Management ❑ Incident Response **Recommended Decision Support Framework:** ■ To be determined based upon the structure of the Security Advisory Council and its subcommittees at the time of extension.	**Deliverable(s):** To be determined based upon the configuration required at the time of extension. **Time frame:** ■ For a period of one year (year 4 of Program) ■ Pricing to be at the then prevailing DSIT price

Extension Option #3. Security Program Support Services (Year 5)	
Task 13. Program Office Support	***Deliverable(s) and Time Frame***
Objective: ■ DSIT program office fully responsible for Program decision making with Gartner limited secondary support ■ Program management, coordination and communication primary responsibility of DSIT Program resources ■ DSIT leading security assessments to all remaining state agencies ■ Continue developing the State of South Carolina statewide enterprise reporting on security and risk management ■ Continue developing a consolidated view of the overall Program for updates, status reporting and progress **Activities performed by Gartner:** ■ Assist DSIT in the management, scheduling and work activities of Gartner resources for the agency SRM assessments ■ Review findings from assessments in order to advise in the creation of the ongoing State-wide Security Scorecard ■ Provide advisory support to DSIT in producing the Statewide Enterprise Report, updated quarterly, on SRM and reflecting the “state of the state” ■ Assist in preparations for quarterly workshop with DSITDSITDSIT leadership to provide status of program and discuss “State Security Report Card” ■ Transition ongoing interface to Gartner analysts for scheduling of inquiry calls, workshops and webinars to DSIT resources **DSIT responsibilities:** ■ Manage and schedule work activities of DSIT resources for performing SRM assessments ■ Review findings and final deliverables from each SRM assessment for completeness, conciseness and ability to execute the recommendations and roadmap ■ Create status reports in order to closely manage expectations and schedules of the Program. ■ Lead the development of the Statewide Enterprise Report (State Security Report Card), updated quarterly ■ Schedule, coordinate and lead the quarterly workshops in order to obtain feedback and support to the program ■ Work with Gartner to assist in the coordination of Gartner events (non-assessment related)	**Deliverable(s):** ■ Advise in decision support on Security and Risk Management efforts ■ Gartner monthly status reports ■ Advisory Support in developing Statewide Enterprise Security Reporting (updated quarterly) **Time frame:** ■ Year 5 of overall Program

Task 14. Security Assessment Support	***Deliverable(s) and Time Frame***
Objective: ■ Gartner provides limited assistance to perform security assessments for the next 10 agencies defined and prioritized by DSIT – as defined in Task 4, Steps 1 - 6 ■ DSIT resources will have leadership role in the execution of these assessments **Activities performed by Gartner:** ■ Targeted and select Subject Matter Expertise support for the execution of the security assessments ■ Provide guidance and SME assistance to the DSIT team as requested ■ Review final deliverables and recommendations **DSIT responsibilities:** ■ Responsible for leading the assessments ■ Responsible for collection of information, evaluation and assessment of data points ■ Develop gap analysis based on findings ■ Develop recommendations and execution roadmap ■ Prepare and deliver a workshop/presentation of findings (final assessment deliverable) to the agency's leadership	**Deliverable(s):** ■ Agency analysis support ■ Gartner will review the final recommendations and roadmap deliverable, for the selected agencies, and provide feedback and observations to the delivery team **Time frame:** ■ 12 months (year 5 of Security Program)
Task 15. Ongoing Decision Support	***Deliverable(s) and Time Frame***
Objective: ■ Provide baseline education of security governance, practices, policies and architecture to an Advisory Council of State security practitioners, architects, IT managers and key executives ■ Provide the decision support framework and tools to develop a statewide security architecture ■ Provide frameworks that will give the state a security governance and operations models ■ Describe the functions of security and risk forums and committees ■ Assist in establishing processes that IT security officials must own ❑ Security Governance ❑ Policy Management ❑ Awareness and Education ❑ Identity and Access Management ❑ Vulnerability Management ❑ Threat Management ❑ Incident Response **Recommended Decision Support Framework:**	**Deliverable(s):** To be determined based upon the configuration required at the time of extension. **Time frame:** ■ For a period of one year (year 5 of Program) ■ Pricing to be at the then prevailing DSIT price

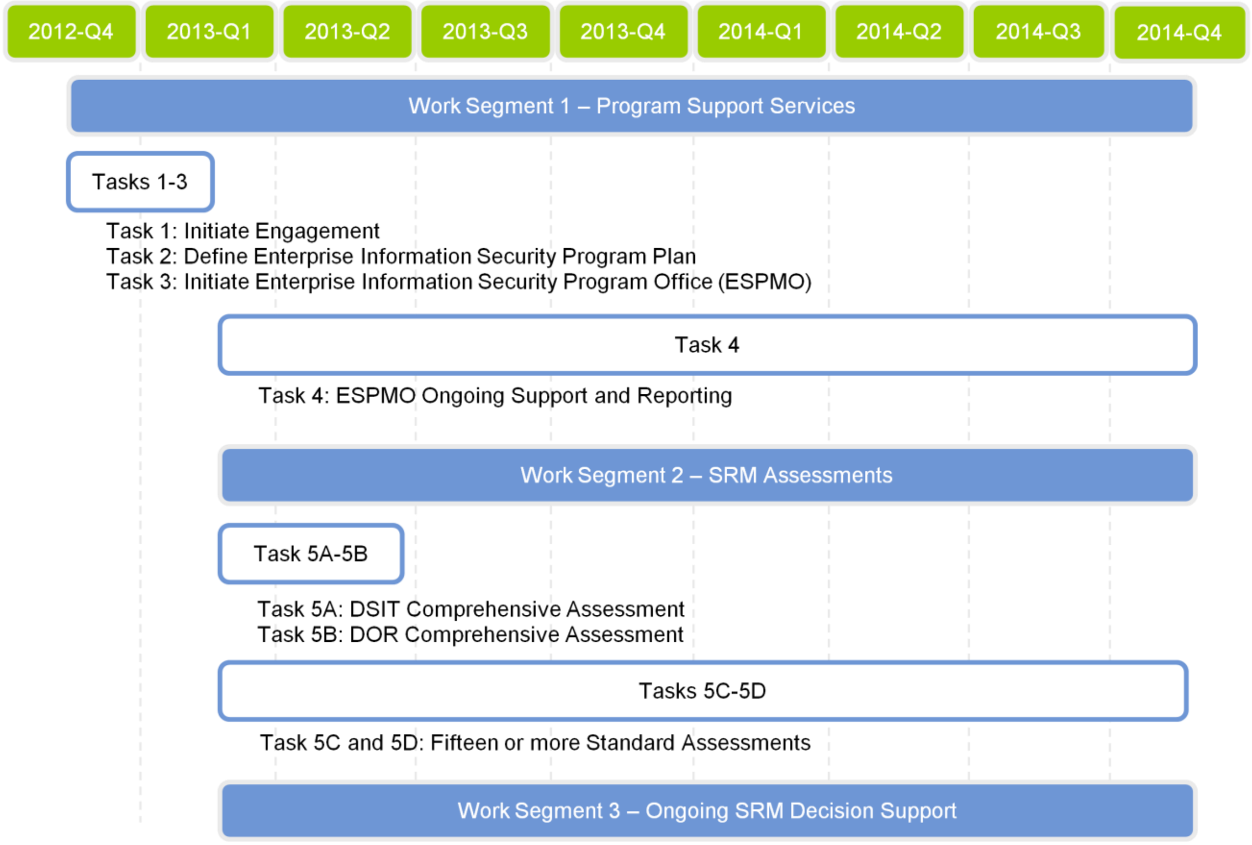
■ To be determined based upon the structure of the Security Advisory Council and its subcommittees at the time of extension.	

