Deloitte.

State of South Carolina Information Security and Privacy Final Report

Public Report

Contents

Our services were performed in accordance with the Statement on Standards for Consulting Services that is issued by the American Institute of Certified Public Accountants (AICPA). We provided to the State of South Carolina our observations and recommendations. However, our services did not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, we will not express an opinion or other form of assurance with respect to our services. In addition, our services did not constitute an examination or compilation of prospective financial information in accordance with standards established by the AICPA. We did not provide any legal advice regarding our services; the responsibility for all legal issues with respect to these matters is the State of South Carolina's. It is further understood that the State of South Carolina's management is responsible for, among other things, identifying and ensuring compliance with laws and regulations applicable to the State of South Carolina's activities.

The sufficiency of the services performed is solely the responsibility of the State of South Carolina. In addition, we assumed that the information and data provided to us by the State of South Carolina was complete and accurate.

1. Executive Summary

Since March 22, 2013, Deloitte & Touche LLP ("Deloitte & Touche" or "D&T", or "we") has assisted the State of South Carolina ("State") in assessing its information security and privacy risks and vulnerabilities. In addition, D&T has assisted the State with the development and implementation of a statewide Information Security ("INFOSEC") and Privacy program. This *Information Security and Privacy Final Report* provides observations by D&T since the initiation of the engagement and includes remediation recommendations related to the ongoing implementation of the INFOSEC and Privacy programs.

The executive summary is divided into three sections: (1.) Security Assessment Background and Results; (2.) INFOSEC and Privacy Program Progress; and (3.) INFOSEC and Privacy Program Recommendations. Each section is subdivided into three dimensions of information security and privacy: People; IT Security Processes; and IT Security Technology.

1. Security Assessment Background and Results

Deloitte & Touche conducted 18 agency INFOSEC and Privacy program assessments. Each agency assessment included both a technical Information Technology (IT) vulnerability assessment and a broad IT security risk assessment. The information security risk assessments ("ISRA") evaluated the agencies' security controls against the State's information security framework.

Analysis of the aggregated assessment results identified a number of high-risk INFOSEC program area weaknesses. Additional identified risks and program development needs are outlined in sections 3-5.

People

- No statewide INFOSEC or Privacy organization to provide standardized, consistent guidance to agencies. This has contributed to inconsistent policies and technologies, as well as ad-hoc, duplicative procurement and implementation of information security and privacy tools among agencies.

- Lack of security awareness and privacy training available to employees and contractors serving the State. Security awareness and privacy training is foundational for effective INFOSEC and Privacy programs and is consistently identified as a top cybersecurity initiative for states. Page 8. ***2014 Deloitte-NASCIO Cybersecurity Study - State governments at risk: Time to Move Forward* October 2014**.

- Lack of qualified cybersecurity professionals and specialized INFOSEC and Privacy training. As a common practice, agencies had staff performing security and privacy job functions without training or certifications. Open positions were difficult to fill due to lack of availability of qualified candidates and salary constraints.

IT Security Processes

- Inconsistent business continuity management (BCM). Evaluation of the agencies revealed that 72% had no formalized business contingency documentation and processes, putting mission delivery at risk in the event of a natural disaster or a man-made disaster or crisis such as a cyber-attack.

- Lack of IT risk management and IT risk strategy. Of the agencies evaluated, 66% had not developed an IT risk strategy outlining how their security risks would be mitigated, transferred, or accepted. Agencies were unaware where they had INFOSEC risks (e.g., out-of-support Microsoft XP systems) within their organizations.

- Poor security governance and management. In total, 60% of assessed agencies lacked effective processes for security management. The assessments identified **50** examples of missing security updates for known security vulnerabilities. In addition, over **100** examples of improper or weak configuration management were found. If exploited, vulnerabilities could lead to compromise of citizen and State data, as well as it could affect the availability of mission-critical systems.

IT Security Technology

- Lack of patch management tools. The evaluation indicated that 60% of the assessed agencies did not have a tool to support the process of identifying and installing security updates on systems, which serve to reduce the risk of exploitation of known vulnerabilities.

- Inconsistent use of multifactor authentication. More than half of assessed agencies that processed sensitive data lacked multifactor authentication for individuals with direct access to sensitive citizen data.

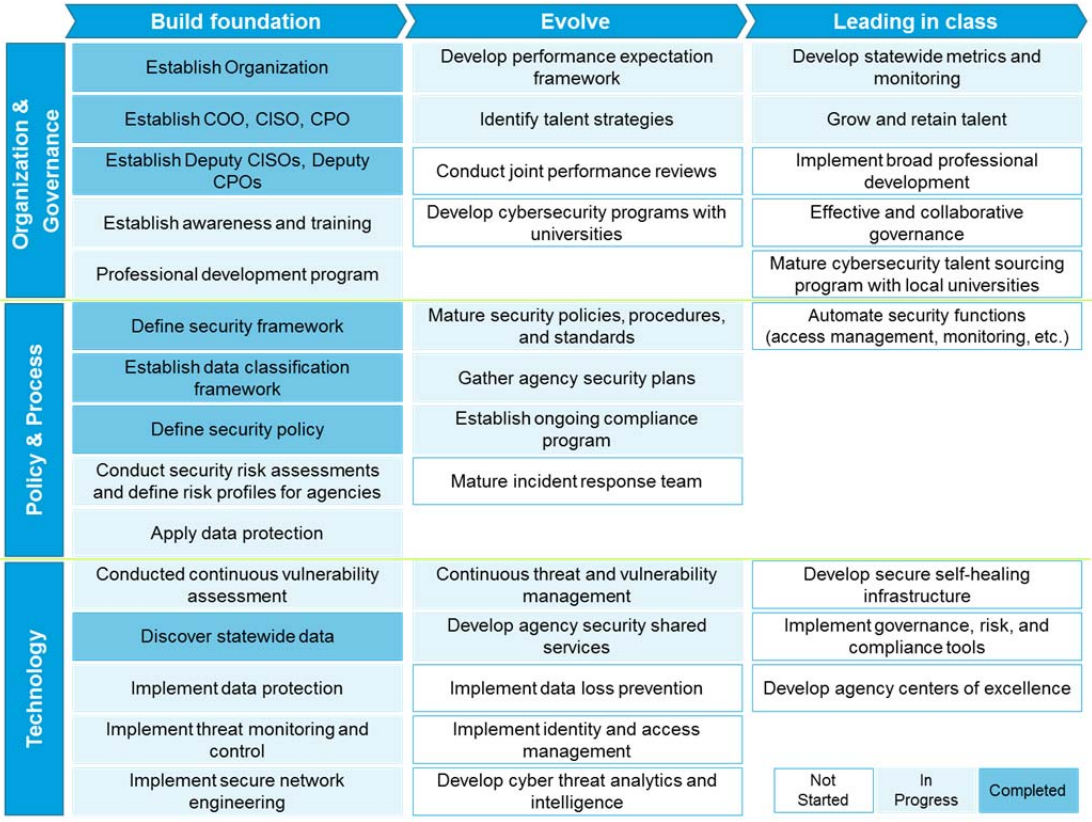
- Inconsistent use of encryption. More than half of assessed agencies were using no encryption, or only partial encryption, to protect sensitive data. This is especially important for mobile devices such as laptops, which are easily lost or stolen.

- Islands of computing. Many State agencies operate their own IT infrastructures, from servers in unprotected closets to data centers. This decentralized approach presents a number of risks and program challenges, including increased complexity for the implementation of statewide security information event monitoring (SIEM); proliferation of security tool vendors selected to provide security capabilities; inability to efficiently provide reporting on the security posture of the State; and additional cost and time required to roll out statewide consolidated service security tools and programs.

2. INFOSEC and Privacy Program Progress

Deloitte & Touche provided recommendations as part of a multi-year roadmap for the implementation of the State's INFOSEC program. At the time of this report, the Division of Information Security (DIS) and Enterprise Privacy Office (EPO) are "in process" of developing and delivering a number of the INFOSEC initiatives.

Figure 1: D&T recommended INFOSEC and Privacy roadmap*



*Status of the roadmap activities represents progress made by State leadership, DT, DIS, and EPO. Progress made by individual agencies is not represented.

Due in part to the autonomy of each individual agency's IT procurement practices (including security tools) and the historical lack of a statewide information security function prior to the creation of the Division of Information Security (DIS), the INFOSEC and Privacy policies, processes, and technologies vary significantly among State agencies. As a result, implementation of the statewide INFOSEC program is complex and time consuming, requiring significant financial, time, and human resource commitment. This is most evident with the implementation of statewide INFOSEC technology solutions, which are required to work in IT environments that differ significantly from agency to agency.

While the DIS and the EPO have defined statewide policies, processes, and initiated the rollout of enterprise solutions, agencies will need time for implementation within their respective organizations.

The following outlines progress the State has made in implementing the INFOSEC program.

People

- Implementing a federated information security governance model. Statewide INFOSEC professionals report directly to the Chief Operating Officer ("COO") of the Division of Technology ("DT"), including the State's Chief Information Security Officer ("CISO") as head of the DIS, and the State's Chief Privacy Officer ("CPO") responsible for the EPO. The State has also filled all Deputy CISO ("D-CISO") positions within DIS, two Deputy Chief Privacy Officers ("D-CPO") within the EPO, and continues to hire information security professionals for the INFOSEC program.

- Building a professional development program. The program is designed to attract, train/develop, and retain INFOSEC and Privacy staff.

- Providing online cybersecurity awareness training for State employees. This training is essential for the State to establish a strong INFOSEC and Privacy posture, as the State's employees are the first line of defense against cybercrime and data breaches**.**

- Providing training to State cybersecurity professionals. This training provides continuous learning opportunities for INFOSEC professionals to develop the skill sets necessary for specialty areas within the cyber-security workforce.

IT Security Processes

- Publishing the State's data classification schema to categorize data for more efficient and effective data protection. This data classification schema helps agencies and the State prioritize investments in information and data security.

- Publishing foundational INFOSEC policies and providing agencies with guidance and education for the adoption and implementation of these policies.

- Developing INFOSEC program key performance indicators ("KPIs"). These KPIs help the State monitor adoption of the INFOSEC policies at State agencies. They are the key input to a program "maturity dashboard" that will facilitate reporting progress made by individual agencies, as well as statewide progress towards the implementation of the INFOSEC and Privacy programs.

IT Security Technology

- Developing and rollout of information security self-assessment tool. State agencies can use the tool for internal risk assessments of INFOSEC capabilities, as well as in developing remediation plans to address the risks identified.

- Initiating statewide implementation of enterprise INFOSEC technology solutions. These include technologies for laptop encryption, virtual private network/two-factor authentication, patch management, privileged user management, enterprise vulnerability assessments, and data discovery.

