State of South Carolina Initial Security Assessment

Deloitte & Touche LLP

Date: May 1, 2013

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.

This assessment is intended solely for the information and internal use of the South Carolina Budget & Control Board, and is not intended to be and should not be used by any other person or entity.

Table of Contents

1 Executive summary

The State of South Carolina ("State") selected Deloitte & Touche LLP ("Deloitte & Touche") to perform an assessment of the State's security vulnerabilities and to assist with the development and implementation of an information security (INFOSEC) program for the State. The recommendations stemming from Deloitte & Touche's assessment of the State's security vulnerabilities are summarized below.

Provide the necessary support to establish and mature the State's INFOSEC program over the long-term. The implementation of a statewide INFOSEC program is an evolutionary process which requires a long-term commitment of funding, and both legislative and executive leadership support. Deloitte & Touche recommends that the State leadership and legislature affirm their commitment to the State's INFOSEC program by providing the organizational, governance and financial support required to implement the foundational aspects of the program in fiscal year 2014 and to further evolve and mature the program in subsequent years.

Establish an enterprise information security organization with the authority to set, independently assess and enforce policy and to implement the INFOSEC program. Privacy, information security, and technology & security operations comprise the three interrelated core components of an information security program. To establish collaboration between these three components of the State's INFOSEC program, Deloitte & Touche proposes that the State establish a single enterprise information security organization and create a Chief Operating Officer (COO) role or an equivalent executive position to oversee it. Further, Deloitte & Touche recommends a federated governance model for the State's INFOSEC program. A federated governance model provides an opportunity for the State to develop and implement statewide enterprise security policies, while holding agencies responsible for implementing them. Recognizing that it will likely take several months to hire personnel and to establish the organization, we recommend creating an interim governing authority with responsibility for reviewing, approving, and coordinating enterprise and agency information security procurements and projects.

Implement an enterprise security awareness program for state employees and strengthen the State's cybersecurity workforce. Deloitte & Touche recommends strengthening the State's current and future cybersecurity workforce through an enterprise security awareness program for State employees, professional development for State information security personnel, and an internship program developed in partnership with local universities to help develop a pipeline of talent.

Implement the immediate security technology recommendations as a foundation for enterprise and agency level security improvements. Based upon the security assessment activities performed, we have provided the State recommendations that implementable in the near term to improve the security posture of the enterprise.

Evaluate governance options and recommend a model to improve the State's technology governance. The State's current decentralized Information Technology (IT) governance model is likely to continue constrain the effectiveness of the INFOSEC program. To overcome the challenges associated with multiple points of security risk evaluation, control and enforcement, we recommend that the State consider moving to a federated governance model for IT.

2 Background

In December of 2012, the State of South Carolina's Budget and Control Board authorized the Executive Director of the Board to issue a Request for Proposals (RFP) to assist the State of South Carolina ("State") with a statewide information security (INFOSEC) program and assistance in identifying and addressing serious information security vulnerabilities. The RFP was issued by the Budget and Control Board in January of this year.

Through a competitive procurement, Deloitte & Touche LLP ("Deloitte & Touche") was awarded a three year contract, containing two task orders:

- Task A: Assess security vulnerabilities and provide an initial report by May 1, 2013.
    - Assess security vulnerabilities
    - Recommend appropriate structure and governance to manage INFOSEC program for the State
    - Provide guidance and estimates for fiscal year 2014 budget
    - Deliver an initial report by May 1st, 2013
- Task B: Assist with the development and implementation of an INFOSEC program for the State.

A summary of the observations and recommendations from Task A are outlined in this document.

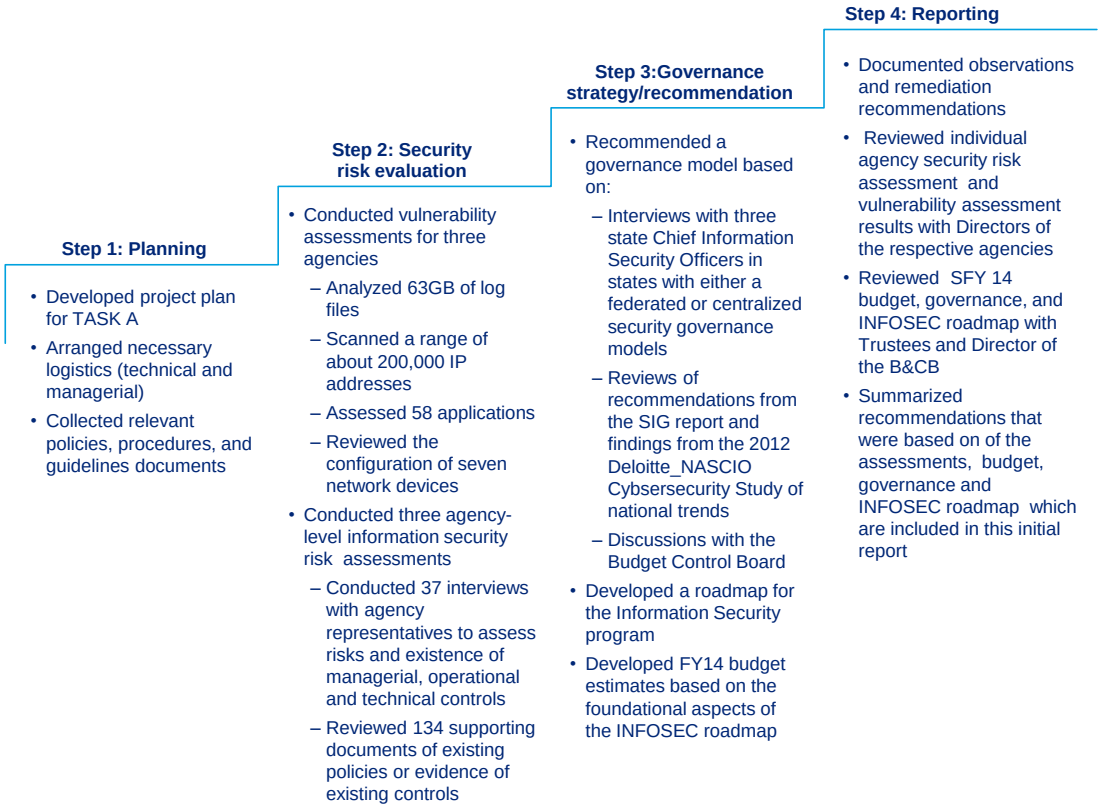
3 Approach

As approved by the State, Deloitte & Touche used a four step approach to perform the activities included under Task A (outlined in Figure 1). For the agency security risk assessments, we used a broad security risk assessment framework ("framework") that was reviewed and finalized with the State. The framework is based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev 3, as well as a number of other standards, such as those set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and in Internal Revenue Service (IRS) publication 1075. Using the framework, we conducted security risk assessments for a representative sample of three state agencies. Additionally, we conducted technical vulnerability assessments for those same agencies. The technical vulnerability assessments included external network vulnerability evaluation, internal network vulnerability evaluation and web application evaluation.