2.1.2 Base Period Project Schedule

Gartner anticipates completion of the base period scope of services outlined in Segments 1, 2 and 3 of this SOW within 24 months of engagement initiation. During the first ten weeks, Gartner will work with DSIT to define the Enterprise Security Program Plan and Program Management Office (ESPMO). The ESPMO will establish the requirements, frameworks, and direction of the program and manage day-to-day operations of the program. In addition, the ESPMO will prioritize execution of the security assessments at each of the pre-determined state agencies. The ESPMO will coordinate and facilitate assessment initiation and communication, and provide the ongoing SRM decision support capabilities. Day-to-day management of assessments including schedule definition, timelines, deliverables, governance, priorities, and project status communications will be provided by the individual Gartner Consulting assessment teams in conjunction with the individual department points-of-contact.

The Figure 4 below reflects the high- level timeline anticipated for the execution of the Work Segments 1, 2 and 3 over the base period (Years 1 and 2):

Figure 4. Estimated Engagement Calendar Year Schedule


2012-Q4
2013-Q1
2013-Q2
2013-Q3
2013-Q4
2014-Q1
2014-Q2
2014-Q3
2014-Q4
Work Segment 1 – Program Support Services
Tasks 1-3
Task 1: Initiate Engagement
Task 2: Define Enterprise Information Security Program Plan
Task 3: Initiate Enterprise Information Security Program Office (ESPMO)
Task 4
Task 4: ESPMO Ongoing Support and Reporting
Work Segment 2 – SRM Assessments
Task 5A-5B
Task 5A: DSIT Comprehensive Assessment
Task 5B: DOR Comprehensive Assessment
Tasks 5C-5D
Task 5C and 5D: Fifteen or more Standard Assessments
Work Segment 3 – Ongoing SRM Decision Support

2.2 Gartner Project Team

2.2.1 Proposed Project Team

Gartner has created a project team structure for this engagement that ensures high-level sponsorship and quality assurance, strong day-to-day program management, a focused team of project advisors, research analyst, and deep subject matter expertise. Following is a description of the project team roles and responsibilities for this engagement.

Table 4. Project Team Roles and Responsibilities

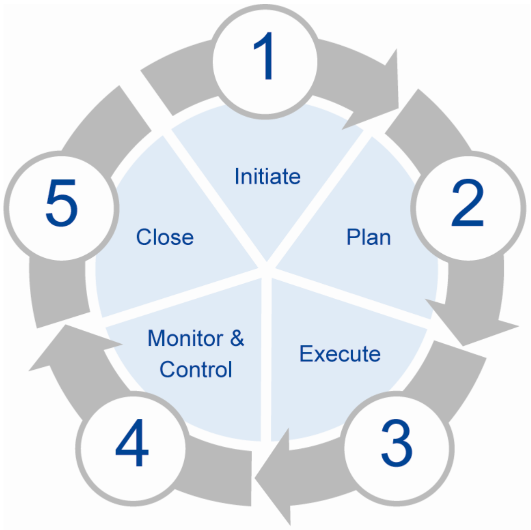
Gartner Associate	Role	Responsibilities
Jeff Perkins	Managing Partner and Program Advisor (State Government and State IT Management)	■ Ensure that Gartner activities support DSIT goals ■ Build and maintain a long-standing relationship with DSIT and security governance body ■ Provide high-level oversight to the project and become more heavily involved should any issue resolution be necessary
Kris Doering	Enterprise Security Program Manager	■ Responsible for development of Enterprise Security Program Plan and initiation of Enterprise Security PMO
Mike Samsen	Program Advisor (Governance and IT Management)	■ Provides input and advise regarding Enterprise Security Program Plan and initiation of Enterprise Security PMO
Bob Smock	Enterprise Program and Security Advisor and Lead Consultant	■ Provide day-to-day consulting leadership and support for project tasks ■ Be supported by additional project consultants as needed
Frank Lesar	Project Manager (Assessments)	■ PMP and 30 years relevant experience ■ Be responsible for the day-to-day management of securoty and risk assessments ■ Ensure that project deliverables are completed on time and meet the Gartner quality standards ■ Act as the primary point of contact for the Gartner team for assessments ■ Work closely with assessment participatns to ensure that Gartner is meeting its needs
Bob Smock	Core Project Consultant	■ 30 years relevant experience; CISSP and CISM certifications ■ Provide day-to-day consulting support for project tasks ■ Be supported by additional project consultants as needed
Kim May	Core Project Consultant and Delivery Team Lead	■ 17 years relevant experience; PMP certification ■ Provide day-to-day consulting support for project tasks ■ Be supported by additional project consultants as needed
Chris Weldon	Subject Matter Expert and	■ 30 years relevant experience

Gartner Associate	Role	Responsibilities
	Delivery Team Lead	■ Support the core project team by providing subject matter expertise as needed throughout the engagement ■ Participate in deliverable creation, deliverable review and client presentations as needed
Randy Stalnaker	Subject Matter Expert	■ 30 years relevant experience; CISSP certification ■ Support the core project team by providing subject matter expertise as needed throughout the engagement ■ Participate in deliverable creation, deliverable review and client presentations as needed
Derek Nwamadi	Subject Matter Expert	■ 15 years relevant experience; CISSP ■ Support the core project team by providing subject matter expertise as needed throughout the engagement ■ Participate in deliverable creation, deliverable review and client presentations as needed
Manish Jyoitishi	Subject Matter Expert	■ 25 years relevant experience ■ Support the core project team by providing subject matter expertise as needed throughout the engagement ■ Participate in deliverable creation, deliverable review and client presentations as needed
Christian Byrnes	Research Analyst	■ Support the core project team by providing a context sensitive perspective to issues specific to DSIT based on Gartner industry-leading research ■ Participate in analysis and comparisons, and review deliverables as needed
Doug Simmons	Global Security Practice Leader, Quality Assurance	■ 30 years relevant experience ■ Provide quality assurance review of Gartner project plan and Gartner deliverables throughout the engagement ■ Ensure value through use of the Gartner Project Management Life Cycle detailed in this document

2.3 Gartner Project Management Life Cycle

The Project Management Life Cycle Gartner uses for every engagement is based on our internal subject matter expertise and lessons learned, as well as external sources including the Project Management Institute's (PMI$^{®}$'s) Project Management Body of Knowledge (PMBOK$^{®}$) Guide. Gartner aligns with this globally recognized standard (ANSI/PMI 99-001-2008) to maximize value for our clients, minimize the risk for our clients' projects and ultimately ensure client satisfaction.

Figure 5. Stages of Gartner Project Management Life Cycle



Our approach is comprehensive — starting before the project kickoff and ending after the project close — to deliver results at every stage. The following table describes the typical activities, results and value provided by Gartner during the project management life cycle. However, it is important to note that Gartner views a project as an event that happens *with* a client — not *to* a client. We work closely with our clients to adapt leading practices to fit each client's environment and each project's requirements.

2.4 Assumptions

The deliverables, schedule and pricing in this Statement of Work are based on the following assumptions:

- The due diligence (as is) data are reasonably available via interviews and documentation review.
- DSIT will provide timely access to all appropriate personnel to be interviewed. These personnel will have the ability to provide data necessary to complete this project, answer questions, provide existing documentation and attend working sessions.
- Project pricing assumes that Gartner will conduct two comprehensive security assessments and 15 standard security assessments over 24 months, and that DSIT will arrange all subject matter expert interview sessions with DSIT personnel as described in the individual segment tasks
- All data collection and interviews/workshops will take place remotely via telephone or in person in Columbia, South Carolina and/or as agreed to at the project kickoff.
- Resumes of key personnel provided in this proposal assume a project start date of 15 November. If the actual project start date is different, proposed individuals may not be available. In this event, we will work with DSIT to identify alternative personnel with appropriate skills and background.
- DSIT will designate a project manager to act as the primary point of contact for this project. The DSIT project manager will be expected to work closely with the Gartner employees as needed and will: (a) approve project priorities, detailed task plans and schedules; (b) facilitate the scheduling of Gartner interviews with appropriate client

personnel; (c) notify Gartner in writing of any project or performance issues; and (d) assist in resolving project issues that may arise.