- Expanding the coverage of the SIEM monitoring solution to non-cabinet agencies. Cabinet agencies were previously integrated per the Governor's executive order in December 2012.

3. INFOSEC and Privacy Program Recommendations

Though initial progress has been made with the INFOSEC program, a significant number of both "foundational" and "evolve" recommendations from the roadmap (in the May 1, 2013, Initial Security Assessment Report) are either in process or not yet started. Agency assessments covered 18 of 73 agencies; considering the significant number of systemic / cross-agency risk areas identified, the State will need to continue investing in the INFOSEC and Privacy program to help mitigate the risk of losing State data and compromising State information systems. The need for continuing investment is especially urgent in light of the ever-increasing sophistication of cyber criminals, who are intent on stealing citizen and business data and compromising critical IT infrastructure.

In addition, it is likely that numerous vulnerabilities exist in agencies that were not surveyed, as well as in other organizations, including municipalities, county offices, and K-12 educational institutions. Organizations that are required to connect to State agencies in order to share data for their respective missions are a point of entry for threats into State information systems.

The monies made available to DIS and EPO to support the statewide initiatives include funding for personnel, security awareness training, and technology initiatives such as two-factor authentication, patch management, encryption, and sensitive data identification. Our estimated budget to fulfill the DIS and EPO FY15 objectives, as outlined in the October 2013 interim report, was $20.8M. The amount funded by the General Assembly was $16.2M. The reduction necessitated extending the timeframe required to implement technologies for the remediation of the State's vulnerabilities and reduced the number of agencies that DIS was able to support during the fiscal year.

Based on common risk areas identified across many of the agencies reviewed, we recommend that the State continue to focus on the development of the statewide INFOSEC and Privacy Programs – specifically the rollout of those initiatives that are currently in flight and initiating additional "evolve" and "leading class" recommendations (from the May 1, 2013 Initial Security Assessment report). In order to meet its recommended goals and objectives, DIS and EPO will need additional sustained funding for ongoing support of statewide security and privacy program needs.

The following provides a summary of the recommended next steps as the State continues to improve its INFOSEC and Privacy programs, makes progress towards addressing INFOSEC and privacy risks, and assists its agencies and institutions in achieving more effective security and privacy postures.

People

- Continue to build an efficient INFOSEC and Privacy governance model. Establish statewide processes and additional shared resources. Focus on delivering effective security and privacy capabilities in a cost-efficient manner.

- Review and improve the security awareness training program. Determine if alternative providers would be more cost-effective and have greater impact.

- Roll out the initial phases of the statewide professional development program. Focus on attracting, developing, and retaining INFOSEC and Privacy staff. These people are on the front lines of safeguarding citizens' data and will help to protect the State against internal and external threats.

- Collaborate further with external organizations that have sophisticated cybersecurity, capabilities. As the cybersecurity mission expands from protection of citizen data to protection of broader statewide critical infrastructure, DIS should further mature the State's Fusion Center (a term for entities that are designed to integrate federal intelligence efforts with those of state and local authorities) capabilities and further develop its relationship with the Multi-State Information Sharing and Analysis Center (MS-ISACs).

IT Security Processes

- Continue to oversee statewide development and rollout of the agency INFOSEC and Privacy programs. This includes such activities as: agency implementation of statewide INFOSEC policies and procedures; agency self-assessments using the State's security framework; completion of asset inventories of the IT environment and subsequent data classification to identify systems and data that require protection; and creation and execution of agency-level risk mitigation plans for risks identified through information security risk assessments.

- Implement a statewide governance, risk and, compliance (GRC) program. This will enable the measurement of the security posture and progress at the agency and statewide levels. This type of program also assists with investment prioritization.

- Continue and improve agency-level implementation of the State's asset inventory and data classification processes. Creating an inventory and data classification identifies what data and systems need protection. The State can then determine what technology investments are required to deliver the needed protection.

IT Security Technology

- Continue deployment of the recommended enterprise technology solutions statewide, including technologies for laptop encryption, virtual private network/two-factor authentication, patch management, privileged user management, enterprise vulnerability assessments, and data discovery.

- Procure and implement an enterprise/statewide GRC tool. This will allow for a tools-based implementation of the GRC processes described above, which provides automation and dashboard reporting capabilities.

- Begin to design and implement a data loss prevention (DLP) solution for agencies that deal with sensitive data. This initiative will build on the foundation constructed during the rollout of data discovery tools.

- Invest in network technology to improve threat detection and containment within the statewide network environment.

- Identify opportunities to provide additional consolidated services and reduce the islands of IT computing. The number of IT computing centers is directly related to the number of INFOSEC controls required to mitigate risk of losing confidentiality, integrity, and availability of the State's IT systems and data. Reducing the number of computing centers will mean fewer devices and systems needing protection and monitoring. Having fewer locations would also lower the cost of statewide business continuity and disaster recovery programs, enable faster rollout of INFOSEC technology solutions, and improve the State's ability to respond to security incidents.

Given the complex, highly autonomous IT operating model and associated INFOSEC and Privacy environments across the State, it will be important, both fiscally and time-wise, to look for opportunities to implement consolidated service models for security. Talent will continue to be an issue for the foreseeable future, and the complexity of implementing processes and technologies in a heterogeneous operating environment means that the investment of time, talent, and budget will need to be maintained, if not grown, for the next five or more years.

The core mission of a state is to provide services to its citizens in a cost-effective and efficient manner, while protecting their confidential information, including tax, health, and other personal information. The State is encouraged to consider the recommendations in this report while making its funding decisions for FY16 and beyond. Reducing investment could have serious implications for the agencies, their missions, and ultimately the citizens of the State of South Carolina.

2. Background and Overview

2.1 Background

On October 10, 2012, the South Carolina Department of Revenue ("SC DOR") discovered a data breach that had compromised tax return data and Personally Identifiable Information ("PII") of South Carolinians.

The State hired Mandiant, a technology consulting company, to assess the extent of the data breach. Mandiant found that an unauthorized party had used a "phishing" email attack to obtain an employee's account information and later leveraged this information to further compromise SC DOR's systems. As a result, attackers were able to exfiltrate / steal a total of 74.7 gigabytes of data from 23 database backup files, which represented approximately 3.8 million taxpayer records.

By October 20, 2012, the Department of Revenue implemented Mandiant's recommended containment plan.

To diminish the chances of further breaches, Governor Nikki Haley requested that the State Office of the Inspector General ("OIG") review South Carolina's information security policies and procedures. On November 30, 2012, the OIG responded with an interim report, "**Current Situation & A Way Forward**." The report concluded that South Carolina lacked a statewide information security policy, writing: "There is no State entity with the authority, or responsibility, to provide leadership, standards, policies, and oversight." It further explained: "By default, authority has been delegated to each agency to decide its own risk tolerance for data loss and its own INFOSEC plan." (OIG, 2012, p. 2)

In the report, The OIG offered three major recommendations:

- First, that the State appoint an interim statewide CISO.
- Second, that the State adopt a federated governance model for data security, rather than either the current decentralized approach, or a less nimble, fully centralized model.
- Third, that South Carolina hire an outside vendor to develop a statewide governance framework and implementation plan that would strengthen its information security posture.

2.2 Overview

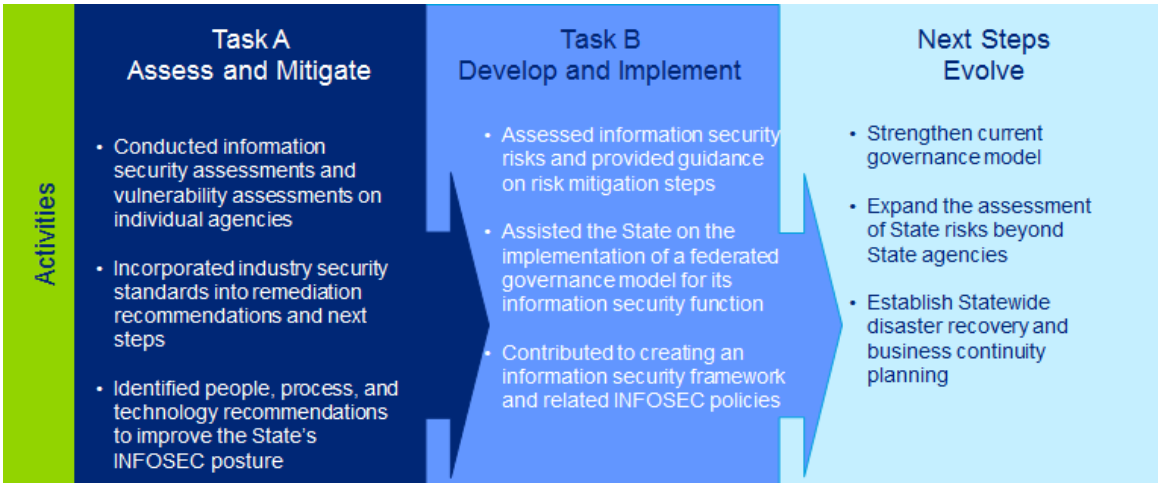
Following a request for proposals (RFP) responded to by Deloitte &Touche, and in which multiple information security vendors participated, the State of South Carolina awarded a three-year information security contract to Deloitte & Touche. The contract contained two task orders:

- Task A, which was to assess and recommend mitigation steps to address security vulnerabilities in an initial five-week effort; and

- Task B, which was to develop and implement an information security program for the State.

The figure below illustrates a summary of activities performed in Task A and Task B, as well as ongoing activities and next steps for the State to improve its information security posture and protection of the information of its citizens and the businesses of the State.