In addition to the assessment activities, we assisted the State with the development of a governance model for the INFOSEC program being implemented within South Carolina. Based on the governance model assessment we conducted, as well as the results of individual agency assessment activities, we drafted a proposed enterprise INFOSEC budget for state fiscal year 2014 and a corresponding strategy and roadmap for implementing the State's INFOSEC program.

This initial assessment report summarizes the recommendations that we are providing to the State for the establishment of an INFOSEC program and for improving the security posture of the State.

Figure 1: Approach and activities performed under Task A[1]



[1] Note: Task B is outside the scope of this report and therefore is not included in this document.

4 Recommendations

4.1 Summary

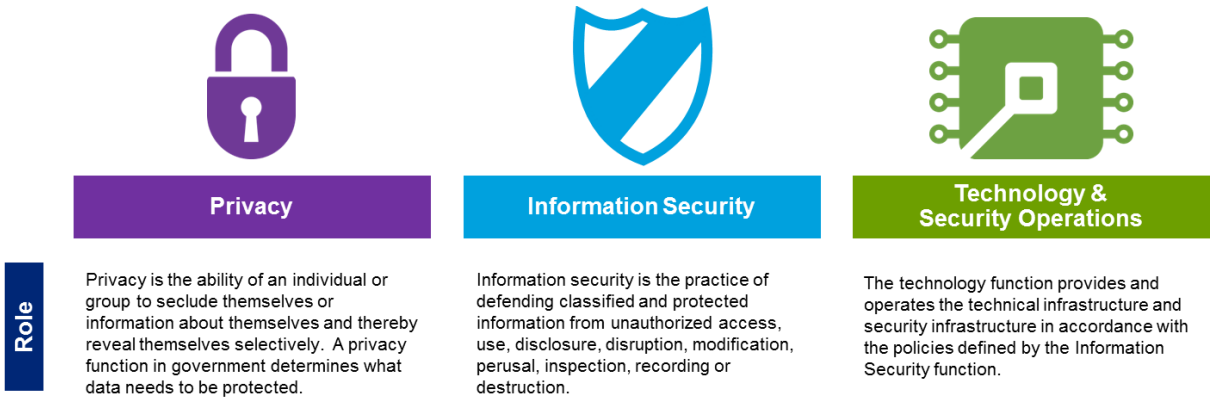
Deloitte & Touche developed information security recommendations for the State for three areas:

- Governance – an enterprise organizational structure responsible for developing statewide enterprise security policies, with state agencies responsible for implementing them
- Roadmap – a set of prioritized recommendations to help improve the security posture of the state
- Budget – budgetary estimates for implementing the foundational aspects of the INFOSEC program in state fiscal year 2014

4.2 Governance

Privacy, information security, and technology & security operations are the three interrelated core elements of an information security program (see Figure 2). The privacy function defines "what" personally identifiable information (PII) should be protected, as well as the degree to which a particular type of PII should be protected based upon its sensitivity. Once the privacy function classifies the types of data that need to be protected, the information security function defines "how" that data will be protected. Protections include policies, standards and procedures, as well as preventive, detective and corrective security controls. After data protection policies and their associated controls are defined, the technology & security operations function protects information assets through the provision and operation of technical and security infrastructure. Given the need for close collaboration among these three functions, a single functional unit for the three functions is recommended. Figure 2 below provides functional descriptions for privacy, information security and technology & security operations as defined in the Merriam Webster dictionary.[2]

Figure 2: Core security functions



Through the evaluation of other state security functions, discussions with State personnel on prevailing practices in the current environment, and drawing from Deloitte & Touche's experience implementing information security programs across public and private sector organizations, Deloitte & Touche

[2] Merriam Webster online dictionary, <http://www.merriam-webster.com/dictionary>.

assisted the State with the development of an organizational model reflecting the three tenets of privacy, information security and technology & security operations. The functional activities of the recommended three component security program are further elaborated and grouped within core functional areas depicted in Figure 3.