- The work effort described in this Statement of Work assumes that DSIT personnel are available to assist in the project as defined in this Statement of Work. In the event that DSIT personnel are not available, a change of scope may be necessary.
- DSIT will review and approve documents within five business days. If no formal approval or rejection is received within that time, the deliverable is considered to be accepted by DSIT.
- DSIT is to schedule DSIT resources for project activities and provide meeting facilities as necessary.
- DSIT personnel will be made available per the final project schedule.
- Office space, telephones and access to the open Internet will be made available to Gartner staff at DSIT locations for on-site project time.
- Gartner will have access to printing/copying services at DSIT locations.
- Any requests for additional information (beyond the details described in the tasks above) that are made by DSIT will be considered a change in scope for this engagement and will be handled accordingly (see Changes to Scope section of this Statement of Work).
- All deliverables will be developed using Microsoft products (for example, Project, Excel, Word and PowerPoint).
- It is assumed for the pricing of Work Segment 3 for year two of the base term that DSIT will not cancel this service for convenience.
- This SOW contains no scope to provide support in the event of a 3rd party lawsuit involving the State.

2.5 Pricing and Invoicing

2.5.1 Base Period (Years 1 and 2) Pricing and Invoicing

For the base period of years 1 and 2, Gartner will conduct Work Segments 1, 2 and 3 tasks in this Statement of Work for a firm-fixed price of $3,790,092 (USD). Gartner's firm fixed price is inclusive of all fees and travel expenses.

In addition, Gartner is providing three, one-year extension options below to be exercised at DSIT's discretion and at a date subsequent to the date of executing this SOW.

Gartner will invoice for the professional fees in accordance with the invoicing schedule below. Fees for year 1 of Work Segment 3 services will be invoiced at contract signature, and year 2 fees for Work Segment 3 services will be invoiced at the one year contract anniversary date (commencement of year 2 services).

All invoices are payable net 30 days from date of invoice. While we do not itemize billing for advisory services, we agree and will comply with any reasonable requests for records substantiating our invoices.

Years 1 & 2 Pricing & Invoicing Schedule (Base Period)
Work Segment 1 – Program Support Services

Milestone / Deliverable	Estimated Duration	Amount
Task 1: Initiate Project Task 2: Define Enterprise Security Program Plan Task 3: Initiate ESPMO	Ten (10) weeks	$ 230,000 (USD) total - $50,000 (USD) due at completion of Task 1 - $180,000 (USD) due at completion of Task 2 and Task 3
Task 4: ESPMO Ongoing Support and Reporting	21.5 months	$946,000 (USD) total - $44,000 per month invoiced monthly
Work Segment 1 Sub-Total:		**$1,176,000**
Work Segment 2 – Scurity and Risk Management (SRM) Assessments		
Milestone / Deliverable	**Estimated Duration**	**Amount**
Task 5A: Conducting DSIT Comprehensive Security Assessments	Ten to fourteen (10 to 14) weeks	$225,000 (USD) total - $50,000 (USD) due at completion of project initiation - $175,000 (USD) due at project completion
Task 5B: Conducting DOR Comprehensive Security Assessments	Ten to fourteen (10 to 14) weeks	$225,000 (USD) total - $50,000 (USD) due at completion of project initiation - $175,000 (USD) due at project completion
Task 5C: Conducting 15 Agency Standard Assessments	21.5 months or less (6 to 10 weeks per agency)	$1,875,000 (USD) total - $125,000 (USD) per assessment with $25,000 (USD) due at each assessment initiation and $100,000 (USD) due at each assessment completion

Task 5D: Conducting Agency Standard Assessments (as requested – undetermined amount)	21.5 month or less (6 to 10 weeks per agency)	No total estimated at this time - $140,000 (USD) per assessment with $30,000 (USD) due at each assessment initiation and $110,000 (USD) due at each assessment completion
Work Segment 2 Sub-Total:		**$ 2,325,000**
Work Segment 3 –Ongoing SRM Decision Support Services		
Milestone / Deliverable	**Estimated Duration**	**Amount**
Task 6, Year 1 Ongoing Decision Support (Research)	12 months (invoiced at the beginning of year 1)	$ 139,092 (USD) total - $91,617 (USD) Enterprise IT Leaders and Workgroup (1 advisor seat plus 3 workgroup seats) - $47,475 (USD) Gartner for Technical Advisor (SMB Enterprise)
Task 6, Year 2 Ongoing Decision Support (Research)	12 months (invoiced at the beginning of year 2)	Estimated at $150,000 - price to be finalized in 2013
Work Segment 3 Sub-Total:		**$289,092 (USD)**
Total of Work Segments 1, 2 & 3 (Years 1 & 2 Total):		**$3,790,092 (USD)**

2.5.2 Extension Options Pricing for Years 3, 4 and 5

The following pricing schedule reflects estimated three, one year extension options to be exercised at DSIT's discretion. Gartner will work with DSIT to finalize the estimated options for the Ongoing Decision Support fees in Tasks 9, Task 12 and Task 15 at the beginning of the "extension" year. The remaining estimated options will be invoiced on a monthly basis for ESPMO Support Services and at the completion of each agency assessment.

Extension Option #1 for Year 3 Services		
Milestone / Deliverable	**Estimated Duration**	**Amount**

Task 7, Ongoing Program Office Support	12 months	$ 25,000 per month
Task 8, Security Assessment Support (10 agencies)	12 months	$ 50,000 per assessment
Task 9, Ongoing Decision Support	12 months	$ 150,000*
*Base year pricing will be adjusted to the then prevailing DSIT pricing		
Total of Extension Option #1 (Year 3):		**$950,000 (USD)**
Extension Option #2 For Year 4 Services		
Milestone / Deliverable	**Estimated Duration**	**Amount**
Task 10, Ongoing Program Office Support	12 months	$ 20,000 per month
Task 11, Security Assessment Support (10 agencies)	12 months	$ 40,000 per assessment
Task 12, Ongoing Decision Support	12 months	$ 150,000*
*Base year pricing will be adjusted to the then prevailing DSIT pricing		
Total of Extension Option #2 (Year 4):		**$790,000 (USD)**
Extension Option #3 For Year 5 Services		
Milestone / Deliverable	**Estimated Duration**	**Amount**
Task 13, Ongoing Program Office Support	12 months	$ 15,000 per month
Task 14, Security Assessment Support (10 agencies)	12 months	$ 35,000 per assessment
Task 15, Ongoing Decision Support	12 months	$ 150,000*
*Base year pricing will be adjusted to the then prevailing DSIT pricing		
Total of Extension Option #3 (Year 5):		**$680,000 (USD)**

2.5.3 Validity Period

The Statement of Work, including the Statement of Work, is valid for 30 days from 5 November 2012.

2.5.4 Period Of Performance

The Segment 3 Gartner research based services reflected in this SOW shall commence on November 15, 2012 and continue for a period of two years. We anticipate that the Segment 1 and 2 services reflected in this SOW shall commence on or about November 15, 2012.