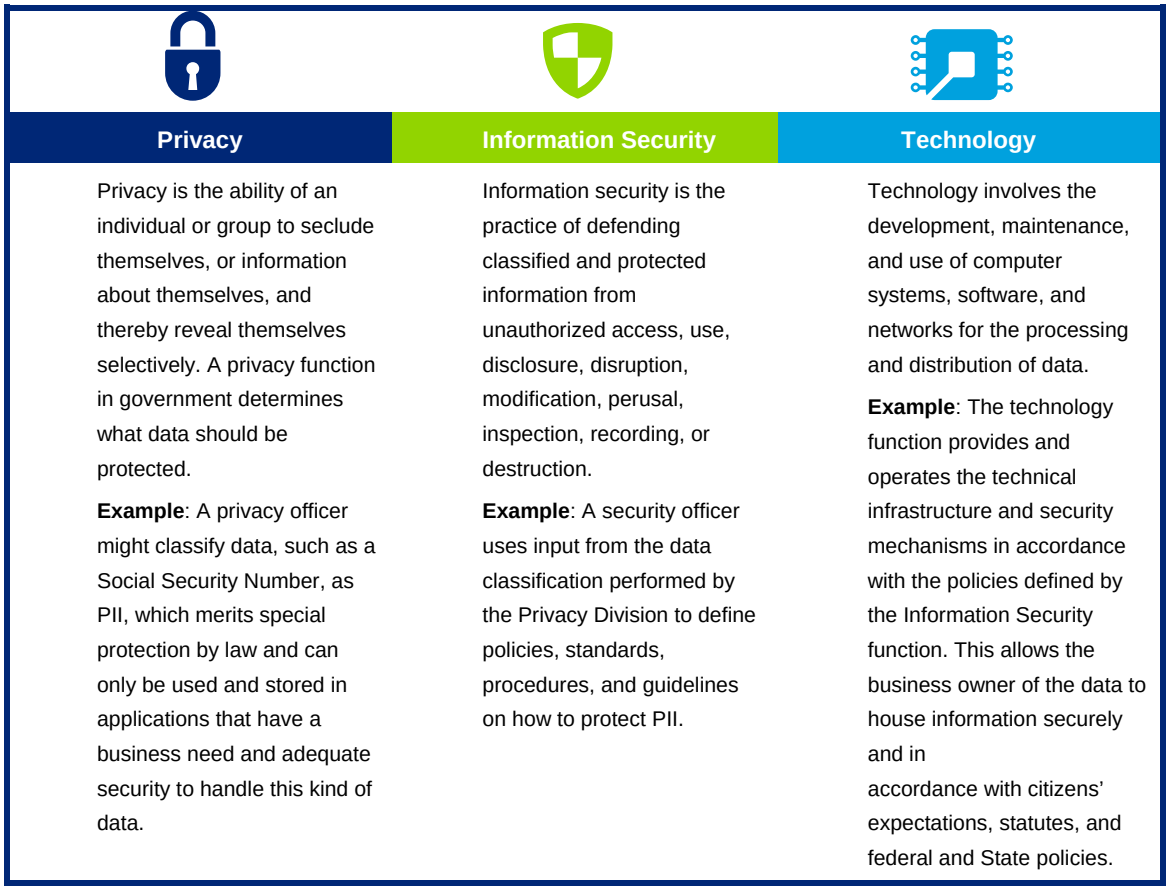
Figure 2: Tasks and Activities



Task A — Assess and Mitigate

As part of Task A, through the initial phase of information security risk assessments and technical assessments, we identified a number of security vulnerabilities within the State. Based on the knowledge gained through the assessments and analysis, we made recommendations to enhance information security. The picture below represents the three major pillars that are the foundation for improving information security within the State. The components build on one another to provide a security solution that helps manage the risk to the State's data-related assets.

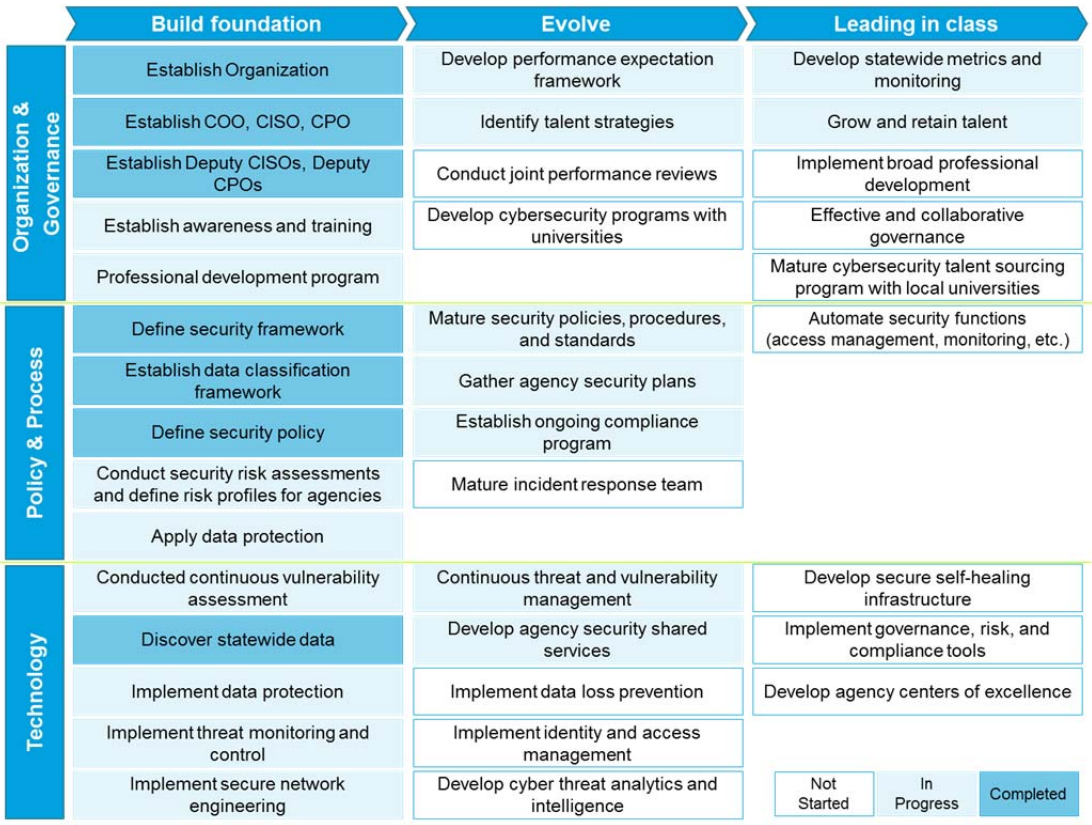
Figure 3: Privacy, Information Security, Technology



We assisted the State by building a roadmap with foundational recommendations for Fiscal Year 2014. Additional risk and vulnerability assessments informed our approach as we continued to identify risks to the State. Phases for implementing the information security program include:

1. **Build Foundation (year 1):** The focus of this phase is on addressing the risks and vulnerabilities identified, as well as implementing the foundational aspects of the INFOSEC and Privacy programs.
2. **Evolve (years 2-4):** This phase consists of building on the foundation that was established in fiscal year 1 and continuing to evolve the program.
3. **Leading in Class (years 5 and beyond):** The focus of this phase is on sustaining leading INFOSEC and Privacy programs that continue to evolve in order to stay on top of rapidly changing cybersecurity threats.

Figure 4: D&T recommended INFOSEC and Privacy roadmap*



*Status of the roadmap activities represents progress made by State leadership, DT, DIS, and EPO. Progress made by individual agencies is not represented.

The three phases reflect the relative maturity of the INFOSEC and Privacy programs and are depicted in Figure 3, above. The activities under each of the phases are grouped into three categories: organization & governance, policy & process, and technology. The majority of Task B's activities and progress fell within the "Build Foundation" and "Evolve" phases of the recommended roadmap. These are the focus of this report. The figure above depicts the progress made on each of the recommendations in the roadmap produced in Task A.

3. Implementing Information Security and Privacy Programs

3.1 Implementing Information Security and Privacy Programs

Based on the recommendations from Task A, we formulated a strategy for Task B to build the INFOSEC and Privacy program foundations from three perspectives:

1. **Organization & Governance:** The organizational recommendations focused on establishing a governance structure, developing a staffing plan, securing funding, developing job descriptions, and hiring resources. The organizational recommendations also included creating an end-user awareness and training program, as well as a professional development program that would formalize expected roles and responsibilities and help build requisite knowledge for the State's Information Security and Privacy talent.

2. **Policy & Process:** The process and policy recommendations focused on development and adoption of enterprise-wide information security policies designed to help agencies improve their data protection and risk management practices, based on the State INFOSEC and Privacy frameworks. A number of initiatives derive from the process and policy recommendations, including data classification, information security risk assessments, and the security framework.

3. **Technology:** The technology recommendations detailed the specific technologies or tools that would improve the State's information security posture. Some of these technologies include:
    - Threat-monitoring and control through a SIEM solution;
    - Secure network engineering through VPN and two-factor authentication; and
    - Data protection through hard drive encryption, patch management, and data discovery tools.

These three types of recommendations offered the State a way to take a multi-faceted approach to strengthening its information security posture. The sections below detail the State's progress in each of these areas, based on the roadmap provided in Task A.

3.2 Organization & Governance Recommendations

Introduction

To enable the State of South Carolina to establish an INFOSEC and Privacy structure, we worked with the DIS to finalize an organizational and governance structure, which includes executive leadership and information security awareness training. The table below details the current status of the Foundation phase of the roadmap that will assist in further developing the State's INFOSEC and Privacy programs.

Figure 5: Organization & Governance Recommendations

Foundation	Current Status	Next Steps
Establish INFOSEC organization with Enterprise Authority: INFOSEC program should have the authority to monitor agencies' compliance with State and federal regulations.	Established a statewide INFOSEC program led by DIS.	Create a compliance-monitoring mechanism. Conduct joint performance reviews by DIS and State agencies.
Establish Chief Operating Officer (COO): Develop a job description, obtain funding, and establish a COO position.	Established a COO for the newly created Division of Technology, which is comprised of three divisions that serve agencies and institutions statewide	Further mature the governance model by establishing communities of interest with representation from State agencies.
Establish CISO: Develop a job description, obtain funding, and establish a CISO position to oversee and provide guidance on statewide INFOSEC initiatives.	Established a CISO as the head for DIS; one of the three divisions that comprise the Division of Technology	Establish security liaisons at State agencies to direct local INFOSEC initiatives in coordination with DIS.
Establish D-CISOs: Develop a job description, obtain funding, and establish the D-CISO positions.	DIS current organization has five D-CISO positions as opposed to the seven positions recommended by D&T. DIS has staffed all five Deputy CISO positions	Implement a mechanism for the ongoing communication and collaboration between D-CISOs and information security liaisons / CISOs at State agencies. Designate a formal role and dedicated resources to establish and manage a communications program for facilitating agency collaboration.
Establish CPO: Develop a job description, obtain funding, and establish a CPO position.	The Division of Technology has created the EPO and has hired D-CPOs.	Staff the CPO position.
Establish End User Awareness Program: Provide employees with relevant security information and training to reduce the number of security incidents.	DIS issued a RFP and has hired a vendor to provide security awareness courses for State employees. Security Awareness 101 and Fundamentals of Social Engineering are currently available online, and new courses are being developed.	Establish a process to help ensure content from courses remains current and is applicable to the State environment and risks. Evaluate the effectiveness of the security awareness training program.
INFOSEC and Privacy Professional Development: Develop training catalog to provide INFOSEC and Privacy professionals with visibility into continuous learning and growth opportunities. Develop an INFOSEC and Privacy training curriculum as a foundational component for the later implementation of a statewide INFOSEC Professional Development Program ("PDP"). Conduct talent assessment to determine immediate, medium-, and long-term staffing requirements.	Developed an INFOSEC and Privacy Training Matrix comprised of INFOSEC and Privacy categories, specialty areas, and associated training courses and certifications. Conducted preliminary workforce assessment activities, such as: • Deployment of an INFOSEC and Privacy skills assessment survey to better understand INFOSEC and Privacy staff at State agencies; and • Execution of focus groups workshops to understand constraints and challenges that INFOSEC and Privacy staff faces in meeting their goals.	Continue to develop a statewide PDP to include: • A specialized training plan for system users with significant security responsibilities; • Increased focus on recruitment and retention of the core INFOSEC and Privacy staff through internships and incentive programs; • Development of a career path model for INFOSEC and Privacy staff to understand what is required to advance their career; and Succession planning activities, such as rotational development programs, to help the State begin cultivating future INFOSEC and Privacy leaders.