Figure 3: Information Security functional areas

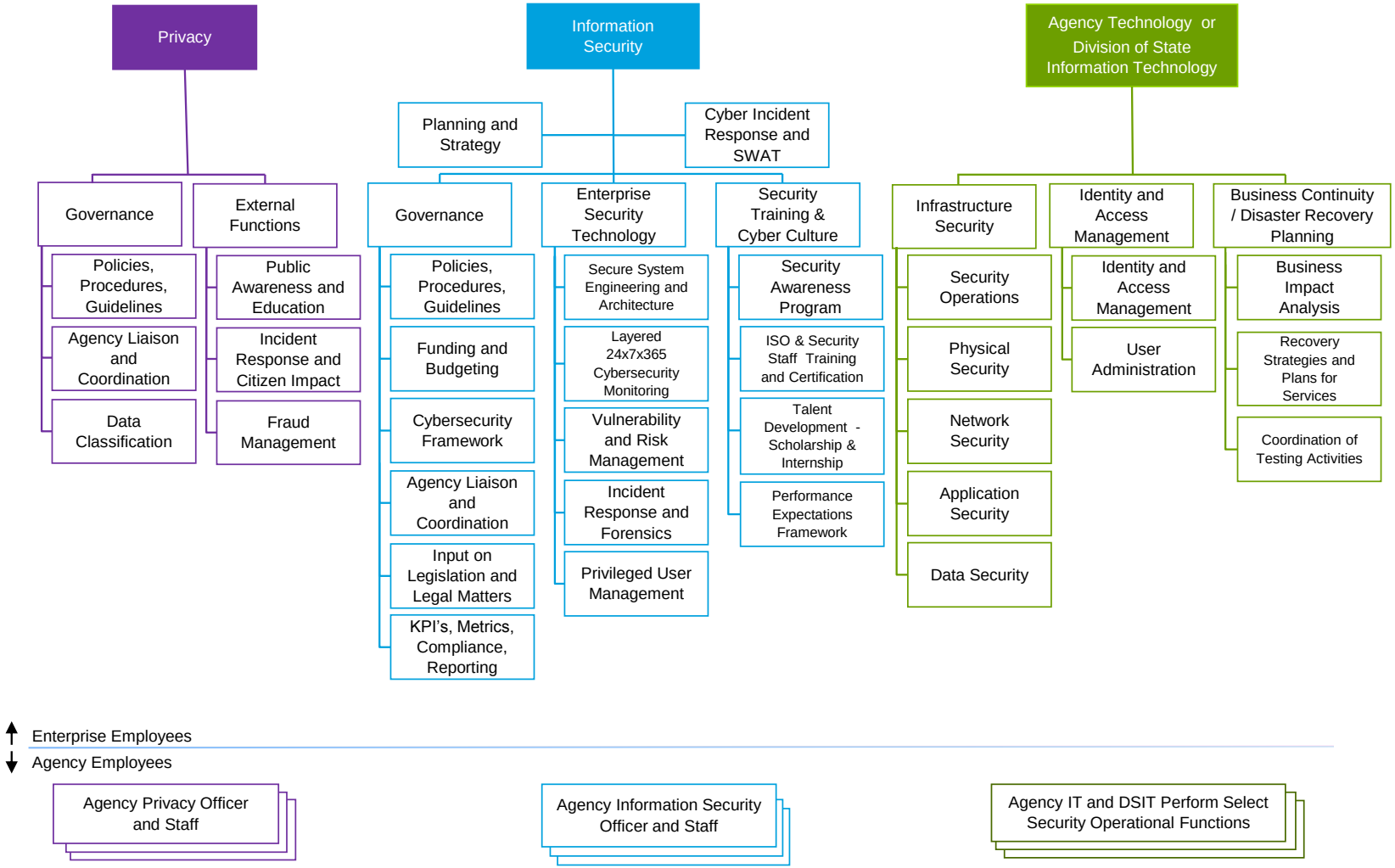
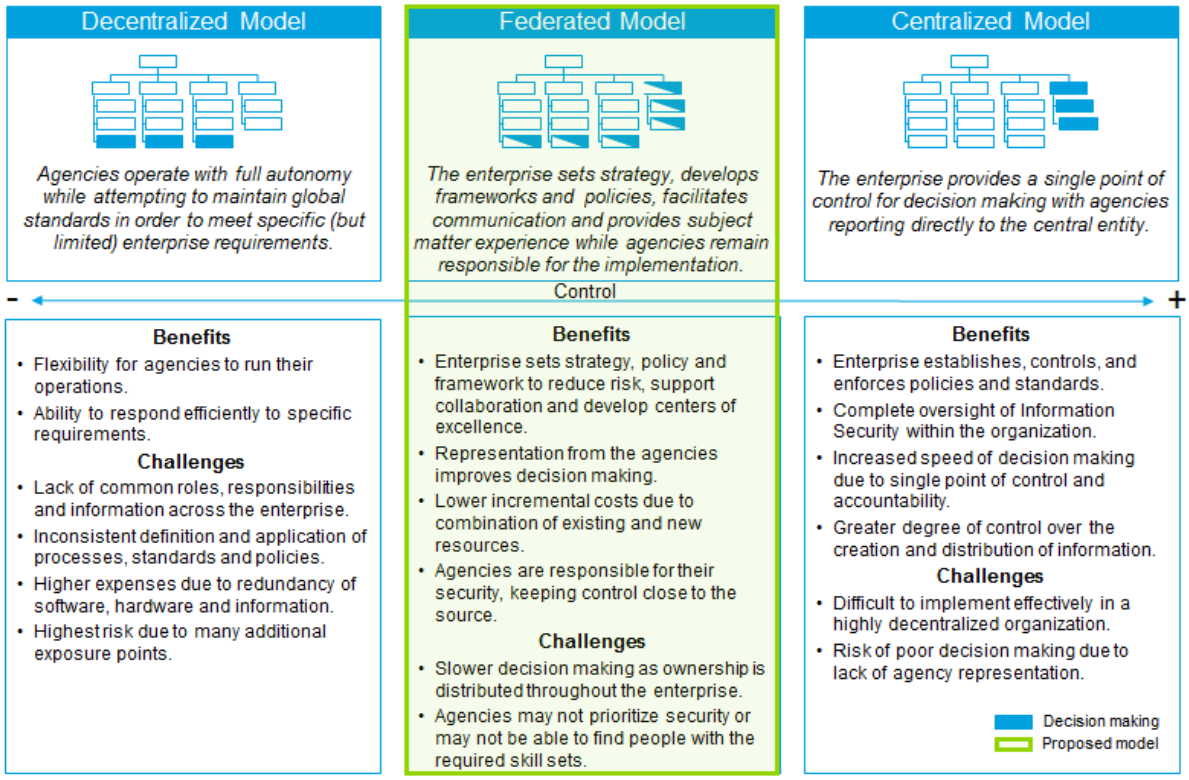


Figure 4 depicts the governance model options that were considered for the State's information security program. In order to assess which of the three possible governance models would be well suited for the State's INFOSEC program, workshops with State Budget Control Board personnel were conducted, findings from the State Inspector General's report and the 2010 and 2012 Deloitte-NASCIO Cybersecurity Study were reviewed and the decentralized nature of the State's current Information Technology (IT) governance model and assets was taken into account. Based on these observations and considerations, a federated governance model was recommended for the implementation of the State's INFOSEC program.[3,4]

Figure 4: Governance models



A federated model for the State's INFOSEC program provides an opportunity for the State to develop and implement statewide enterprise security policies, while holding agencies responsible for implementing them. As was evident in our interviews with other state CISOs, as well as in state CISO survey data (published in the Deloitte-NASCIO Cybersecurity studies), a federated governance model is not without its disadvantages (depicted in Figure 4). To overcome the challenges associated with a federated governance model, the following measures are recommended:

- **Enterprise authority:** We recommend that enterprise authority be granted to periodically perform independent, risk-based assessments of every agency's security posture and their compliance with both State INFOSEC policies and with state and federal regulations. Further, we recommend that authority be granted to enforce corrective action plans in instances in which an agency's security posture is below the desired level. Corrective action plans would be carried out in a collaborative manner with agency directors.

[3] Deloitte-NASCIO, "2010 Deloitte-NASCIO Cybersecurity Study", September 27, 2010, <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_state_2010DeloitteNASCIOCybersecurityStudy_092710.pdf>.

[4] Deloitte-NASCIO, "2012 Deloitte-NASCIO Cybersecurity Study", October 19, 2012, <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_nascio%20Cybersecurity%20Study_10192012.pdf>.

- **Agency participation and collaboration:** We recommend active agency participation in the INFOSEC program at multiple levels:
    - Agency executive director level participation in establishing and executing the INFOSEC strategy
    - Agency Information Security Officer (ISO) level participation in enterprise information security policy and standard setting sub-committees
    - Agency security workforce level participation in training, certification and career development for information security professionals

Building on a federated governance model and the need to establish collaboration between the three core functions of the INFOSEC program, Deloitte & Touche further proposes that the State designate a single executive with both business and information technology experience to lead the core functions of the program. Additionally, the State should consider placing the INFOSEC organization within an organization that is visible and has access to State level executive leadership. Deloitte & Touche recommends establishing a Chief Operating Officer (COO) role or an equivalent executive position to oversee all three components of the proposed INFOSEC program. This position would report to the Executive Director of the Budget & Control Board. The COO (or equivalent) and the Executive Director would be accountable for the effectiveness of the program and would be responsible for resolving potential differences in opinion between the core security function leaders and agency leaders.

Deloitte & Touche recognizes that many state agencies may already have personnel performing various aspects of the core privacy, security and technology functions at the agency level. Moreover, the Division of State Information Technology (DSIT) currently supports certain enterprise level security operations elements of the proposed INFOSEC program. Consequently, Deloitte & Touche recommends establishing an organization and personnel to support the enterprise level privacy and security functions described in Figure 3. Deloitte & Touche further recommends that the State DSIT and agency leaders, in collaboration with leaders from the enterprise security and privacy offices, assess their current capabilities and staffing needs against the proposed INFOSEC model.

Further details of each of the core INFOSEC program functions and the recommended reporting relationships are included in the sections that follow.