2.5.5 Changes to Scope

The scope of this engagement is defined by this Statement of Work. All DSIT requests for changes to the SOW must be in writing and must set forth with specificity the requested changes. As soon as practicable, Gartner shall advise DSIT of the cost and schedule implications of the requested changes and any other necessary details to allow both parties to decide whether to proceed with the requested changes. The parties shall agree in writing upon any requested changes prior to Gartner commencing work.

As used herein, “changes” are defined as work activities or work products not originally planned for or specifically defined by this SOW. By way of example and not limitation, changes include the following:

- Any activities not specifically set forth in this SOW
- Providing or developing any deliverables not specifically set forth in this SOW
- Any change in the respective responsibilities of Gartner and DSIT set forth in this SOW, including any reallocation or any changes in engagement or project manager staffing
- Any rework of completed activities or accepted deliverables
- Any investigative work to determine the cost or other impact of changes requested by DSIT
- Any additional work caused by a change in the assumptions set forth in this SOW
- Any delays in deliverable caused by a modification to the acceptance criteria set forth in this SOW
- Any changes requiring additional research analyst time or changes to research analyst resources

2.5.6 Authorization

This Statement of Work is submitted under the terms and conditions of Master Services Agreement (Consulting and Measurement) between Gartner, Inc. and State of South Carolina dated May 9, 2006.

When signed by Gartner and DSIT, this SOW is an attachment to and governed by the Master Consulting Services Agreement (MCSA) between the parties. These two documents will set forth the relationship between the parties for this engagement. This Statement of Work may be modified at anytime provided such changes are agreed by the parties in writing.

SUBMITTED ON BEHALF OF GARTNER, INC.

SIGNATURE	SIGNATURE
Jeff Perkins, Managing Partner, State of Local Government	Bill Kumagai, Group Vice President
PRINT NAME AND TITLE	PRINT NAME AND TITLE
5 November 2012	5 November 2012
DATE	DATE

AGREED ON BEHALF OF STATE OF SOUTH CAROLINA - DIVISION OF STATE INFORMATION TECHNOLOGY

SIGNATURE

PRINT NAME AND TITLE

DATE

PO NUMBER (IF APPLICABLE)

2.5.7 Further Assurances

Gartner Research and Consulting recommendations are produced independently by the Company's analysts and consultants, respectively, without the influence, review or approval of outside investors, shareholders or directors. For further information on the independence and integrity of Gartner Research, see "Guiding Principles on Independence and Objectivity" on our website, gartner.com or contact the Office of the Ombudsman at ombudsman@gartner.com or +1 203 316 3334.

Attachments

3.0 Attachments

Project Team Biographies

Following are the project team members who will likely work on this proposed engagement. If the individuals proposed herein are not available, Gartner will substitute another qualified professional with similar expertise and credentials.

Bob Smock

Senior Director, Gartner Consulting

Based in Houston, Texas, Bob Smock is an experienced consultant with almost 30 years of IT experience including more than 20 years in IT and information security and mission-critical risk management. He has provided leadership and expertise for numerous successful IT and security projects across a wide spectrum of industries including aerospace, defense, financial services, government, health care, education, insurance, manufacturing, and service providers. Bob has extensive experience in IT security architecture strategy and security program development and management, including executive management experience. Specific security process experience includes security policy and governance, computer and data protection, identity management including multi-factor authentication, risk analysis and threat assessment, business continuity and disaster recovery, incident response and forensic investigation, training and awareness, intrusion detection and monitoring, IT audit and change management with assurance, PKI and encryption, and secure application development. Bob is familiar with numerous security standards including NIST, (including FISMA, PIV, and HSPD-12), Cobit, NERC CIP, and ITIL security management. Representative recent consulting engagements include:

- Developed the Unified Access Strategy for convergence of physical and logical access control on a smartcard for one of the largest international banking, financial services, and investment corporations.
- Developed the Consumer Authentication Strategy for worldwide clients of one of the “Big 4” audit and consulting companies.
- Conducted a full assessment of the Network and Data Protection infrastructure for the international organization charged with overseeing the global financial system, using the results to develop a comprehensive Security Architecture improvement initiative.
- Developed the strategic Information Security and Identity Management Reference Architecture for a major northeast insurance provider.
- Conducted infrastructure assessments and used the results to develop full Identity and Access Management Strategies for a major international heavy vehicle manufacturer and a major electricity provider in the Northeast.

Prior to joining Gartner/Burton Group in 2008, Mr. Smock spent 17 years as the CISO and Director of IT Security with contractor management responsibilities for providing the protection of NASA’s ground-based IT resources that supported space operations at several NASA manned spaceflight centers. Before that, Mr. Smock provided program management and technical leadership as director of Rockwell International Information Security Consulting, and was the director of R&D for a private engineering and software development firm.

Mr. Smock is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), a certified Project Management Professional (PMP), and is a graduate of the Federal Law Enforcement Training Center (FLETC). He has numerous professional organization affiliations in IT architecture, security, and project management. Bob is also a college-level educator, writer, and public speaker, and holds an approved U.S. Government National Agency Check with Inquiries (NACI) background investigation and (formerly) a SECRET clearance. Mr. Smock also holds a Bachelor of Science degree in Computer Science and Engineering Technology from Texas A&M University.

Kimberly H. May

Director, Gartner Consulting

Kimberly May is an experienced project and delivery consultant with 20 years of IT experience including seven years in security and identity management. She has provided leadership and expertise for numerous successful IT and identity management projects across a wide spectrum of industries including aerospace, defense, financial services, government, health care, education, insurance, manufacturing, and service providers. Kim has extensive experience leading projects focusing on strategic IT planning, identity management, identity data directories, resource provisioning, multi-factor authentication including PIV credentials, PKI, ERP implementations, project management, messaging, desktop strategies, content management, ITIL, and IT governance. Kim has led over 50 IT infrastructure and strategic architecture projects including multiple infrastructure and security technology implementations, migrations and upgrades. Representative consulting engagements include:

- Developed the strategic Information Security and Identity Management Reference Architecture for a major northeast insurance provider.
- Conducted infrastructure assessments and used the results to develop full Identity and Access Management Strategies for a major international heavy vehicle manufacturer and a major electricity provider in the Northeast.
- Supported a state CIO in developing a directory consolidation strategy and governance model as the foundation for identity management information sharing in support of the state's 150,000 employees.
- Conducted a comprehensive study for a global financial services company regarding cloud-based and hosted messaging services.
- Supported a global 100 oil and gas company in development of their enterprise desktop strategy including examination of application and desktop virtualization approaches.
- Developed an enterprise MS SharePoint governance model and implementation strategy for a global greeting card manufacturer.
- Assisted with Service-Oriented Architecture Strategy development and steering for a nationally recognized secure facility. Participated in guidance during implementation.

Prior to joining Gartner/Burton Group, Ms. May was a senior member of the Strategic Planning and Integration Organization reporting to the CIO of a major aerospace contractor at NASA. As such, Kim was responsible for strategic IT decisions, leadership, and delivery of enterprise technology initiatives including a $10M Identity Management implementation, a $63M Oracle e-Business implementation, a $9.4M PeopleSoft HR and Financials re-implementation, and the initial Active Directory implementation/domain consolidation. Kim also led a number of other strategic enterprise infrastructure initiatives including messaging systems, desktop rollouts, compliance measures and other core infrastructure.