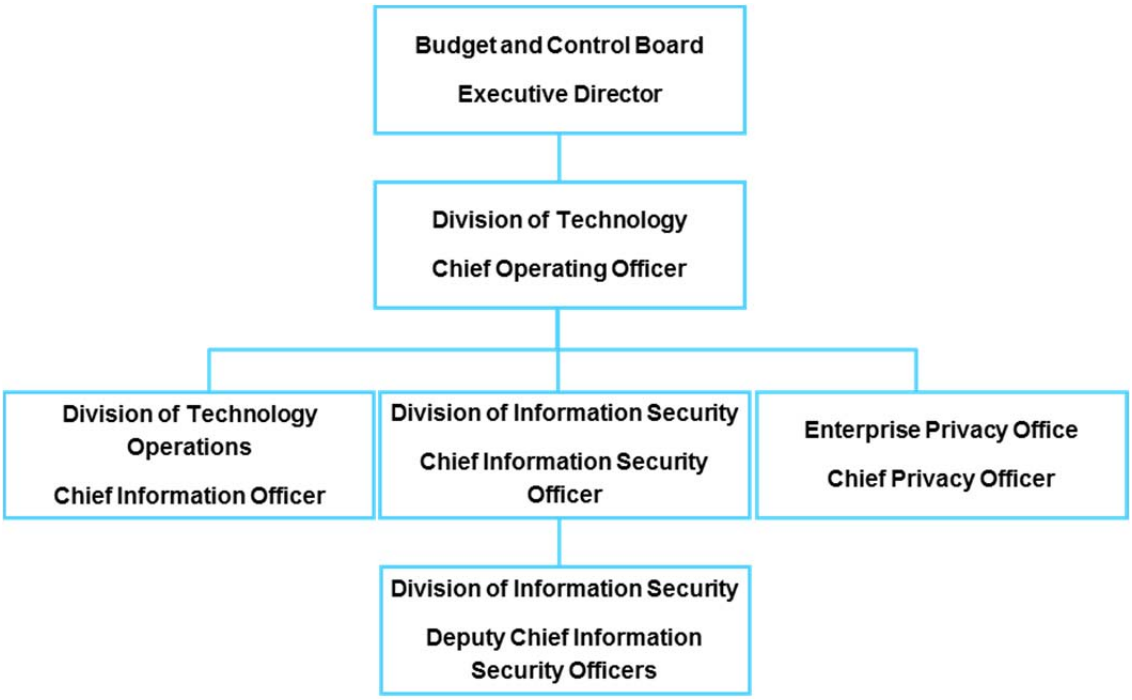
Governance Recommendations

The State has transitioned from a decentralized governance model with little enterprise direction to a federated governance model that allows the enterprise to set the strategy develop frameworks and policies, facilitate communication, and provide subject matter guidance, while agencies remain responsible for the implementation of information security and privacy policies, procedures, and controls. State leadership (COO, CISO, CIO, and CPO) for the federated governance model has been established and communicated to the agencies to encourage consistent practices across the State and to assess compliance and effectiveness. The State should consider establishing cross-functional working groups or committees to further improve its governance structure and promote collaboration across the organization.

Governance Implementation

We recommended several organization and governance strategies, in particular, the establishment of an INFOSEC Organization with enterprise authority. The State acted upon this recommendation by creating the Division of Technology (DT), comprised of the Division of Technology Operations, the Division of Information Security, and the Enterprise Privacy Office. The following illustration depicts the Organization's structure.

Figure 6: State of South Carolina INFOSEC, Privacy, and Technology Organization



The DT sets the direction for the State's use of technology and supports the provision, use, and administration of information technology. This division falls under the Budget and Control Board and consists of three divisions:

1. **DT Operations**: This division is responsible for the enterprise technology efforts.
2. **Division of Information Security**: This division is responsible for the enterprise information security efforts.

3. **EPO**: This division oversees the privacy aspects of the State's data. The EPO is discussed in Section 5, "Implementing a Privacy Program."

Under this organizational structure, the CISO, CIO, and CPO report to the COO, who coordinates centralized activities and functions within the State. The State adopted the initial recommendations and modified them to align with the new leadership's strategy for the enterprise organization.

Figure 7. Governance Model with newly created DIS and EPO

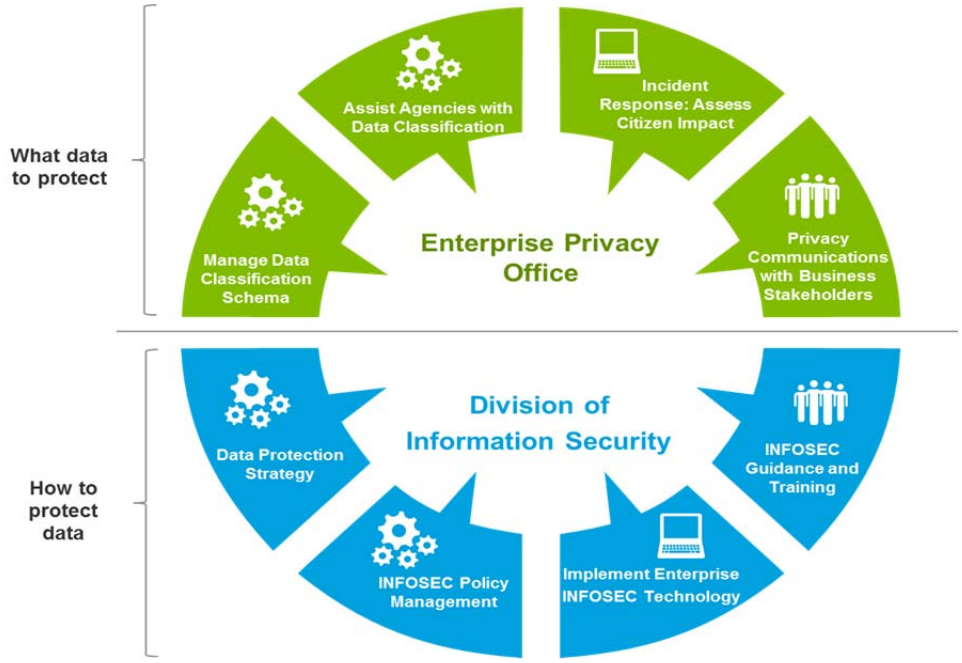
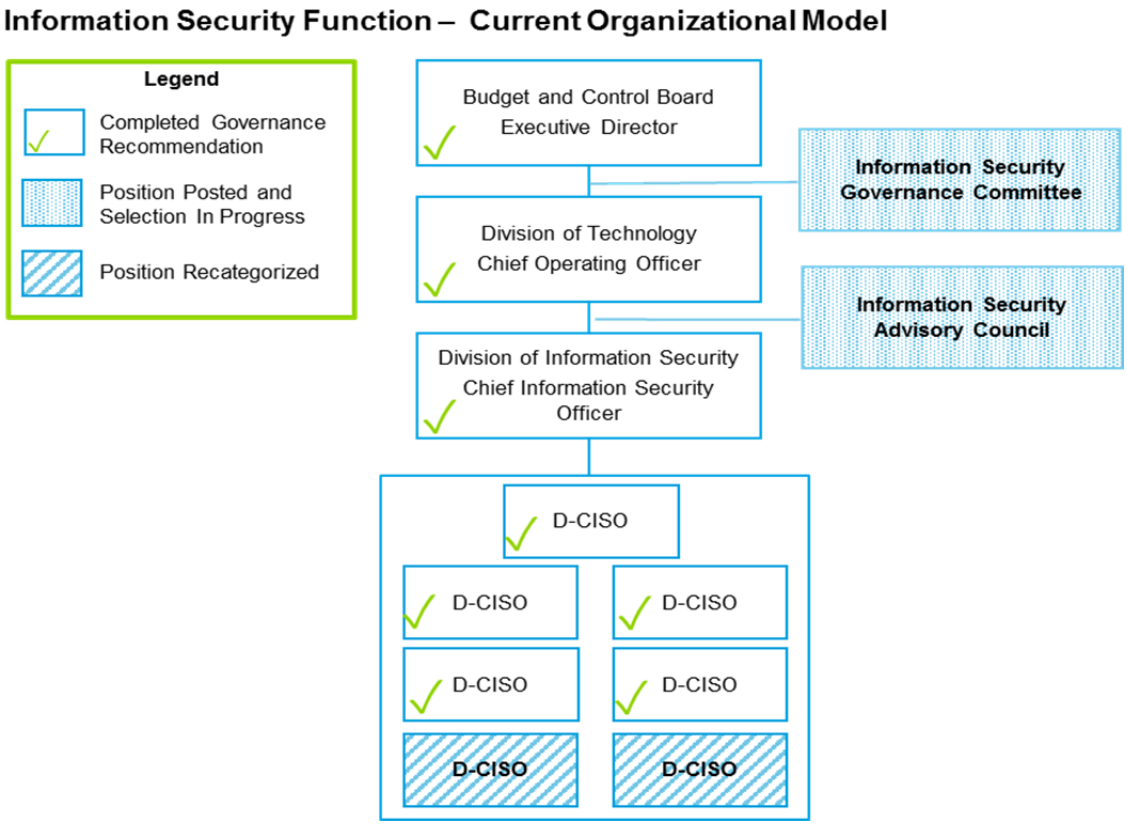


Figure 8: INFOSEC Organizational Model



Organizational Implementation

As seen in figure 7, the State has taken many strides to implement the recommendations of Task A. Moving forward, the State should consider the following:

1. **Establishing the Information Security Governance Committee**: The mission of the Information Security Governance Committee is to set the information security strategy and guide the program. Committee members include leaders from the Budget & Control Board and its Information Security, Technology, and Privacy divisions. The Budget & Control Board should also appoint one delegate from each "Community of Interest," including: education; regulatory; health and social rehabilitation services; institutes of higher education; executive and administration; conservation, natural resources; development; transportation; and judicial, corrections, and criminal justice.