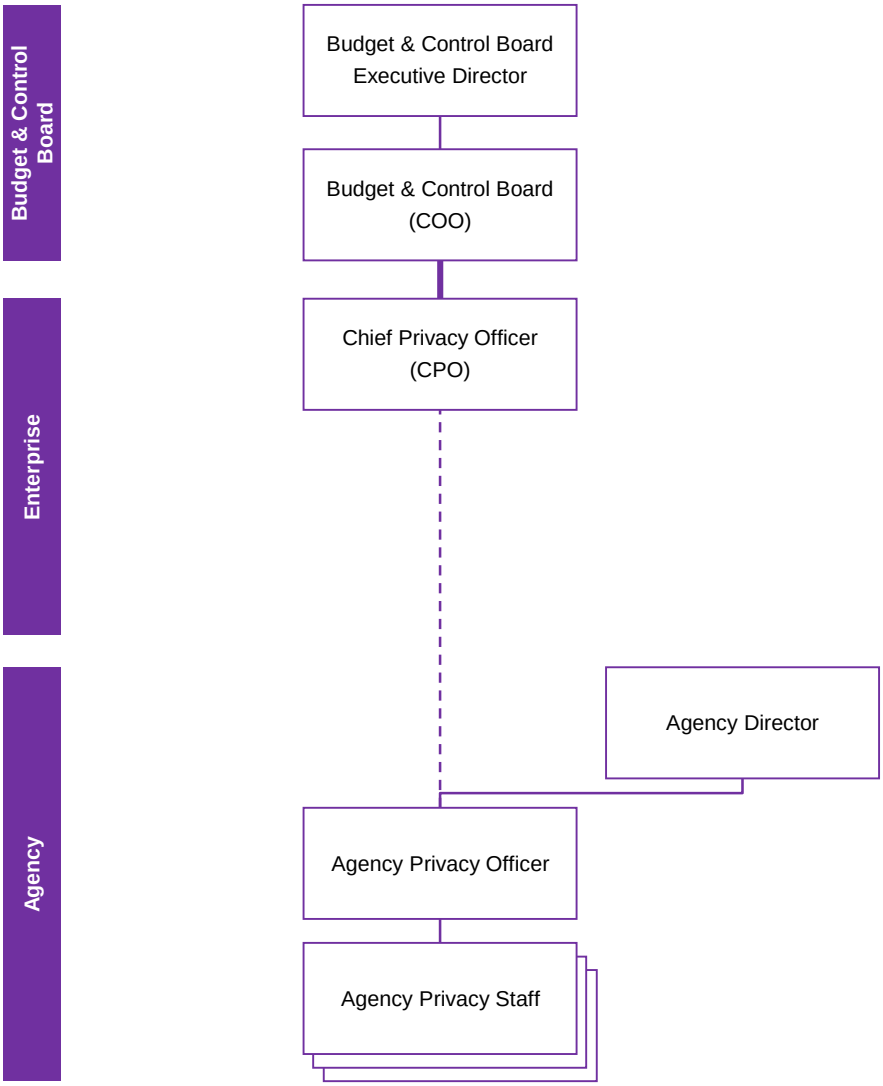
Privacy function

Figure 5 depicts the proposed governance structure of the privacy organization. The salient aspects of the proposed governance structure are outlined below:

- Establish a **Chief Privacy Officer role** at the enterprise level. This role would report administratively to the Chief Operating Officer (COO) of the Budget & Control Board. This person would establish enterprise privacy policies related to PII.
- Establish an enterprise privacy unit supporting privacy function activities outlined in Figure 3.
- Agencies that collect, store, share and process sensitive information should designate an agency level **Privacy Officer**. (Note: This does not necessarily need to be a full-time position).

The **Agency Privacy Officers** (APO) would report administratively to the Director of their Agency, with the Chief Privacy Officer providing input on hiring and performance reviews. The APO would also have a secondary reporting relationship to the CPO. Activities that fall under the purview of this secondary reporting relationship include effectively collaborating on, influencing and implementing enterprise policies at the APO's respective agency.

Figure 5: Privacy function governance structure

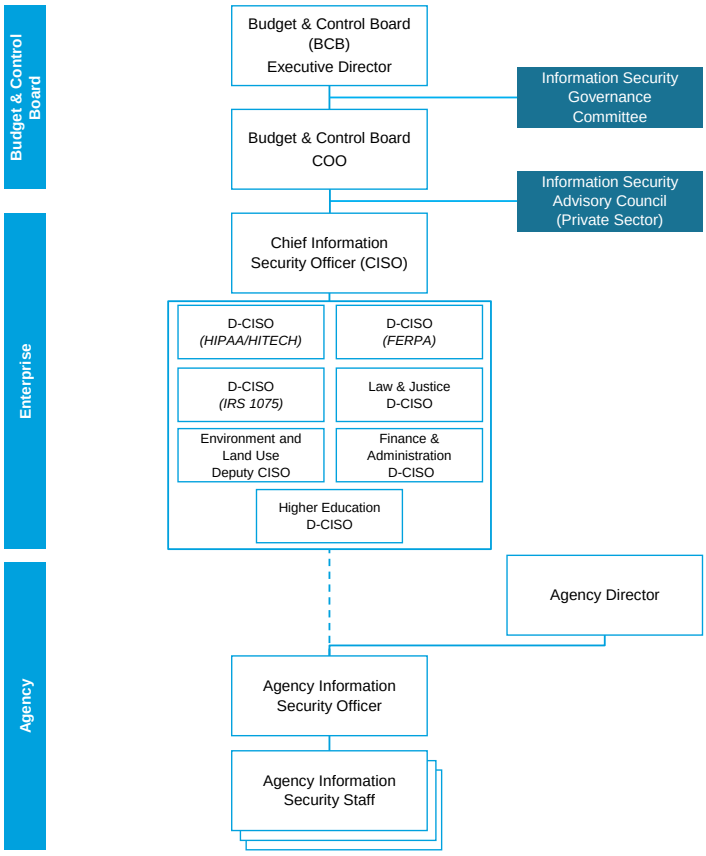


Security function

Figure 6 depicts the proposed governance structure of the security organization. The salient aspects of the proposed governance structure are outlined below:

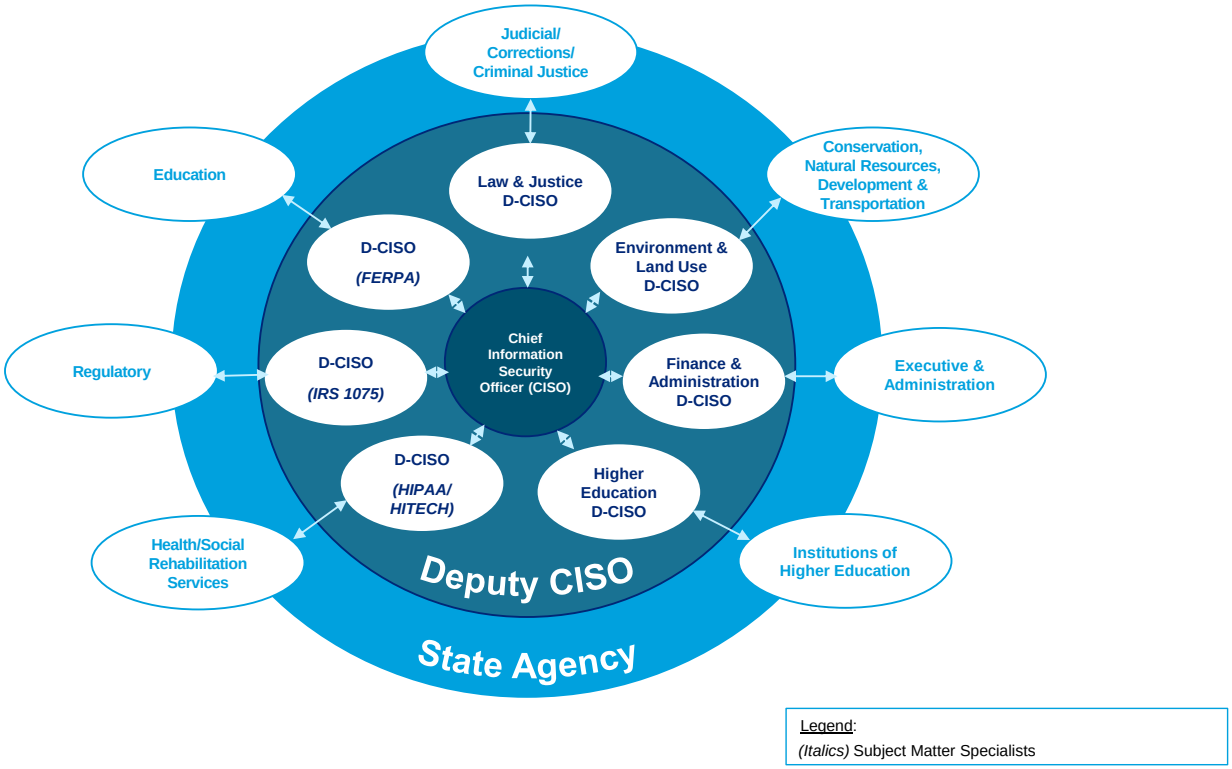
- Establish a **Chief Information Security Officer (CISO)** role at the enterprise level. This role would report administratively to the Chief Operating Officer of the Budget & Control Board.
- Establish seven **Deputy Chief Information Security Officers (D-CISO)** roles at the enterprise level. Each Deputy CISO would serve as the primary point of contact for a group of state agencies and would serve as a subject matter specialist in a certain security regulatory domain. These roles would report administratively to the Chief Information Security Officer.
- As it relates to the implementation of security measures to support agency programs and business, Agency **Information Security Officers (ISO)** would report administratively to the director of their agency. Agency ISOs would also have a secondary reporting relationship to the CISO. Activities that fall under the purview of this secondary reporting relationship include effectively collaborating on, influencing and implementing enterprise policies at the ISO's respective agency, and career development within the INFOSEC program. The enterprise Deputy Chief Information Security Officer is responsible for providing input on hiring and performance reviews for the ISOs. Once the enterprise INFOSEC program has been established, Agency ISOs are responsible for working with their agency CIO and Director, in coordination with the enterprise, to assess their agency's security, privacy and technology staffing needs.
- The Agency ISO may not be a full-time position for some agencies. In certain circumstances, the Agency ISO may report to another technology executive such as the Agency Chief Information Officer, rather than reporting directly to the Agency Director.

Figure 6: Security function governance structure



- Align **Deputy CISOs** with **state agencies**. Each Deputy CISO would serve as the primary point of contact for a group of state agencies and serve as a subject matter specialist in a certain security regulatory domain (see Figure 7). Should the State Agency submit a request that does not fall under the primary Deputy CISO's area of expertise, the primary Deputy CISO would identify and consult with the appropriate Deputy CISO and would facilitate agency transactions until the request is resolved.

Figure 7: Proposed alignment of Deputy CISOs and state agencies



Establish an INFOSEC governance committee and an INFOSEC advisory council, the details of which are described in figures 8 and 9.

Figure 8: Proposed Information Security Governance Committee

Information Security Governance Committee

- Membership:
  - Chair: Executive Director, BCB
    - CISO to prepare the agenda
  - COO, DSIT-CIO, CISO, CPO
  - One agency executive director or delegate from each Community of Interest, appointed by the BCB
    1. Education
    2. Regulatory
    3. Health / Social Rehabilitation Services
    4. Institutes of Higher Education
    5. Executive & Administration
    6. Conservation, Natural Resources, Development & Transportation
    7. Judicial / Corrections / Criminal Justice
- Function: Establish, steer, and guide Information Security program and strategy

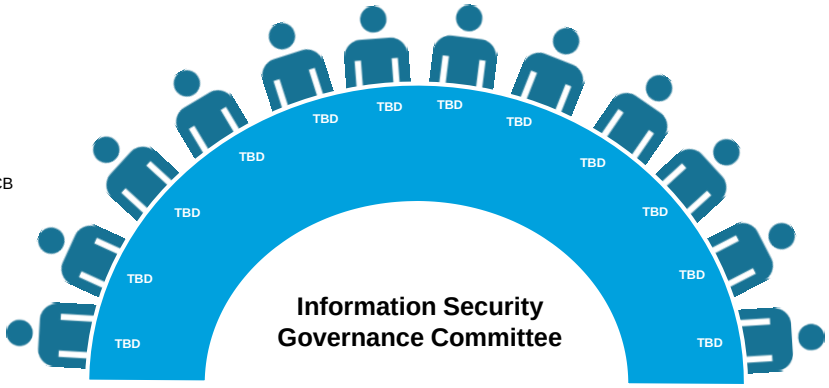
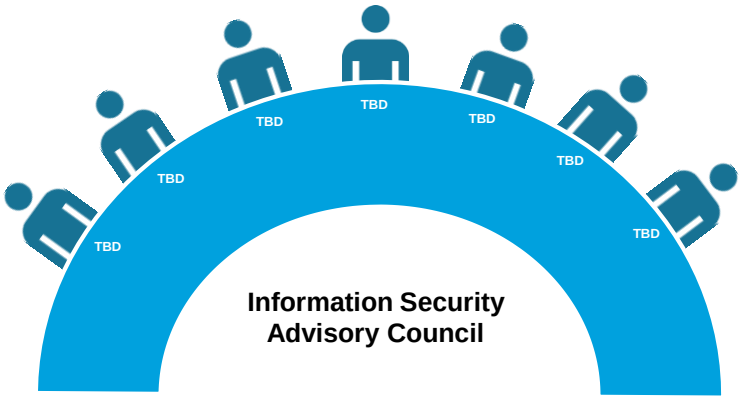


Figure 9: Proposed Information Security Advisory Council

Information Security Advisory Council

- Membership:
  - Chair: COO, BCB
    - CISO to prepare the agenda
  - DSIT-CIO, CISO, CPO
  - Private sector CISO, CPO and CIOs
- Function: Discuss leading Information Security practices