Ms. May is a certified Project Management Professional (PMP) with a Masters Certificate in Project Management from Villanova University and an Executive Management certification from Rice University. She is also a member of the Project Management Institute (PMI). Kim holds an approved U.S. Government National Agency Check with Inquiries (NACI) background investigation and has a Bachelor of Science in Finance as well as a B.S. in Marketing from the University of South Florida

Chris Weldon

Associate Director, Gartner Consulting

Chris Weldon is an experienced Information Technology consultant with over 25 years experience in a wide variety of technologies, platforms and architectures. He covers security and risk management, identity and access management, virtualization, infrastructure, enterprise architecture and networking. Prior to joining Gartner, Chris was the Chief Technology Engineer for Infrastructure Engineering at United Space Alliance, L.L.C. at Kennedy Space Center, Florida. There, Chris was responsible for architecture and technical guidance on a variety of areas including Identity and Access Management, Server and Desktop Virtualization, Active Directory, PKI, Centralized Management of Server and Desktop Infrastructure, and Information Technology Security.

Chris has provided significant technical leadership for numerous major, enterprise infrastructure and mission critical systems projects.

Representative consulting engagements include:

- Identity and Access Management assessment, architecture and strategy
- Data Loss Prevention assessment, architecture and strategy
- Security and Risk Management assessment, architecture and strategy
- Disaster Recovery assessment, architecture and strategy
- Desktop Virtualization architecture and strategy
- End User Computing assessment, architecture and strategy

Credentials

Chris holds a Bachelor of Science in Engineering (Aerospace Engineering) and a Master of Engineering in Industrial and Systems Engineering from the University of Florida. He holds U.S. Government-approved technical certifications in Microsoft Windows Administration and Network Security. He also holds an approved U.S. Government National Agency Check with Inquiries (NACI) background investigation. Chris is trained in ITIL Foundations.

Emphases

Infrastructure and Environment Management, Identity and Access Management, Active Directory, Information Technology Security and Risk Management, and Server and Desktop Virtualization.

Randy Stalnaker

Associate Director, Gartner Consulting

Randy Stalnaker is a consultant with 25 years of IT experience including more than 13 years in IT security. Security specific experience includes; risk analysis and threat assessment, risk mitigation strategies, writing security governance policies and procedures, business continuity and disaster recovery, information protection, change impact assessment and secure communications.

Representative consulting engagements include:

- Baseline security gap and maturity assessments
- Developed risk mitigation strategy and deployment plans
- Wide Area and Local Network assessments

Prior to joining Gartner in 2011 Randy lead a team that brought the NASA Shuttle support systems into compliance with Federal Information Security Management Act of 2002 (FISMA) regulations. To complete the FISMA compliance effort he worked with NASA to and several contractors to help define the NIST requirement implementation needs in the NASA environment. Randy's experience includes risk assessments for more than 40 systems managed for or by NASA from administrative to mission critical systems. Randy was the Computer Security Official for the Shuttle Launch Processing System from the inception of FISMA requirements till the last Shuttle launch in 2011. Randy was on the team that developed and tracked the risk mitigation plans for the NASA Shuttle systems to gain accreditation per the National Institute of Standards and Technology 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems.

Randy is a Certified Information Systems Security Professional (CISSP) and a Certified Accreditation Professional. Randy holds an approved U.S. Government National Agency Check with Inquiries (NACI) background investigation and a SECRET clearance. Randy has a Bachelor of Science degree in Business Administration from the University of Florida.

Derek Nwamadi

Associate Director, Gartner Consulting

Mr. Nwamadi has over 13 years of IT consulting and business development experience in a broad range of industries including financial, manufacturing, healthcare, education, utility, communication, and government. Over the past several years he has been dedicated to growing Gartner's Benchmark Analytics consulting practice.

Mr. Nwamadi has led engagement pursuits internationally and is now responsible for delivering various projects associated with security, governance and risk management.

Assignments/engagements include the following:

- A security assessment for a large education institution seeking to identify security-related gaps and the required/desired future state.
- A large statewide Security Program working in conjunction with the State CISO to deliver baselines assessments, recommendations and roadmap.
- An infrastructure and Operations benchmarking assessment for a state agency seeking to baseline their overall IT cost, staffing and services levels and identify key areas for improvements.
- Provided a competitive market price assessment for a tier-1 service provider to ensure that their services are in line with current market trends.
- Provided a competitive market assessment for a large telecommunication provider, including benchmarking data related to pricing and other key factors driving the telecommunication sector.
- Assessed the market competitiveness of this healthcare providers application support services to ensure that they are optimizing their vendor relationships.
- Provided the CIO of a financial services firm with an IT Business Effectiveness assessment to determine the impact, as well as the internal client perception of the firms IT services. This engagement was essential in helping the team to determine service gaps and areas for improvement.
- Provided an Enterprise Computing Overview benchmark for a large financial institution to identify cost, productivity and serve level performance gaps along with recommendations and a foundation for continuous improvement.

Prior to joining Gartner, Mr. Nwamadi worked for various technology companies such as Yahoo and Intel. He also has a strong sales and marketing background.

Education:

Mr. Nwamadi holds a Bachelors of Business Administration in Management degree from Texas Tech University.

Credentials:

Certified Information Systems Security Professional (CISSP)

Daniel G. Beckett, Jr.

Associate Director, Gartner Consulting

Mr. Beckett has over 24 years of experience in information technology, specializing in Privacy, Information Security and Identity Management. As a domain expert, he has published various methodologies, white papers and articles for clients, industry associations, and trade publications. Mr. Beckett has also served as adjunct professor at Michigan State University, teaching and developing the security architecture curriculum for the Department of Telecommunications.

Mr. Beckett's time in industry has encompassed a wide gamut of experience, including web and application development, operations support, systems integration and implementation, program and policy development, strategic consulting and practice development, and independent software sales, training, and implementation. He has real-world experience leading some of the largest Identity Management and Security projects in North America and Europe, spanning Public Sector, Financial Services, Life Sciences, Health Care, Higher Education, Insurance and Manufacturing. Representative engagements include:

- Subject matter expert for all identity- and security-related pursuits at **Covisint**, including the successful extension of the Law Enforcement Information Sharing Program's Trusted Broker project, sponsored by the U.S. Department of Justice, and participation as an advisor to various industry working groups, including Energistics, AIAG, and CableLabs, to help guide the direction of identity, security, and federation standardization.
- As an Adjunct Professor at **Michigan State University**, developed the curriculum for and taught the first information security course in the history of MSU's Computer Science and Telecommunications programs. The course focused on a pragmatic approach to Security Architecture based on industry-recognized good practices and field-tested operational techniques.
- As the Director of Technical Architecture, Identity/Privacy/Security Consulting Services at **Burton Group**:
  - ❑ Project manager, lead consultant, and co-author of an assessment for SecureChannel, a government-wide security infrastructure program for the **Government of Canada**, including the development of an internally-focused Identity Management architecture.
  - ❑ Project manager and lead consultant for the **International Monetary Fund** for developing a comprehensive privacy strategy and program in order to reconcile their constituents' expectations, multi-jurisdictional issues, and the institutions diplomatic immunity.
  - ❑ Project manager and lead consultant for **Eli Lilly** for developing their Identity Management architecture, strategy, and governance program, including assistance with the development of RFP, evaluation criteria, and vendor selection instruments.
  - ❑ Project manager and lead consultant for **Wells Fargo** for developing a comprehensive network security policy and risk management program consistent with industry good practice and ISO17799.
  - ❑ Project manager and lead consultant for **CapitolOne** for developing a comprehensive information security architecture, addressing all aspects of network, infrastructure, and application security.

  - Project manager and lead consultant for **Coca Cola** for reviewing and assessing an enterprise Identity Management strategy and architecture.
- As the CTO and Practice Director (Security & Access Management) at **Dewpoint**:
  - Led a security architecture assessment and the creation of the technology roadmap including the selection and implementation of Calendra CDM, RSA Cleartrust, RSA SecurID, Radiant Logic, AD.
  - For **USFreightways**, provided project oversight for multi-site security vulnerability assessment utilizing ISS Internet Scanner, System Scanner, Database Scanner, and multiple open source tools.
- As the Senior E-Business Architect at **Hayes Lemmerz International**, was responsible for all enterprise information security (including Firewalls & VPNs), enterprise messaging & directory services, and development and maintenance of all public and private websites.