2. **Establishing the Information Security Advisory Council**: The Information Security Advisory Council encourages information sharing by providing internal and external INFOSEC leaders a forum through which to discuss information security practices. The Information Security Advisory Council should draw from both State INFOSEC and Privacy leadership, as well as private sector INFOSEC and Privacy leadership.

Professional Development Guidance

The State of South Carolina has established the PDP, a development program for its core Information Security and Privacy professionals. To lay the groundwork for PDP, the State conducted a series of activities to evaluate the current INFOSEC and Privacy workforce. We helped the State develop an INFOSEC and Privacy Training Matrix to lay out the requisite skills, abilities, associated knowledge, and commensurate training expected of current professionals. The matrix was based on leading practices from the National Initiative for Standards in Technology's ("NIST") National Initiative for Cybersecurity Education ("NICE") Framework.

To help prioritize the focus areas for the PDP, we worked with the State and the various agencies to determine the size and task category of their current INFOSEC and Privacy staffs. Information gathered included staff location (i.e., at DIS or agency), current level of INFOSEC knowledge, and what knowledge they needed to effectively perform their jobs and increase the security posture of the State. Recommendations for professional development include:

- Define INFOSEC and Privacy roles and responsibilities, including competency models that outline required skills and proficiency levels;
- Map role expectations to industry standards;
- Create dedicated INFOSEC and Privacy roles, where appropriate;
- Identify learning opportunities and training programs to increase staff INFOSEC and Privacy knowledge; and
- Increase focus on recruitment, retention and succession planning.

Moving forward, it is important for the State to engage in a more holistic approach to the PDP, including establishing a competency model with clear roles and responsibilities, a specialized training plan, identification of a career path, increased focus on recruitment and retention, and development of a succession plan.

3.3 Policy & Process Recommendations

We drafted a set of policies that enable the State to govern INFOSEC operations and efforts at an enterprise level. These policies provide the foundation for a consistent program that can evolve over time, as well as a mechanism for monitoring the program.

Figure 9: Process & Policy Recommendations

Foundation	Current Status	Next Steps
Security Policy: Develop guidelines to define governance of information security throughout the enterprise and across agencies.	Developed and published 13 information security policies to be adopted by agencies statewide. **http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx** Providing State agencies with guidance and direction for the adoption of statewide INFOSEC policies.	Develop standards for how the State and its agencies will enforce INFOSEC policies. Create a mechanism to measure agency compliance with INFOSEC policies.
Adopt a Security Framework: Adopt an information security framework, derived from	The State adopted a customized INFOSEC framework that currently serves as the basis for information	Develop a process for keeping the customized INFOSEC framework up-to-date with authoritative

Foundation	Current Status	Next Steps
authoritative sources such as NIST, Payment Card Industry ("PCI"), and Health Insurance Portability and Accountability Act ("HIPAA"), among others.	security risk assessments and INFOSEC policies.	sources, including both widely accepted security standards and local laws and regulations.
Information Security Risk Assessments: Conduct periodic enterprise and agency-level risk and vulnerability assessments. Perform recurring assessments based on agency risk profiles.	Conducted information security risk assessments at 15 selected State agencies between June of 2013 and June of 2014. Deployed an information security self-assessment tool that is designed to assist agencies in identifying their information security risks.	Establish guidance to help agencies develop a Plans of Action and Milestones ("POA&M") and perform remediation of risks identified via information security risk self-assessments.
Agency Risk Profile: Establish risk profile categories for State agencies based on the agencies' data classification effort, as well as their information security self-assessments.	Created an information security self-assessment and data classification tool to help agencies auto-classify internal information security risks and sensitive data.	Establish a process to gather results from data classification efforts and information security risk assessments, and create a mechanism for agencies to designate risk profiles. Develop risk profiles to be used by DIS in evaluating agencies and help determine risk mitigation strategies.

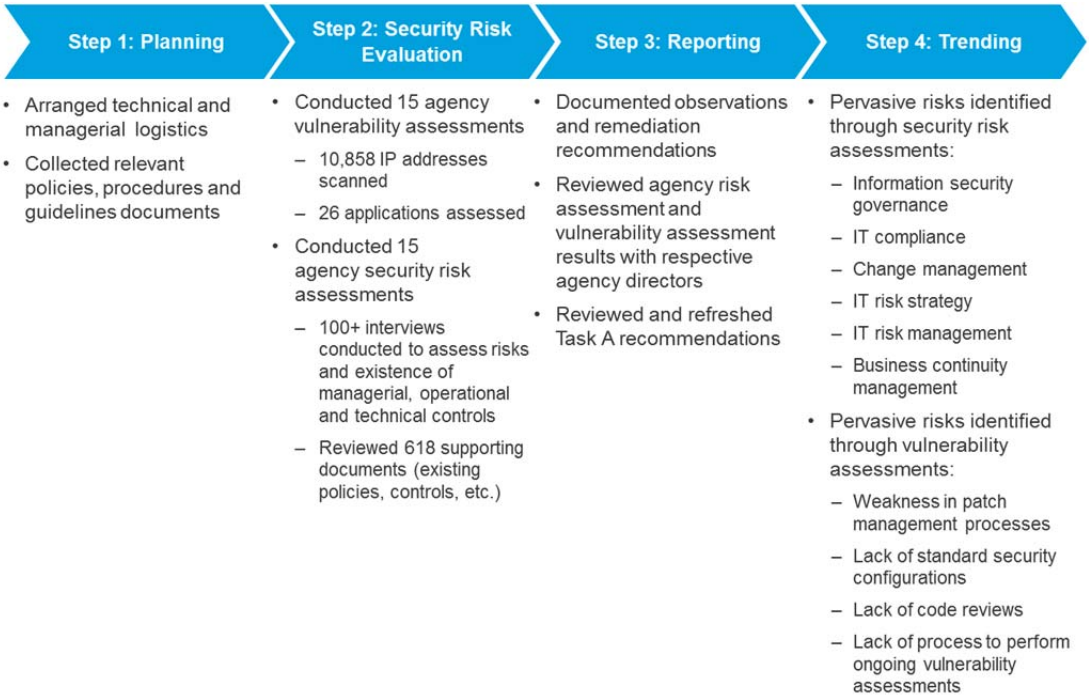
Information Security Policies

Policies provide baseline requirements for the agencies and suggest a method for meeting them. The current policies address the risk and vulnerabilities that have been identified through 18 information security risk assessments, using the established statewide information security framework, and are based on current industry requirements. We developed 13 additional policies covering areas such as asset management, access control, risk management, and IT compliance. These policies were based on Task A, as well as a review of current policies that identified gaps compared with leading practices. Please see the appendix for links to the full list of enterprise-wide policies.

Information Security Risk Assessment and Technical Vulnerability Assessments

As part of Task B, we evaluated security vulnerabilities at an additional 15 agencies, using two different assessments: information security risk assessments that evaluated security controls related to people, processes, and technology against the statewide information security control framework. Technical vulnerability assessments evaluated the technical controls of infrastructure components (e.g., firewalls and routers) and applications components (e.g., web applications).

Figure 10: Security Risk and Technical Vulnerability Assessments



INFOSEC Policy Training and Guidance

To disseminate the State's new INFOSEC policies throughout State agencies, we assisted DIS in developing and delivering training to specific personnel for a selected number of agencies. Activities included policy working sessions, policy pilot workshops, and on-site visits with agency stakeholders.

- **Policy working sessions**: Delivered to groups of selected stakeholders at more than 50 State agencies, these sessions provided a training forum for INFOSEC policies, outlined mitigation strategies, and addressed attendees' implementation concerns.

- **Policy pilots workshops**: These deep-dive workshops addressed implementation concerns, especially for the policies that were considered high-priority. We worked with agencies to conduct gap analyses and to review the agencies' implementation plans.

- **On-site visits**: We provided specific guidance to individual agencies, in partnership with their INFOSEC policy champion and INFOSEC policy deployment team. During these visits, we evaluated the current agency environment, performed gap analyses, and reviewed policy implementation materials, as well as addressed implementation challenges and mitigation strategies.

3.4 Technology Recommendations

As a part of Task A, we recommended a number of technologies and/or information security tools to help the State improve its information security posture. These recommendations, which were included as part of the Fiscal Year 2014 budget, included data protection through laptop encryption, patch management, and data discovery. The recommendations also included secure network engineering through virtual private networks and two-factor authentication for

remote connections. The roadmap also addressed ongoing threat monitoring and control, primarily through expansion of the State's SIEM solution. These recommendations comprise a suite of tools that will help the State continue to enhance its information security posture in areas with identified vulnerabilities.

Figure 11: Technology Recommendations

Foundation	Current Status	Next Steps
Data Discovery and Encryption: Perform a data discovery exercise to identify the presence of sensitive data within the State's databases and employ appropriate encryption to secure the databases. The scope includes establishing disk-level encryption of the State's laptop devices.	The State has initiated a project to implement a data discovery solution for use by interested agencies. This provides agencies the ability to scan their environment to identify the nature and location of sensitive data. Additionally, three recommended data discovery products have been placed on State contract and are available for agencies to procure and implement. The State has initiated a project to implement an enterprise laptop encryption solution and make it available to interested agencies. With this solution, agencies will be able to encrypt laptop computers housing sensitive data.	Conclude pilots. and broadly deploy the data discovery tool in FY2015. Conclude pilots. and broadly deploy the laptop encryption tool in FY2015. Budget for additional licenses as required to implement encryption for mobile devices.
Two-Factor Authentication for Remote Users: Use strong authentication techniques to provide the State's information system and organization with more confidence regarding a user's identity prior to allowing them access to the State's network. The scope of this implementation is focused on remote access to the State's network by State employees (it does not include Internet-facing applications)	The State has initiated a project to implement an enterprise VPN solution supported by two-factor authentication, providing agencies secure remote access capabilities for end users. Additionally, three recommended VPN and 2FA tools have been identified and placed on State contract and are available for agencies to procure and implement.	Conclude pilots, and broadly deploy the VPN and 2FA tool in FY2015.