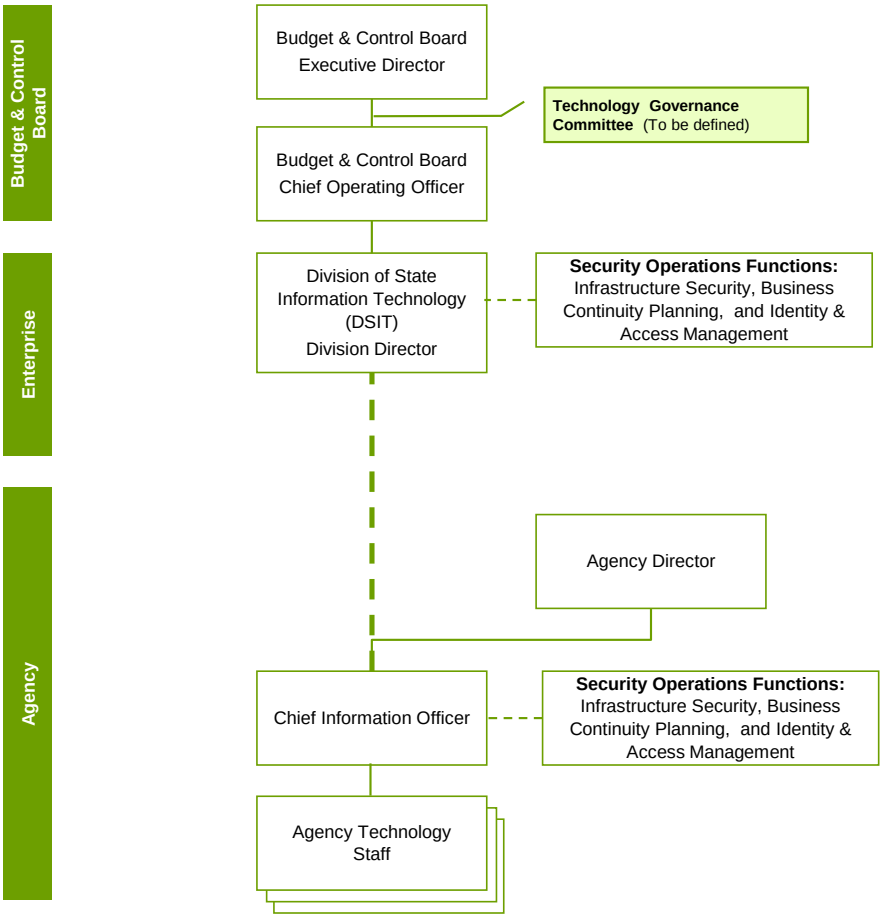


Technology and security operations function

Deloitte & Touche recommends a federated approach to coordinate the operational aspects of the security functions between the enterprise and agencies. Agency CIOs would be responsible for implementing enterprise level policies set forth for the operational security functions, while the DSIT Division Director and Agency CIOs would coordinate the operational aspects of security.

The current decentralized Information Technology (IT) governance model for the non-security technology functions (including technology strategic planning, investment governance and budgeting, enterprise architecture and infrastructure, innovation, solution delivery, and technology project management), is likely to constrain the effectiveness of the information security program. To overcome the challenges associated with multiple points of security risk evaluation, control and enforcement, we recommend that the State consider moving to a **federated governance model for IT** (depicted in Figure 10)**.** In addition to helping improve the State's information security posture, improved IT governance should also yield cost savings through the efficiencies achieved.

Figure 10: Technology and security operations function governance structure



4.3 Roadmap

The implementation of an information security program is an evolutionary process which requires a long-term commitment of leadership support and funding. Based on our observations of the State environment and our assessment of the security risks and vulnerabilities identified in a representative sample of three state agencies, the following three phase approach is recommended for establishing and maturing the State's INFOSEC program:

1. **Build foundation (year 1):** The focus of this phase is to address the immediate risks and vulnerabilities identified and to implement the foundational aspects of the INFOSEC program in fiscal year 2014 (FY14).
2. **Evolve (years 2-4):** This phase consists of building on the foundation that was laid in FY14 and continuing to evolve the program.
3. **Leading in class (years 5 and beyond):** The focus of this phase is on sustaining a leading INFOSEC program that continues to evolve in order to stay on top of rapidly changing cybersecurity threats.

The three phases provide a roadmap for investment in the State's INFOSEC program and are depicted in Figure 11. The activities under each of the phases are grouped into three categories: organization (i.e. people), process/policy and technology. A detailed description of each of the steps within the roadmap can be found in Appendix B of this report.

This initial report focuses exclusively on the first phase of the roadmap – the foundational phase – and proposes plans for each of the various initiatives (that can be found in Appendix C) for the State's consideration. As part of Task B of the current contract, Deloitte & Touche will perform some of the activities under the process/policy category of the first phase of the roadmap.

It should be noted that as a part of the first phase of the roadmap, Deloitte & Touche recommends that the State implement an enterprise security awareness program for state employees and strengthen the State's cybersecurity workforce through professional development and in partnership with universities through the development of an internship program.

Figure 11: Roadmap

	Build Foundation	Evolve	Leading in Class

Organization	• Governance
	  • Establish organization
	  • COO, CISO, Deputy CISOs
	  • CPO
	• Awareness, training and talent
	  • End user awareness and training program
	  • Training and professional development
	  • Internship and campus recruiting program
		• Job performance expectations framework for Information Security workforce
		• Joint performance reviews of agency ISOs
		• Identify talent strategies
		• Work with universities to evolve cybersecurity programs
			• Effective and collaborative governance
			• Grow and retain talent
			• Broad professional development
			• Metrics and monitoring
			• Mature cybersecurity talent sourcing program with local universities

Process / Policy	• Security framework • Security risk assessments • Security policy • Data classification • Agency risk profile	• Security policies, procedures and standards complementing agency specific policies, procedures, and standards • Agency security plans • Incident response team – Digital first responders • Establish ongoing compliance program	• Automated security functions allow for automated identification, prevention and closure of risks
Technology	• Secure network engineering • Data protection • Threat monitoring and control • Continuous vulnerability assessment and remediation	• Agency security shared services • Continuous threat and vulnerability management • Expand data protection • Identity and access management • Cyber threat analytics and intelligence	• Secure self-healing Infrastructure • Implement governance, risk, and compliance tools • Develop agency centers of excellence

Please refer to Appendix B for a detailed description of the roadmap.

4.4 Fiscal year 2014 budget

This section provides an overview of the budget estimate for implementing the proposed strategies and recommendations for fiscal year 2014 (see Figure 12). As part of the activities and deliverables for Task B of our contract with the State, Deloitte & Touche will provide budget recommendations for subsequent years during the fiscal year 2015 budgeting process. It is important for the State to support the INFOSEC program by providing appropriate budgetary support for the program.