Mr. Beckett is a security subject matter expert and an experience public speaker, including national conferences such as GSA Identity Summit, CableLabs Identity Working Group, AIAG, Catalyst Conference, DIDW, Directory Experts, as well as presentations to regional chapters of organizations such as ISSA, ISACA, and Infragard. Mr. Beckett has published numerous articles and technical white papers on relevant topics to Security, Identity, and Access Management.

Manish H. Jyotishi

Associate Director, Gartner Consulting

Manish Jyotishi is a result-oriented seasoned technology leader with ability to aligning business needs to IT capabilities. He has more than 15 years of experience in the IT Industry with proven track record solving challenging business problem with innovative, scalable, and profitable enterprise solutions. His work experience includes development and execution of the global IT Infrastructure strategies, business plan development, program and portfolio management, process engineering, and P&L based product and operation management.

In his current assignment at the NYC Local Government, Mr. Jyotishi is supporting government agencies with the delivery of$42 Million IT services portfolio management in support of modernization and the consolidation of the NYC public safety infrastructure and the call dispatch functionalities. The focus includes development of the Infrastructure strategy, Execution methodology, Performance metrics, Governance model, and Operational support methodology for Network and Security infrastructures. Furthermore, he is also spearheading the development of project framework, risk analysis and the mitigation strategy to effectively implement the interoperable communications and information sharing platform across all NYC public safety agencies.

Past experiences include:

- Assisted with the development of a product strategy for the global low latency trading, market data, and clearing infrastructure platform.
- Architected, implemented, and provided day-to-day management of the global network infrastructure providing consolidated access to the global financial market. Managed and directed team to support pre and post-sales operations of $25 million product delivery.
- Advised financial services company on global market data and trading platform service contracts.
- Developed voice network strategy for the stock exchange trading platform to transform to modernized Voice-over-IP (VOIP) based technologies.
- Assisted stock exchanges in renegotiating MPLS and the Extranet data network contracts.
- Assisted with the development of an RFP for a national managed data network. Developed operational practices to provide SLA backed network provisioning and performance systems.
- Spearheaded Business Development activities for IP based Electronic Pool Notification (EPN) and Mortgage Backed Security Clearance Infrastructure.
- As part of Technical business development, assisted a number of multi-national financial services providers in selecting a vendor for their global data networks based on MPLS and Extranet architecture.
- Prepared an IT Infrastructure Disaster Recovery for the leading banks and the trading partners.
- On behalf of a Financial Clearance Companies, assisted with the development of IT Infrastructure and the Data Center consolidation strategy.
- Developed global LAN and WAN network strategy for prominent insurance company.

- Development IT and Security framework for the financial service providers.
- On behalf of a leading stock exchange, developed the IT provisioning process and the matching SLA to enhance operational performance measurement.

Prior to joining Gartner, Mr. Jyotishi was a Senior Director of NYSE, where he was responsible for leading technical sales engineering, network engineering, project management, and operations management teams. During his tenure at NYSE, he had led numerous critical infrastructure initiatives including roll-out of Financial Extranet, low-latency trading environment, datacenter consolidation, and technical consultative services to the financial institutions and exchanges on the infrastructure enhancements and technology roadmap.

Mr. Jyotishi holds master’s degree in Telecommunications Management (MS) from the Stevens Institute of Technology and an undergraduate degree in Telecommunications Engineering from City University of New York (CUNY).

Douglas Moench

Associate Director, Gartner Consulting

Douglas Moench is an Associate Director for Gartner Consulting specializing in the development of Identity and Access Management (IAM) architectures, provisioning solutions, and federation technologies. Mr. Moench has over 25 years experience documenting current state business processes and related IT system environments, and developing recommendations for improving the infrastructure to simplify administration, improve security, and strengthen collaboration with partners via standards-based technologies.

Since the mid 1980s, Mr. Moench has successfully designed and implemented general-purpose directory, access management, provisioning, and federation solutions for various national and international companies and consortiums, including many Fortune 500 companies. Mr. Moench joined Burton Group in March 2000, and became a Gartner employee with the recent acquisition.

Recent assignments include:

- Development of detailed strategy assessments for the United States and Canadian eGov initiatives.
- Development of global Active Directory designs and identity management strategies and architectures for global manufacturing, energy, higher education, health care, and financial services organizations
- Contributed to Burton Group's Reference Architecture methodologies and best practices in the identity management and security spaces

Previously, Mr. Moench held various Management, Project Management, and Technical Lead positions for companies in the computing, IT services and electric utilities industries. He has received numerous awards for technical innovation and achievement and is a 1981 graduate of the State University of New York at Potsdam. Mr. Moench is based in the Albany, New York area.

Doug Simmons

VP and Practice Leader for Security and Risk Management, Gartner Consulting

Doug Simmons brings more than 25 years of experience in IT security and identity and access management (IAM). He has performed hundreds of engagements as the subject matter expert, and for the past several years has lead a team of senior consultants focused solely on IT security, risk management and IAM. This work includes information protection posture (IT security) assessments, data loss prevention (DLP) strategies, IAM strategies, architectures and source selection of technologies including directory services, meta-directory services, role management and role based access controls, e-authentication solutions, digital certificates and PKI, and single sign-on (SSO). Additionally, his security work has covered process areas such as human resources, content management, IT, physical and personnel security as well as specific business processes. Mr. Simmons has experience with a broad range of security products and solutions from BM/Tivoli, CA, Oracle, Symantec, McAfee and many others. A few illustrative samples of Mr. Simmons's recent consulting experience include:

- Developed the access management and data protection architecture for the National Nuclear Security Administration (under the Department of Energy), comprised of a dozen autonomous yet collaborative nuclear weapons engineering, manufacturing and testing sites. Architecture included cross-site Kerberos authentication, federated web authentication and virtualization of autonomous user databases into a single logical LDAP structure, which is used for authentication and application authorization. Architecture components include LDAP directory servers, LDAP proxy servers, meta-directory and user management utilities.

- Developed a security architecture and enterprise governance strategy for a large North American electric utility company that focused on meeting NERC Critical Infrastructure Protection (CIP) requirements and improving overall security posture between Operations Technology (OT) and corporate IT.

- Conducted IT security and information protection posture assessment for a global electronics manufacturer, leading to restructuring and re-budgeting for the Chief Information Security Officer (CISO) function and a number of process and technical improvements.

- Designed the security architecture to support a global PKI implementation for a large, multi-national credit card company. Design included publishing certificates and CRLs to an existing LDAP directory infrastructure as well as to new certificate repositories for use by end users, servers and network devices.

- Conducted a Visioning and Planning engagement involving recognized industry security experts to develop a strategy and architecture for technology and investment planning for one of the U.S.'s largest banks and financial services companies.

- Assisted the Federal Reserve Bank in developing their current information protection strategy through the delivery of a series of workshops.

Mr. Simmons received a Bachelor of Science degree in computer science and a second major in business administration from Bryan University' in May of 1989. Prior to working at

Gartner, Mr. Simmons worked at IBM from 1989-1995, first as an X.500 directory services engineer and then as an IAM and network security consultant for the IBM Consulting Group.