Patch Management: Provide an enterprise-wide centralized solution to agencies in order to identify and patch out-of-date third-party and operating system software versions.	The State has initiated a project to implement an enterprise Patch management solution for use by interested agencies. This enables agencies to: • Identify current third-party and operating system patch levels on workstations, as well as out-of-date software versions; • Download and build patch packages for distribution via existing software deployment tools (e.g., System Center Configuration Manager /Windows Server Update Services); and • Report and track patch compliance status. Additionally, two recommended patch management products have been identified and placed on State contract and are available for agencies to procure and implement.	Conclude pilots, and broadly deploy the patch management solution in FY2015.
Expand Information Security Monitoring and Threat Management: Enhance current monitoring and reporting capabilities to include the State's Internet-facing web applications and databases containing highly sensitive data.	The State has initiated a Security Information and Event Management expansion project to increase DIS security monitoring capabilities. This will allow agencies not currently being monitored by the DIS SIEM solution to participate.	Conclude the design and build phase of the SIEM expansion, and begin deployment.
Continuous Vulnerability Assessments and Remediation: Identify the sensitivity of the State's Internet-facing web applications and prioritize for application security vulnerability testing. Perform application vulnerability testing to detect and mitigate potential security vulnerabilities and insecure coding/configuration practices.	Conducted vulnerability assessments in parallel with risk assessments. Agencies were given the results of the vulnerability assessments to better understand weaknesses in their environment. The State has initiated a project to deploy an enterprise vulnerability assessment solution, giving agencies the capability to conduct routine, repeatable vulnerability scans.	Conclude the design and build phase of the vulnerability assessments and begin deployment.
Privileged User Management: Provide an enterprise-wide centralized solution that secures, manages, and logs the State's privileged accounts based on pre-defined security policies; manages user credentials; supports regulatory requirements; and smoothly integrates enterprise systems.	The State has initiated a project to evaluate a Privileged User Management solution and develop a FY2015 deployment strategy and approach for agencies. Additionally, three recommended Privileged User Management products have been identified and placed on State contract, and are available for agencies to procure and implement.	The data Privileged User Management project is currently in the pilot phase. Conclude pilots and broadly deploy Privileged User Management in FY2015.

The State has begun to pilot, test, and deploy these technologies at selected agencies. The deployment is complex and will take some time reach the majority of the agencies. The DT and DIS will continue to deploy these technologies to the agencies into Fiscal Year 2015.

4. Information Security Program Evolve Phase

The Evolve phase consists of building on the foundation for Fiscal Year 2014 and continuing to develop the State's INFOSEC and Privacy programs. The State should strive to carry out the "Evolve" portion of the Task A roadmap by addressing remaining organization & governance, policy & process, and technology recommendations.

4.1 Organization & Governance

After establishing a foundational organization and governance model, the State of South Carolina should consider advancing the model by continuing its PDP, unifying performance reviews of INFOSEC staff, establishing INFOSEC governance committees and roundtables, and building relationships with universities to cultivate new cybersecurity talent. This type of holistic approach will help the State improve the skills of its current employees, grow a pool of future employees, and leverage the learnings of external INFOSEC professionals.

Figure 12: Evolve INFOSEC – Organization & Governance Recommendations

Evolve	Current Status	Next Steps
Establish a Professional Development Program: Implement a development program for INFOSEC and Privacy staff that will define expectations, develop required skill sets, provide commensurate training, and establish a formal career path for information security professionals. This will include the creation of standardized INFOSEC roles and responsibilities across State agencies, a competency model to define knowledge, skills, and abilities expected from the State's specialized INFOSEC professionals, and a training plan to help bridge knowledge and skills gaps.	Performed current-state INFOSEC workforce assessment and currently developing INFOSEC roles and responsibilities and standard position descriptions based on classes of data.	Continue implementing roles and responsibilities and standard position descriptions for State agencies. Create competency and performance management model, a training curriculum, and a career path for INFOSEC staff statewide. Develop recruitment and retention plan, and succession plan for INFOSEC roles.
Unified Performance Reviews of Security Liaisons, ISOs, and CISOs: Establish a common process and tool through which performance of INFOSEC personnel can be reviewed periodically.	Developed roles and responsibilities for INFOSEC personnel. Developing position descriptions to establish performance expectations facilitate annual performance reviews.	Define a competency model, and implement a single, automated process to review INFOSEC personnel performance on an annual basis.
Strengthen Governance Structure: Establish an INFOSEC Governance Committee with representation from specific communities of interest, such as Health & Social Services,	Defining information security groups that will have representation from State agencies.	Implement a governance structure that enables DIS, agencies, and State leadership to disseminate, define, and monitor INFOSEC initiatives.

Evolve	Current Status	Next Steps
Judicial/Criminal Justice, Regulatory, Conservation, Natural Resources, Development, and Transportation, Education, Executive & Administration. This committee will provide guidance and direction on the information security strategy for the State.		Establish information security roundtables to be organized by the type of data handled and size of agency. Roundtable groups should be comprised of agency personnel with information security roles, including CISOs, D-CISOs, and information security liaisons.
Establish Cybersecurity Programs with Technical Schools and Universities: Collaborate with the State's higher education institutions in the development of a curriculum based on the State's INFOSEC and Privacy competency models. Benchmark against other higher education INFOSEC degree programs to help create the next generation of INFOSEC employees.	Planning recruitment and retention strategies for INFOSEC professionals, including working with higher education institutions, as part of the Professional Development Program.	Begin identifying higher education institutions nationally that have established and implemented an INFOSEC and/or Privacy curriculum.

4.2 Process & Policy Recommendations

After developing and implementing the 13 INFOSEC policies, the next step for achieving an evolved INFOSEC program is establishing INFOSEC standards and procedures that align with the INFOSEC policies. These standards and procedures offer agencies specific guidance on executing the new policies as part of day-to-day operations. To encourage progress in implementing enterprise policies, procedures, and standards, the State should adopt a mechanism to measure agencies' implementation efforts and level of compliance. Additionally, creating detailed information security plans and incident response processes will move the INFOSEC program towards a more evolved state of maturity.

Figure 13: Evolve INFOSEC – Process & Policy Recommendations

Evolve	Current Status	Next Steps
Security Standards and Procedures: Develop information security standards, technical standards, and supplemental guidance to help guide implementation of INFOSEC policies.	Currently providing policy adoption guidance to State agencies via workshops and onsite visits. The State is also conducting INFOSEC policy adoption pilots with three selected State agencies. It plans to create a policy implementation handbook to offer additional guidance for policy implementation.	Develop INFOSEC standards to outline the requirements for procedures and technical controls that will further enable agencies to align with INFOSEC policies.
Agency Security Plans and Roadmap: Implement a methodology and process for developing information security plans that can be leveraged by agencies. This methodology should identify and mitigate security risks and enhance compliance with INFOSEC policies.	Agencies are receiving assistance with the adoption of policies, including the governance and IT risk strategy. The risk strategy includes requirements for establishing an information security plan and processes to measure INFOSEC performance.	Build upon the information security risk self-assessment tool and methodology and provide agencies further guidance--including methodologies, templates, and training--to enable them to develop and maintain information security plans and roadmaps.
Incident Response: Enhance the statewide incident response process,	Performed review of current incident response procedures and identified	Implement streamlined incident response process, including

Evolve	Current Status	Next Steps
including the establishment of incident first responders for the enterprise and agencies.	areas of opportunity and risk. Developed training plan for incident response personnel at the Security Operations Center ("SOC") managed by DIS.	enhancements of the triage process, early identification of data involved in incidents, and escalation and reporting. Consider collaborating with the Multi-State Information Sharing & Analysis Center ("MS-ISAC"). In addition, leverage the federated model to encourage interagency collaboration and cooperation between the DIS and the agencies. This cooperation could be facilitated by the creation of INFOSEC and Privacy roundtables, committees, councils, or other interactive bodies.
Establish Compliance Program: Develop an operating model to track the compliance of State agencies with INFOSEC policies, including a reporting mechanism such as a balanced scorecard (or dashboard) of KPIs that are regularly distributed to relevant stakeholders (e.g., agency leadership, State CPO, and CISO).	Developed an operating model and defined KPIs to enable DIS and State agencies to gather data to measure compliance with INFOSEC policies adoption.	Automate the process for the ongoing gathering of compliance information and generation of a balanced scorecard with results from KPIs and key risk indicators (KRIs). Provide guidance to agencies on steps required to gather and report KPI / KRI data.

4.3 Technology Recommendations

As the State becomes more advanced in its technical abilities, it should consider the additional steps required to achieve an evolved INFOSEC program. The following table offers recommendations on bringing the State's foundational INFOSEC technology to the next level.

Figure 14: Evolve INFOSEC – Technology Recommendations

Evolve	Current Status	Next Steps
Continuous Threat and Vulnerability Management: Expand the established application vulnerability assessment process.	The State has initiated a security information and event management expansion project to increase DIS' security monitoring capabilities, as well as a project to deploy an enterprise vulnerability assessment (VA) solution. This will allow agencies to conduct routine, repeatable vulnerability scans.	Enhance the State's Incident Response and SIEM capabilities. Assess SIEM to identify gaps between current capabilities and industry practices.
Expand Data Protection: Expand the established data protection process to include the State agencies, boards, and commissions that handle sensitive data.	The State has initiated a project to implement an enterprise laptop encryption solution available to interested agencies. This provides agencies the capability to encrypt laptop computers that house sensitive data. The State has initiated a project to implement a data discovery solution that will be made available to State agencies. This provides agencies the capability to scan their environment in order to identify the nature and location of sensitive data	Continue current laptop encryption and data discovery deployment into FY2015. After asset inventory and data identification activities conclude, sensitive data will need appropriate protections. The State should consider implementing a security control catalog to simplify the selection of security controls that are appropriate based on sensitivity of the data and the specific infrastructure hosting and processing that data.

Evolve	Current Status	Next Steps
Identity and Access Management: Establish an enterprise Identity and Access Management ("IAM") service that addresses the State's business processes, technology, and information supporting the access by employees, contractors, customers / citizens, and other stakeholders to State systems and data.	Currently, the State of South Carolina does not have a consolidated IAM environment. Instead, agencies handle identity and access management independently, which is not only inefficient from an administrative perspective, it also creates a burden on stakeholders who need access to systems across agencies, departments, or divisions.	The State should consider creating a statewide IAM strategy and roadmap. Effective IAM solutions bring a combination of mission enablement, operational efficiency, compliance enablement, and risk management to the organization's management of identity-related information. These systems also decrease excess access, which is a common attack vector used by cyber criminals.
Cyber Threat Analytics and Intelligence: To combat cyber-attacks, employ leading industry practices and tools to perform cyber threat analytics and gather intelligence.	The State is collaborating with MS-ISAC to better understand state sector cyber threat analytics and intelligence.	Further enhance the State's SIEM processes to gain efficiencies and to achieve a higher level of maturity by: •Making data available to cyber threat analysts so that they can understand event context; • Implement statistical analysis and advanced search capabilities; and • Standardize cyber threat processes across State agencies.