Leading information technology, security and privacy salary benchmark reports were consulted as part of formulating the budget estimates for FY14 and local comparisons and adjustments were taken into account in deriving budget estimates for establishing the INFOSEC organization. To confirm the information used during budget development process, Deloitte & Touche reviewed the draft budgetary estimates and underlying assumptions with representatives from the Budget & Control Board. The estimated budget includes estimates for annual salary and benefits for new personnel, estimated startup expenses (including fixed and mobile phones, laptops, monitors and printers, as well as furniture, fixtures and supplies) and operating expenses (including leased office space, landline and cell phone service, travel, training and office supplies).

The security technology initiative budgets for FY14 were derived from estimates and assumptions with input from State personnel. Software, hardware, licenses, and maintenance costs are included in the technology budget. While most of the technology investments included in the budget are targeted toward enterprise level assets, there are some funds set aside in the budget estimates for agency remediation efforts, the allocation of which should be determined on a case-by-case basis. We recommend that the State implement the security technology recommendations as a foundation for enterprise level and agency level security improvements.

Because of the State's current decentralized and diverse technology environment, we recommend that agencies coordinate security related investments, purchases and initiatives with the Budget Control Board. This collaboration will help achieve three objectives:

- Target investments toward enterprise-endorsed security solutions
- Help achieve consistency across agency security implementations
- Enable the State to leverage economies of scale that come with collective purchasing agreements

Figures 12 below provide an overview of the budget estimates for fiscal year 2014. Appendix C provides additional details related to the budgetary estimates for the enterprise privacy organization and the enterprise security organization described within Section 4 of this document.

Figure 12: Fiscal year 2014 budget estimate[5]

	Activity	State FY2014 Budget Estimates	Future Reoccurring Budget Estimates
Organization	• **Enterprise Security Office**		
	• COO Office	$305,000	$283,000
	• CISO Office	$295,000	$276,000
	• Planning and strategy	$290,000	$276,000
	• Governance	$1,210,000	$1,150,000
	• Enterprise security technology	$1,680,000	$1,574,000
	• Cyber incident response and SWAT	$478,000	$448,000
	• Security training and cyber culture	$232,000	$218,000
	• **Enterprise Privacy Office**	$470,000	$440,000
	• **Awareness, Training and Talent**		
	• End user awareness and training program	$350,000	$350,000
	• Training and professional development	$50,000	$50,000
	• Annual security conference	$20,000	$20,000
	• Internship and campus recruiting program	$200,000	$50,000
Process / Policy	• Security risk framework and policy • Security risk assessments • Data classification	*Primarily accounted for by Task B activities*	
Technology	• **Enterprise Technology and Remediation**		
	• Secure network engineering	$2,385,000	$880,000
	• Data protection	$3,170,000	$1,150,000
	• Threat monitoring and control	$1,305,000	$140,000
	• Continuous vulnerability assessment and remediation	$2,490,000	$40,000
		$14,930,000	**$7,345,000**

[5] Please note the fiscal year 2014 budget does not include the costs of credit monitoring for citizens.

5 Conclusion

The implementation of a statewide information security program is an evolutionary process which requires a long-term commitment of funding, and both legislative and executive leadership support. This Initial Assessment Report provides recommendations for enhancing the State's INFOSEC program and outlines the organizational, governance and financial support required to implement the foundational aspects of the program in fiscal year 2014. It also contains recommendations for evolving and maturing the program in subsequent years, and for sustaining the program over the long-term in order to develop a leading INFOSEC program. A summary of the recommendations is outlined below.

State fiscal year 2014 recommendations:

1. Provide the financial support required for the INFOSEC program for fiscal year 2014.
2. Establish an enterprise information security organization with the authority to set, independently assess and enforce policy and to implement the INFOSEC program.
    a. Recognizing that it will likely take several months to hire personnel and to establish the organization, create an interim governing authority with responsibility for reviewing, approving and coordinating enterprise and agency information security procurements and projects.
3. Implement an enterprise security awareness program for state employees and strengthen the State's cybersecurity workforce through professional development and in partnership with universities through the development of an internship program.
4. Implement the immediate security technology recommendations as a foundation for enterprise and agency level security improvements.
5. Evaluate IT governance options and recommend a model to improve the State's technology governance to overcome the challenges associated with multiple points of security risk evaluation, control and enforcement that stem from the decentralized nature of the State's current information technology governance and assets.

In accordance with TASK B scope of work, Deloitte & Touche will continue to assist the State with the implementation of the State INFOSEC program, including supporting the State with the development of enterprise security policies, recommendations and funding estimates for State fiscal years 2015 and 2016.

Beyond fiscal year 2014, Deloitte & Touche recommends that the State business and executive leadership:

- Continue to review security risks on a regular basis
- Challenge the information security organization to stay abreast of evolving trends and threats
- Sustain funding for the information security program

The State not only has an opportunity to improve its overall information security posture through the implementation of the INFOSEC program recommendations, but also to further promote a cyber-savvy workforce and to help develop the next generation of cybersecurity professionals in collaboration with local universities.

6 Appendices

6.1 Appendix A: Description of the core elements of an information security program

Description of core functions: Privacy

Figure 13 describes the functions performed by the privacy organization.

Figure 13: Description of the privacy function

	Function	Description
Privacy	Data Classification	The privacy function defines "what" data should be protected, and the degree to which it should be protected based on the type of data that is being collected. The privacy function is responsible for analysis of the data agencies obtain, use and store within their systems and subsequent classification based on the degree of protection required by state and federal laws, regulations or standards (e.g. Social Security Numbers would be classified as Personally Identifiable Information based on federal & state laws).
	External Functions	• Public Awareness and Education: This function communicates the importance of privacy to the citizens. Examples of activities could include: Champion an annual South Carolina Privacy Day, development of a website dedicated to privacy, development of educational materials, offering of educational seminars. • Incident Response and Citizen Impact: This function operates an informational hotline that serves to answer questions that citizens may have about privacy matters, and provides guidance to citizens who suspect that their private information has been compromised or stolen. • Fraud Management: This function proactively follows and investigates leads about suspected fraud and works with other authorities to drive cases to a conclusion.

Description of core functions: Information security

Figure 14 describes the functions performed by the information security organization.

Figure 14: Description of the information security function

	Function	Description
Information Security	Planning and Strategy	Establishes the plan and the strategy for all information security activities. Responsible for confirming that information security controls are functioning as intended.
	Cyber Incident Response and SWAT	Digital first responders for the enterprise and agencies. Determines the cause, scope, and impact of incidents in order to stop unwanted activity, limit damage, and prevent recurrence.
	Governance	• Policies, Procedures, Guidelines: Development of processes and artifacts that support the governance of information security across the enterprise and all state agencies. • Funding and Budgeting: Development of a yearly budget for Information Security related activities. • Cybersecurity Framework: Adaptation of a recognized information security program framework such as National Institute of Standards and Technology (NIST) to the enterprise. • Agency Liaison and Coordination: Establish an agency liaison as a primary point of contact and coordinator for the requests of a state agency and provide subject matter knowledge in agency specific regulatory compliance. • Input on Legislation and Legal Matters: Provides expertise and input on legislation such as bills with an information security component. • KPI's, Metrics, Compliance, Reporting: Develops reporting mechanism such as a balanced scorecard of key performance indicators (KPIs) related to information security which is regularly distributed to relevant stakeholders (e.g. DSIT Division Director, CPO, Budget & Control Board, Agencies). • Establish Agency Risk Profile based on Data Classification: Together with the Information Security Governance Committee, leverage the data classification conducted by the privacy function to establish high, medium, and low risk profile categories for each agency and determines what the appropriate safeguards are for each category.