Jeff Perkins

Managing Partner, Gartner Consulting

Jeff Perkins has more than 20 years of consulting experience in business and IT alignment, IT strategic planning, IT performance optimization, business process analysis, software and systems integration procurement, program and project management, and large systems integration. Jeff joined Gartner's IT Management Consulting practice in 2000. He is a managing partner within Gartner's state and local government consulting practice and he also has significant consulting experience financial services and manufacturing industries. Prior to joining Gartner, he had an extensive career in systems integration for federal government and telecommunications clients.

Jeff has recently managed and participated in the following engagements:

- For a multiple, large states, led the development of the Health Information Exchange (HIE) strategic and operational plan for a statewide health information exchange. The plan were developed to be aligned to the Office of the National Coordinator's State Health Information Exchange Cooperative Agreement Program and as a grant HIE requirement. Also led development of the HIE Financial Sustainability Plan, which was recognized by ONC as a model sustainability plan for states.
- For a large state's Office of Health Care Reform, led the development of the Health Information Exchange (HIE) strategic plan for a statewide health information exchange. The strategic plan was developed aligned to the Office of the National Coordinator's State Health Information Exchange Cooperative Agreement Program and as a grant HIE requirement.
- For a state Department of Mental Health, Jeff led the program definition, business process analysis, and procurement support for an enterprise electronic health record and health information exchange software solutions and systems implementation services. Under Jeff's leadership, the Gartner team developed a number of program level deliverables prior to creation of the procurement documents. These deliverables include program readiness assessment; program charter and plan; change management plan; and governance structure and processes. The procurement deliverables created by Gartner include business process analysis; use cases; functional requirements, technical requirements, implementation and support requirements; vendor market scan; and formal request for proposal solicitation. As a result of Gartner's efforts, the State was able to prepare the enterprise organization for a successful software and services procurement which is expect to start in early 2009.
- For a large state Department of Motor Vehicles, Jeff led the program redesign and business process analysis support for the DMV enterprise motor vehicles platform. Under Jeff's leadership, the Gartner team assessed, validated, and where necessary identified how to improve key artifacts to be included as part of the subsequent vendor RFP, such as Business use case templates; identification of core use cases for the RFP; consistency, content sufficiency and prioritization of business use case content; conceptual architecture structure, content sufficiency and proposed DDI sequencing; and traceability of functional, technical and implementation requirements through-out the life cycle of the system.

- For a state government funded insurance provider, Jeff led an assessment and analysis the current state core insurance platform in order to develop a future strategy for the organization's platform direction. Gartner's efforts included requirements review, alternatives analysis, risk analysis, technical architecture analysis, cost-benefit analysis, vendor market scan, IT operations, and software development lifecycle review. As a result of Gartner's insight and thorough analysis, the client's Board of Directors approved Gartner's recommendation to move away from home-grown core insurance platforms and begin the process of procurement market available software solutions which will offer greater agility, flexibility, and scalability — all at lower total costs for the client.
- For a statewide law enforcement agency, Jeff led the procurement support efforts to negotiate an effective statement of work between the state agency and a software and systems integration vendor. Gartner's work included a review of stakeholder alignment and program readiness; assessing lessons learned from the agency's prior contract efforts; review and validation of functional and non-functional requirements, including identification of key gaps; development of implementation services statement of work and contract terms and conditions; assisting in review and finalizing statement of work and contract terms and conditions with vendor.
- For Federal government health organization, Jeff led the procurement support effort to bring on board a qualified management and technology consultant to define the future of the agency major business transformation effort. The Gartner team led agency's efforts to identify the list of qualified providers, define the high-level requirements to be included within the solicitation, develop the solicitation document, prepare the CDC team to evaluate vendor responses, and assist the procurement organization in managing the solicitation process — resulting in a successful award under critical and aggressive timelines. The Gartner team also providing management advice on the program conceptual design, organization structure, and governance.
- For a large city government, Jeff led the cross-agency efforts to define the business process analysis and platform strategy for a key enterprise criminal justice application. The purpose of the effort was to expand the thinking of key city-wide process beyond the traditional agency silos, as well as identify an appropriate path forward for city-wide improvement of key operations. The effort included current-state and future-state process analysis and concluded with actionable recommendations for improving city operations across criminal justice, courts, and financial operations.
- For a $13 billion business services firm, Jeff provided critical program management guidance for the project definition phase of a global business transformation initiative. The large transformation initiative was expected to cost in the $100 million to $200 million range and would impact approximately 70,000 employees of the business services firm. Jeff's particular guidance centered on defining the subsequent phases of the transformation effort and defining the business case required to support this initiative.
- For a large county government, Jeff managed the engagement team performing the software vendor and systems integrator selection process for a $20 million enterprise resource planning solution, including finance, human resources and customer management requirements gathering; RFP development; RFP issuance; vendor scoring; vendor scripted demonstrations; final vendor selection; and contract negotiations.
- For a $200 million shared services organization, Jeff led Gartner's team in the cost performance assessment of the shared services organization. The engagement focused on internal and market based efficiency comparisons and resulted in actionable

recommendations for achieving significant annual cost savings going forward. As a follow-up to the initial performance assessment, Jeff also led the team's efforts in developing a telecommunications vendor renegotiation strategy and conducting vendor negotiations, which resulted in over $5.5 million in annual savings for the client.

- For a $3 billion consumer goods manufacturer, Jeff led the development of a three to five-year IT roadmap as part of an overall IT strategy planning effort. The project placed significant emphasis on business and IT alignment, project and applications portfolio management, and IT governance. The engagement resulted in defining the path forward for the client IT organization and took into account both internal and external considerations in the prioritization of future initiatives. A critical success factor for the engagement was building consensus within both business and IT leadership so that everyone was in agreement on the final IT roadmap.
- For a $400 million business services firm, Jeff validated the IT strategy on behalf of the CIO and Board of Directors. Jeff led the development of recommendations to improve the IT organizations management and governance practices and launched new IT initiatives to improve business and IT alignment.
- For a $40 billion diversified manufacturer, Jeff led an IT governance case study effort on behalf of the firm's newly appointed CIO The case study focused on demonstrating key concepts of IT governance applicable to large, diversified corporations.
- For a $13 billion diversified manufacturer, Jeff played a key role in advising the global CIO, business segment leaders, and business unit CIOs in the alignment of IT strategy to new corporate initiatives. As part of this engagement, Jeff led the Business-IT alignment workshop with the IT and business leaders. The overall engagement resulted in a revised IT strategy with an emphasis on meeting cross-business strategic needs and offering flexibility for growth through acquisitions.
- For a major airline, Jeff led the cost performance assessment for both infrastructure operations and application development activities. The project included establishing baseline costs, comparing costs against average and top performing companies, and advising the CIO on actionable recommendations for achieving cost savings of over $20 million.
- For a $2 billion mortgage division of a large financial services company, Jeff led an IT efficiency improvement initiative, which included establishing baseline cost of IT operations, identifying major areas for efficiency improvements, launching efforts to realize targeted efficiency gains, and establishing procedures for tracking efficiency improvements over time.
- On behalf of a large non-profit organization's CEO and CFO, Jeff shared leadership responsibilities in the development of a business-driven IT strategy. The project included IT strategy alignment, IT governance, technology architecture, and major initiative prioritization.
- For a large soft-drink bottler, Jeff led the effort of advising the CIO regarding risks associated with the firm's ERP strategy. The engagement resulted in a modified ERP strategy which decreased overall risk exposure and lowered the ERP total cost of ownership by approximately 25 percent, while positioning the firm for improvements in process and data integration.
- For the Department of State Treasury within a large state government, Jeff led the RFP development and vendor selection process of a $6 million core banking solution,

including requirements gathering, RFP development, RFP evaluation, vendor scoring, vendor scripted demonstrations, and final vendor selection.