5. Implementing a Privacy Program

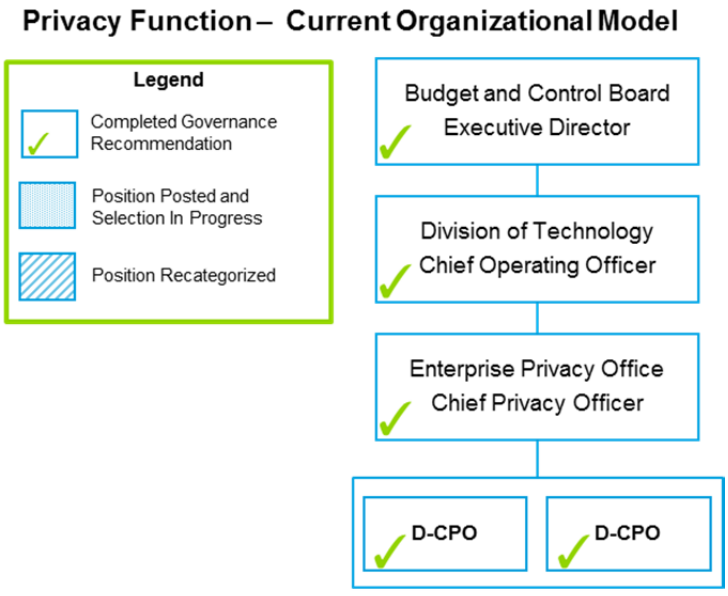
In addition to implementing an INFOSEC program, the roadmap from Task A recommended that the State develop an Enterprise Privacy Office within the Division of Technology, led by a Chief Privacy Officer reporting directly to the COO of the Department of Technology. We also recommended the establishment of Agency Privacy Officers, ("APO" or "Privacy Liaisons") at agencies that collect, store, share and process sensitive data. APOs/Privacy Liaisons report locally, but they should also coordinate privacy efforts with the CPO.

The State of South Carolina has since established the EPO, which is a division at the same level as the DIS and the Division of Technology Operations. The EPO defines what data requires protection and why, while DIS defines how to protect the data. Once fully established, it is recommended that the EPO oversee the three areas of organization & governance, policy & process, and technology.

5.1 Privacy Organization & Governance Recommendations

We worked with the State of South Carolina to establish both the EPO and the enterprise-level CPO role. We also developed role objectives for two Deputy CPOs. In addition, we recommended that agencies institute a Privacy Liaison to oversee Privacy efforts; this role may not warrant a full-time position for many of the State agencies. The following figure depicts the recommended organizational model for the EPO:

Figure 15: State Privacy Organizational Model



Privacy Professional Development Guidance

Professional development of privacy professionals is essential to helping the State understand, classify, and protect sensitive information. As the PDP evolves, a track related to Privacy will be created. However, it is recommended that the State engage in additional PDP activities specific to identifying the many different privacy roles that are needed, as well as relevant competencies, training opportunities, career pathing, and recruitment and retention programs.

5.2 Privacy Policy & Process Recommendations

The EPO sets the strategy for analyzing the data that agencies obtain, use, and store within their systems. D&T assisted the EPO with the development of the State's data classification schema. This schema helps agencies define the categorization of state data based on the degree of protection required by the State, as well as federal laws, regulations, and standards. To assist the State in defining its privacy policy and processes, D&T worked with DIS to provide the following recommendations:

Figure 16: Privacy Policy & Process Recommendations

Foundation	Current Status	Next Steps
Policies, Procedures, Guidelines: Develop and deploy data privacy policies, standards, and other artifacts to better enable agencies to protect sensitive data,	Implemented the INFOSEC policies, which contain some Privacy components.	Establish privacy-specific policies and develop standards and additional guidance to help agencies understand their sensitive data and required security controls.
Agency Privacy Liaison and Coordination: Establish Privacy Officers or Privacy Liaisons at State agencies to oversee data privacy and coordinate with the CPO on statewide privacy initiatives.	The State is in the process of defining the roles and responsibilities for State agencies, including Privacy Liaisons, through the PDP initiative.	Complete staffing of the EPO. Establish a process to help determine if State agencies have designated Privacy Liaisons. Establish mechanisms for agency Privacy Liaisons to work closely with the CPO.
Public Awareness and Education: This function communicates the importance of Privacy to State agencies and citizens. Examples of activities could include: champion an annual South Carolina Privacy Day; develop a website dedicated to privacy; create educational materials; and offer educational seminars.	The State has provided optional training on the Data Classification Schema, as well as data classification materials for agencies and higher education.	Establish a privacy awareness program that includes agencies and public outreach, in coordination with agencies.
Data Classification: The enterprise-level data classification policy forms the foundation for discovering and understanding the data that agencies hold and defines the degree of protection required.	Developed a Data Classification Schema, data inventory tool, training, and procedures for the agencies to follow.	Establish a process for providing guidance on the Data Classification Schema and procedures to agencies.
PDP: Provides a baseline understanding and lexicon of the privacy professional, relevant skill sets, and areas of focus.	The State has begun developing an INFOSEC and privacy PDP for agencies that highlights the importance of privacy in the context of INFOSEC.	Establish an independent Privacy PDP to further identify and develop privacy roles and responsibilities, competencies, training opportunities, career path, recruitment and retention strategies, and succession planning.

Data Classification Schema and Training

In order to effectively protect its data, the State needs to inventory the data, analyze the content, classify it into levels of confidentiality, and then implement appropriate security controls. The Data Classification Schema defines the data classification model for the State. It also includes detailed guidance on the application of the different classification models, which enables a user to better understand the categorization process. The State's Data Classification Schema is below:

Figure 17: Data Classification Schema

State of South Carolina's Data Classification Schema	
Public	Non-sensitive data that is intended or required to be shared with the public
Internal Use	Non-sensitive information that is created by an agency or used in the daily operations of an agency
Confidential	Sensitive information in use or stored by an agency
Restricted	Highly sensitive information that contains statutory penalties and is protected by law and is in use or stored by an agency

The EPO will be responsible for maintaining and updating the Data Classifications Schema, including expanding classification layers and providing specific guidance for safeguards required for any type of sensitive data.

5.3 Privacy Technology Recommendations

Moving forward into the Evolve phase, the EPO should be fully equipped to detect, report, and investigate incidents of suspected fraud. To do this, the EPO should support DIS and DTO on the implementation of the following technologies:

Figure 18: Evolve Privacy Technology

Evolve	Current Status
SIEM /SOC Configuration: Incidents related to privacy will probably be processed by the State's existing SIEM/SOC tool. Consider enhancing the SIEM/SOC tool's configurations to further enable the State to detect intrusions	The State is expanding its SIEM solution capabilities to allow remaining agencies to migrate to its SIEM environment
Data Protection: to preserve privacy, the State of South Carolina should consider data protection technologies, such as: - Data Encryption - Data Masking - Data Tokenization - Data Redaction	The State is deploying a data encryption solution and is reviewing options for data masking and data redaction solutions to further protect its sensitive data.
Data Loss Prevention: This tool will enable the State to detect and potentially prevent data leakage or loss by examining sensitive data when it is in-motion, at rest, or in use.	The State has established its Data Classification Schema to determine which data is considered "sensitive."

6. INFOSEC Budget

6.1 Introduction

This section provides a high-level update on the budget recommended by Deloitte & Touche for the State's Fiscal Year 2015 (FY 15) as compared to appropriated State monies. In addition, this section provides high-level budget recommendations for State Fiscal Year 2016 (FY 16) for the implementation of the proposed strategies and recommendations resulting from the reoccurring trends identified as part of Task A and B.

Deloitte & Touche reviewed the budgetary estimates and underlying assumptions with representatives from the Budget & Control Board and the DIS.

The budget estimates related to salaries are based on industry benchmark reports, as well as South Carolina's experience in filling current INFOSEC positions. Operating budget estimates considered the costs of hiring, onboarding, and recurring expenses like software licenses and office space.

Estimated budgets for technology and recommended technology solutions were based on enterprise-level, rather than agency-level, asset requirements, and reflect the priorities set forth by DIS. We recommend the State coordinate with the Budget & Control Board on security-related investments.

6.2 State Fiscal Year 2016 Recommendations

State Fiscal Year	D&T recommended budget	State appropriated budget	Difference
FY 14	$14,930,000	$10,587,995	$4,342,005
FY 15	$20,887,996	$16,189,847	$4,698,149

As shown above, we recommend that the FY 15 budget be increased by $5,957,996 from FY 14 recommended budget. Based on the current and upcoming initiatives for FY 16, we advise the State to allocate resources that are comparable to those recommended in the budget for FY 15. This will support the continued enhancement of processes, development of INFOSEC and Privacy professionals, and implementation of enterprise technologies at a statewide level. This comes to a total of approximately $21M for INFOSEC and Privacy efforts.

7. Information Security and Privacy Outlook

7.1 Moving Forward

Organization & Governance

7.1.1 IT Assesment Strategy for the State

The State of South Carolina should consider establishing an IT assessment function to operate at a statewide level. The IT assessment function would contribute to compliance monitoring and support the evolution of the overall INFOSEC and Privacy programs. This assessment function should be independent of the State Division of Technology and other State agencies. The IT assessment function should be responsible for providing an objective assessment as to whether the State's IT risk management, governance, and internal control processes, as required by the INFOSEC policies as well as by State and federal laws and regulations, are operating effectively. It will be responsible for assessing processes and controls in the following areas:

- The State's INFOSEC program;
- Information asset protection;
- Governance and management of IT;
- Information systems acquisition, development, and implementation; and
- Information systems operations, maintenance and support.

There will be challenges for the implementation of an IT assessment function in the State of South Carolina, including competition for State resources, political pressures, and lack of human resources to prepare, plan, and implement the new IT assessment function. The State should therefor consider the following:

- Clearly communicate the purpose of the IT assessment function to State leadership, agencies, institutions, and citizens;
- Identify assessment standards;
- Define, document, and disseminate IT assessment policies, processes, and procedures;
- Design the IT assessment function to report directly to a State leadership position and not to the Division of Technology;
- Grant the IT assessment function the authority to independently allocate resources, establish schedules, define scope of work, and set assessment objectives; and

- Consider short-term rotation of qualified agency and enterprise information security personnel to assess roles for specific duration.

7.1.2 INFOSEC Consolidated Services

Moving forward, the State of South Carolina should consider establishing a Shared Services Center to deliver selected INFOSEC services to its agencies. For example, if an agency lacks personnel who can perform application vulnerability scans, it can look to the Shared Services Center for guidance and potential performance of the task. An INFOSEC Shared Services Center will also assist the enterprise in the enhancement of information security policies, development of standards and leading practices, and provide guidance on security technologies, among other INFOSEC resources. The Shared Services Center should also provide leadership on risk intelligence.

For an effective implementation of an INFOSEC Shared Services Center, the State will need to develop the following plan:

- A vision, mission, goals and objectives, and a process for clearly communicating them to State leadership, agencies, institutions, and citizens;
- A process for transferring knowledge and gathering feedback from State agencies and institutions;
- A portfolio of information security services to be made available to State agencies; and
- An organization model that allows interaction and collaboration from State agencies and institutions.

7.1.3 Agency Risk Profiles and Agency Spend in INFOSEC

Initiatives such as risk assessments, vulnerability assessments, and data classification serve as the foundation for agency risk profiles. For example, agency risk profiles leverage the classification from the data inventory. Agency risk assessments conducted by D&T, as well as self-assessments, identify security gaps and vulnerabilities that put data at greater risk of becoming compromised. Risk profiles will assist agencies as they prioritize data and implement security controls for at-risk data and systems. They will also help leadership better understand the State's information risk landscape.

In addition, a detailed analysis of security resources and security budgets for State agencies will help State leadership, DT, and executive directors at agencies set appropriate budget targets for INFOSEC and Privacy initiatives, services, and resources.

7.1.4 Further Understand Risks

One important challenge for the State is to identify cybersecurity and privacy risks, not only at the agencies, but also at institutions and counties that handle, process, and store sensitive data. Implementing a State INFOSEC program has enabled the agencies to achieve a higher level of proficiency and maturity in the handling of these risks. To continue to improve its information security posture, the State should work towards identifying and understanding data security and privacy risks that derive from:

- Users from counties with access to State systems;

- Local government users (e.g., law enforcement) accessing data from State systems;
- School districts and institutions with access to State systems; and
- Contractors and outsourced infrastructure components and systems.

In order to better understand these external risks, the State should consider:

- Assessing security gaps and vulnerabilities associated with the use of sensitive data and access to State systems by local government users, such as law enforcement, school districts, and county employees;
- Providing guidance on developing remedies to address security gaps and vulnerabilities;
- Conducting an assessment to identify processes, systems, and interfaces through which sensitive information is shared among State institutions;
- Identifying security mechanisms and controls in place to protect sensitive data that is transferred, processed, and stored by State institutions and entities other than agencies; and
- Providing guidance on the adoption of statewide INFOSEC policies and other initiatives, such as data classification and information security self-assessment.

Process & Policy

7.1.5 Ongoing Compliance Program

As a part of Task B, we worked with the State to develop an operating model and key performance indicators that will allow DT to gather data related to policy adoption. To achieve a higher level of efficiency and maturity, the State should establish a mechanism or tool to help automate the process of gathering data pertinent to compliance, policy adoption, and maturity of INFOSEC and Privacy controls at State agencies. The State can also leverage this automated compliance monitoring process to facilitate ongoing compliance assessments and reporting to agencies and State leadership.

The State will benefit from performing the following activities as part of the implementation of an automated and ongoing compliance program:

- Clearly communicating compliance expectations to State leadership, agencies, institutions, and citizens;
- Establishing a central entity and a process to help ensure that materials related to regulatory, and INFOSEC, and Privacy requirements are properly disseminated;
- Developing compliance procedures that are clear and accessible to State agencies and institutions;
- Establishing a process for reporting to State leadership and agency executives, and for maintaining records that are in compliance with State requirements. This would include implementation of a formal records management program that would govern the creation, receipt, maintenance, use and disposition of records, including

the processes for capturing and maintaining evidence of, and information about, State business activities and transactions;

- Establishing a process to conduct follow- up examinations and review compliance findings.

Technology

7.1.6 Security Operations Strategy for the State of South Carolina

The State of South Carolina should consider creating an Incident Response ("IR") and SIEM strategy for the State. This strategy should enhance its IR capabilities and provide direction for more mature SIEM / SOC processes. Additionally, this Strategy should promote the continuing close relationship between the State INFOSEC program and the EPO. An IR and SIEM / SOC strategy should include the following components:

- Identifying current capabilities and weaknesses in IR and SIEM processes
- Defining the desired state and requirements for:
    - People: Staffing models, roles and responsibilities, and working groups;
    - Processes: Backoffice, technical support, and customer facing processes;
    - Technologies: SIEM, source data, and threat intelligence solutions; and
    - Governance: Definition of service portfolio, organizational model, and reporting structure
- Developing a plan to facilitate communication with State leadership and agencies on IR and SIEM/SOC strategy issues
- Developing or enhancing current IR and SIEM / SOC policies, standards, and procedures
- Including monitoring alerts from business application logs and business metrics (e.g., fraud monitoring). This will help to further mature incident response capabilities from perimeter defense to business application monitoring

7.1.7 Statewide Identity and Access Management (IAM) Strategy

The State of South Carolina should develop a statewide IAM strategy and roadmap. An adequately implemented IAM solution helps to address an organization's identity management needs and facilitates the implementation of risk mitigation techniques in relation to authentication, authorization, tracking, and review of employees, contractors, and other stakeholders who access data and systems.

The following list of activities will help build a robust IAM strategy and roadmap:

- Define an overall IAM vision and target state with the support of State leadership and stakeholders;

- Define business, regulatory, and technology drivers;
- Map INFOSEC policies, standards, and procedures to the IAM system;
- Define IAM services to be provided;
- Define IAM program monitoring and reporting processes; and
- Upon finalizing a strategy, conduct product selection for an enterprise IAM solution

7.1.8 Centrally Managed Agency Networks

At present, many State agencies operate their IT infrastructures in decentralized, independent environments, introducing a number of challenges and risks. Among these are: higher costs resulting from multiple data centers; added complexity from maintaining diverse operations; and expansion of the threat landscape due to multiple facilities and interaction with a wide array of vendors. We recommend that the State consider centralizing its IT infrastructure to obtain some of the following advantages:

- **Enhanced security**: Technical security controls such as INFOSEC enterprise technologies (e.g., VPN, data encryption) and non-technical controls, such as policies and procedures (e.g., user access management), are implemented centrally, allowing for easier monitoring.
- **Cost effectiveness**: Despite the upfront costs for establishing a high-capacity and secure infrastructure, centralization reduces the investment required of the agencies. Also, enterprise technologies, such as VPN/2FA, and vulnerability assessment tools, can be deployed more effectively and at a lower cost. Eliminating the need to set up and sustain numerous data centers, operations, and security teams further reduces costs.

Adopting and implementing enterprise-wide IT service management practices, such as Information Technology Infrastructure Library (“ITIL” – a series of practices for IT service management) , would help remediate many of the root causes identified as part of the risk and vulnerability assessments.

7.1.9 Implement Governance, Risk, and Compliance Tools

The State and its agencies must comply with numerous requirements for the safeguarding of PII, Protected Health Information (PHI), and certain other sensitive data. Selecting individual solutions to monitor compliance with each law, regulation, or industry security practice, will result in higher costs, both at the enterprise and at the local agency level. Instead, we recommend that the State implement a GRC solution. Implementing a GRC tool using an integrated strategy will improve the quality of data shared between INFOSEC professionals, drive consistency, help reduce risks, and accelerate the delivery of guidance and gathering of compliance data. State leadership should also invest in process improvement and automation through an integrated risk and compliance management system.

7.1.10 Continue to Mature the statewide System Development Lifecycle

Many of the findings from the information security risk assessments indicated a lack of governance processes within the Systems Development Lifecycle (SDLC). Without good foundational IT processes, including SDLC, software solutions can put into production that no only lack adequate administrative controls (e.g., tracking development requests, testing, approvals), but also may introduce of technical vulnerabilities into IT environments. This is especially a concern for applications made available over the Internet. We recommend that the state continue to mature its SDLC and to focusing on enhancing the security review and application risk assessment processes.

7.1.11 Critical Infrastructure Protection

The State and its agencies should continue to assess risks and work to strengthen and maintain secure, functioning, and resilient critical infrastructure-- including assets, networks, and systems-- against both physical and cyber threats. These efforts should address security and resilience in an integrated manner to reflect the interconnectedness and interdependency of critical infrastructure and potential threats.

DT should work with relevant agencies, such as the South Carolina Law Enforcement Division (SLED), South Carolina Department of Transportation, South Carolina Emergency Management Division, and others to help ensure it is adequately addressing INFOSEC risks, reducing vulnerabilities, decreasing consequences, identifying and disrupting threats, and hastening response and recovery efforts. This work would also include participation with SLED in the South Carolina Intelligence and Information Center, the State's version of a "Fusion Center", as well as other collaborative information coordination and response efforts.

Areas of focus should align with guidance provided by the United States Department of Homeland Security and other federal agencies and departments in such critical sectors as communications, government facilities, IT, healthcare and public health, financial services, emergency services, energy, and transportation systems.

7.1.12 Consolidated Services and Infrastructure Optimization

The number of IT computing centers is directly related to the number of INFOSEC controls required to mitigate risk of the loss of confidentiality, integrity, and availability of the State's IT systems and data. Reducing the number of computing centers will in turn reduce the total number of devices and systems that need protection and monitoring. Having fewer locations would also lower the cost of statewide business continuity and disaster recovery initiatives. Finally, it would enable faster rollout of INFOSEC technology solutions and improve the State's ability to respond to security incidents.

8. Conclusion

8.1 Summary

The State of South Carolina has taken initial steps to keep South Carolinians' data secure, including building a federated INFOSEC and Privacy governance model that enables agencies to conduct their operations while enforcing statewide INFOSEC and Privacy policies and regulatory requirements. The federated model is not without trade-offs. It requires significant coordination among the 73 agencies across the State and the DIS, DTO, and EPO. By continuing to look for opportunities to drive alignment from an INFOSEC technology platform perspective, the State will be able to deploy INFOSEC technologies more quickly and cost-effectively.

The NIST-based framework adopted by the State provides a consistent approach for the foundational policies, agency information security risk self-assessments, and the Data Classification Schema.

DIS has developed and disseminated INFOSEC policies to help agencies reduce risk and clarify INFOSEC and Privacy responsibilities. In addition to releasing policies, DIS has also provided guidance and training to assist agencies on policy adoption.

The State has also made significant progress on the implementation of a foundational model for assessing compliance and policy adoption, and it has established metrics and key performance indicators that will help the enterprise gauge progress made by the State.

The State has performed vulnerability assessments and information security risk assessments for 18 agencies where Deloitte & Touche analysis indicated that threat management techniques did not meet industry standards. D&T then offered the agencies guidance on mitigating the risks identified. Enterprise technology implementation projects, such as laptop encryption and improved patch management, will help the enterprise better manage risks. Finally, implementing the PDP and adopting total rewards and improved assessment measures will improve the State's ability to retain INFOSEC and Privacy talent.

As the State continues to take measures to improve its information security posture, it should realize a wide range of benefits, from reduced remediation costs to the enhanced trust of its constituents.