Prior to joining Gartner, Jeff was a program manager for a leading systems integration and professional services firm. He is a graduate of Auburn University, where he received a BS degree in computer engineering and also earned an MBA in management and strategy from Emory University, where he graduated with distinction. Jeff is a member of Beta Gamma Sigma.

Kris A. Doering

Senior Director, Gartner Consulting

Kris Doering has more than 21 years of outsourcing experience in the areas of finance, business development, sales, contracts, and project management.

While with Gartner, Mr. Doering has worked with Fortune 500 clients in finance and banking services, manufacturing, healthcare, utilities, insurance, telecommunications, outsourcing, state and local governments, and various branches of the US Federal government. Engagement examples include:

- For a global, diversified **manufacturing** organization—assessed existing sourcing strategy and assisted in the development of short- and long-term improvements to optimize business results including transitioning the client from a single source to a multi-source environment
- For a major **transportation** company —assessed existing outsourcing agreement vs. best practices and developed strategic sourcing recommendations on enterprise operations center, desktop support, help desk, data network and voice communications.
- For a multi-national **energy** company – performed an IT strategy and assessment on the efficiency and effectiveness of their infrastructure and application delivery areas
- For a global **automotive supplier** — led the team which provided an assessment of the efficiency and effectiveness of the computing services provided by the External Service Provider (ESP)
- For a large **state government** agency – provided an assessment of the efficiency of their business processes
- For a **distribution** company — provided financial analysis and scenario modeling to develop the company's future state support organization and sourcing delivery model
- For a leading provider of **telecommunication** services — provided an assessment of the efficiency and effectiveness of the computing services provided by the External Service Provider (ESP)
- For a major **healthcare** provider—developed service-level agreements covering all IT service delivery areas to be used in conjunction with a renewal of its outsourcing agreement

Prior to joining Gartner, Mr. Doering was employed by Nortel Networks Corporation (Nortel). He held a variety of positions within the network outsourcing practice at Nortel including sales, program management, and business development. These responsibilities enabled Mr. Doering to oversee the profitability and new service introduction for a $100 million revenue base, negotiate multiple global outsourcing deals with customers for a total contract value of more than $200 million, and develop the project management discipline within the outsourcing practice at Nortel.

Prior to joining Nortel, Mr. Doering was employed by Electronic Data Systems Corporation (EDS). He held the positions of senior director, business development, and senior financial analyst within EDS' financial industry group. These responsibilities enabled Mr. Doering to participate in the creation, development, and financial/business structuring of new global financial industry outsourcing contracts worth more than $500 million to EDS.

Mr. Doering earned a Bachelor of Science degree in business administration from the University of Texas at Dallas (UTD). He has held several professional certifications, including Project Management Professional (PMP), Certified Public Accountant (CPA), Certified Management Accountant (CMA), and ITIL Foundation.

Mike Samsen

Vice President, Gartner Consulting

Michael Samsen has more than 30 years of consulting experience, technical leadership and business management experience. He focuses on IT strategy, IT assessment, IT governance, IT performance management, business and technology planning, and management of information intensive businesses. Mr. Samsen is the global lead for Gartner's Business Consulting Solution and the IT Strategy practice. He joined Gartner in 2003 and is based in the Stamford, Connecticut, headquarters. He recently led a multi-year and comprehensive enterprise strategy and planning effort for a local government organization with annual budget in excess of $50 billion.

Prior to joining Gartner, Mr. Samsen was an associate partner with Accenture's Strategic IT Effectiveness practice and a principal with Booz, Allen and Hamilton's Information Technology Group. In addition, he held line operations management positions in financial services, including vice president and division executive for the Global Securities Services business of Bankers Trust and several line operations management positions in securities processing and retail banking at Citibank.

Representative engagement experience includes:

- For a central bank — assessed the IT governance structure across the entire, highly federated organization and recommended improvements to improve the effectiveness and efficiency of IT decision-making.
- For a global electronics parts and services provider — led a team to develop an Enterprise Architecture governance model, including key processes and structures. The new model integrated previously disconnected stakeholders and allowed the client to more effectively move forward with the revitalization of its enterprise architecture.
- For a healthcare provider — developed an IT balanced scorecard, including identifying the key business goals and related IT goals, developing key IT objectives, and specifying key measures and targets for each of the objectives.
- For a defense industry integrator — led a joint Gartner/client team to develop and IT balanced scorecard. The engagement allowed the client to move forward on this key management reporting initiative which had been plagued with false starts and lack of demonstrable progress.
- For a federal executive office agency — facilitated the development of a performance reporting mechanism, including coaching on best practices and analytical frameworks.
- For a global automobile manufacturer — assessed the human capital management environment and developed a long-term vision to address identified gaps and meet future business requirements.
- For a non-profit organization — developed an IT strategy for the business owners including clarifying the business strategies, determining the IT implications, assessing the current state IT environment, aligning IT initiatives with the business needs, defining a high-level IT architecture, and developing a migration plan.
- For a Central European bank — developed an IT strategy to support planned privatization and entry into major new markets and product lines. Improved client's position as a potential investment target for Western European banks.

- For a money center bank — developed an IT strategy for the retail banking group. Strategy focused on transforming the IT organization from an order-taking support group to a proactive member of the business management team. Recommendations included significant organizational restructuring, implementation of a new architecture, and a comprehensive IT renewal plan.
- For a major Asia/Pacific bank — led an engagement to significantly improve the cost-income ratios of its four European subsidiaries by introducing a common technology platform and reengineering the retail branch operations. Recommendations included consolidating operations functions, adopting world class best practices, refocusing branch activities on sales, and implementing a new management structure.
- For a large insurance company — led a systems assessment and developed an IT strategy to align IT initiatives with the business's strategic direction. Created an action plan for addressing technology capability gaps. Repositioned the technology organization to become a business partner.
- For an insurance company — led a root-cause analysis of customer service requests and developed recommendations for reengineering business processes and associated technology to eliminate the causes. Significantly reduced customer service call and correspondence volume.
- For the wealth management business of a leading bank — led a project to assess the adequacy of current technology, evaluate management and governance processes, align the IT strategy with business objectives, and analyze the overall IT cost position. Recommended technology architecture and strategic focus that redirected investments from legacy core processing to more strategic, customer-facing capabilities.
- For a strategic alliance of several major capital markets firms — developed a business case, created an overall systems architecture, and conducted an operational feasibility analysis for creating a joint back-office utility. The architecture combined the core, non-proprietary functions to achieve scale economies, while maintaining the key proprietary capabilities of the individual participants. The resulting configuration dramatically reduced operating costs while maintaining competitive differentiation of each of the participating firms.
- For a leading consultancy — led a cross-functional team to develop a global solutions delivery and outsourcing operating model, resulting in overall cost improvement of 40 percent. Key components included offshore development centers, integrated global delivery center network, cost-effective workforce, and supporting methodologies and tools.

Mr. Samsen holds a BSEE in computer science from Princeton University and an MSIA (MBA) from Carnegie Mellon University.

Any questions regarding this Statement of Work should be addressed to:

Jeff Perkins
Managing Partner, State of Local Government
Gartner, Inc.
Gartner, Inc.
10 Glenlake Parkway, Suite 390
Atlanta, Georgia 30328
Telephone: +1 770-913-2376
Facsimile: +1 770-913-2310
Email: Jeff.Perkins@gartner.com

This Statement of Work was prepared for State of South Carolina - Division of State Information Technology:

Jimmy Earley
Chief Information Officer
State of South Carolina - Division of State Information Technology
SC Budget and Control Board
DSIT
4430 Broad River Rd
Columbia, SC 29210

Telephone: +1 803-896-0222
Email: jearley@cio.sc.gov