	Function	Description
Information Security	Enterprise Security Technology	• Secure System Engineering and Architecture: Design appropriate security architecture and controls in new systems or systems that are undergoing substantial redesign, including both in-house and outsourced solutions. • Layered 24x7x365 Cybersecurity Monitoring: Provides situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities. • Vulnerability and Risk Management: Continuous identification and remediation of vulnerabilities before they can be exploited. • Incident Response and Forensics: Determine the cause, scope, and impact of incidents to stop unwanted activity, limit damage, and prevent recurrence. • Privileged User Management: Definition of special requirements and management of powerful user accounts within the IT infrastructure.
	Security Training & Cyber Culture	• Security Awareness Program: Provides employees at all levels with relevant security information and training to decrease the number of security incidents. • ISO & Security Staff Training and Certification: Develop a training and professional development program leading to information security certifications for state employees in the information security field. Training is to be held on a regular basis and may include virtual instructor led training (ILT) and a semi-annual or annual security conference. • Talent Development - Scholarship & Internship: Establish an internship and work-study program with local universities to create a pipeline of early talent in the information security field. Scale the program to other areas of the organization (e.g. Division of State Information Technology) and increase the number of students in subsequent years. • Performance Expectations Framework: Develop a framework to measure the performance of all information security staff at the agency and enterprise level.

Description of core functions: Technology

Figure 15 describes the functions performed by the technology organization.

Figure 15: Description of the technology function

	Function	Description
Technology	Infrastructure Security	• Security Operations: Assess and address information systems security issues at a technical level. • Physical Security: Protect information systems and data from physical threats. • Network Security: Policies, procedures, standards, and controls related to helping to ensure the confidentiality of information on the network, protection of the integrity of the network itself and the information it is used to transport and the availability of the network to perform its function. • Application Security: Measures taken throughout an application's lifecycle to prevent exceptions in the security policy of an application or the underlying system through flaws in the design, development, deployment, upgrade, or maintenance of the application. • Data Security: Responsible for protecting information on computers and servers that routinely interact with untrusted devices on the internet or may be prone to loss or theft.
	Identity and Access Management	• Identity and Access Management: Establish the processes and technologies to manage identities of users and devices and control their access to resources and data on a need to know basis. Collect audit logs of user activities. • User Administration: Perform user account management and administration.
	Business Continuity (BC) / Disaster Recovery Planning (DRP)	• Business Impact Analysis: Predict the consequences of the disruption of a business function and gather and process information needed to develop recovery strategies. • Recovery Strategies and Plans for Services: Establish priorities and recovery time objectives for information technology including systems, applications and data. Priorities for IT recovery should be consistent with the priorities for the recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. • Coordination of Testing Activities: Practice BC/DRP scenarios and activities which would need to occur in the event of a disaster.

6.2 Appendix B: Description of components of the roadmap

Roadmap: Build foundation

Figure 16 details the activities included in the foundation building phase of the INFOSEC program roadmap.

Figure 16: Build foundation roadmap

	Function	Description

Organization	Governance	• Establish Organization: Finalize organizational structure and secure funding.
		  • COO, CISO, and Deputy CISOs: Develop job descriptions and hire resources.
		  • CPO: Develop job descriptions and hire resources.
		  • Develop staffing plan for the organization and execute.

	Awareness, Training and Talent	• End User Awareness and Training Program: Provide employees at all levels with relevant security information and training to reduce the number of security incidents. • Training and Professional Development: Professional training for security and technical workforce at Budget & Control Board and Agencies. • Internship and Campus Recruiting Program: Conduct talent needs assessment to determine immediate, medium and long-term staffing needs. Establish an internship and pilot work-study program to create a pipeline of early talent in the Information Security field.
Process / Policy	Security Framework	Adapt a recognized information security program framework, such as National Institute of Standards and Technology (NIST) and include technical controls and state specific elements from the SANS Institute.
	Security Risk Assessments	Conduct periodic enterprise and agency level risk and vulnerability assessments. Perform recurring assessments based on agency risk profiles.
	Security Policy	Develop artifacts that support the governance of Information Security throughout the Enterprise and across all Agencies.
	Data Classification	Establish an enterprise level Data Classification policy. The policy forms the foundation for discovering and understanding the data agencies hold and defines the degree of protection required.
	Agency Risk Profile	Together with the Information Security Governance Committee, leverage the data classification conducted by the privacy function to establish high, medium and low risk profile categories for each agency and determine appropriate security measures for each category.
Technology	Secure Network Engineering	Implement network security solutions to protect the communication session, control access, and provide protection against malicious threats.
	Data Protection	Identify the presence of sensitive data within the State's information technology (IT) environment and employ the appropriate level of data protection, including encryption.
	Threat Monitoring and Control	Enhance the current IT security monitoring and reporting capabilities through the use of logging, aggregation and analysis.
	Continuous Vulnerability Assessment and Remediation	Conduct continuous vulnerability assessments to identify, analyze and mitigate infrastructure and application vulnerabilities.

Roadmap: Evolve

Figure 17 details the activities included in the evolve phase of the INFOSEC program roadmap.

Figure 17: Evolve roadmap

	Function	Description
Organization	Performance Expectation Framework	Develop a framework to measure the performance of all Information Security staff at the agency and enterprise level.
	Joint Performance Reviews	Develop an annual performance review process for all Information Security employees.
	Identify Talent Strategies	Articulate what the value proposition of the organization is for employees. Investigate options in the areas of: recruiting, total rewards, early talent, leadership development and succession planning, and workplace customization.
	Work with Universities to Evolve Cybersecurity Programs	Work with universities to tailor the curriculum of the cybersecurity programs offered and continue to develop professional training program for security and technical personnel at the Budget & Control Board and Agencies.
Process / Policy	Security Procedures	Develop processes that support the governance of Information Security throughout the Enterprise and across all Agencies.
	Agency Security Plan	Document the approach that agencies will use to implement security measures.
	Incident Response Team	Establish the team that will be responsible for determining the cause, scope, and impact of incidents in order to stop unwanted activity, limit damage, and prevent recurrence.
	Establish Ongoing Compliance Program	Establish a program to track the compliance of individuals and agencies with Information Security policies, procedures and guidelines. Develop a procedure for addressing cases of non-compliance.
Technology	Agency Security Shared Services	Pooling of resources in a shared services capacity will allow the State to better address fluctuations in demand for these resources over time and to avoid the over-allocation of funds for dedicated resources that are already available elsewhere within their project portfolio.
	Continuous Threat and Vulnerability Management	Expand the established application vulnerability assessment process.
	Expand Data Protection	Expand the established data protection process to include the State's agencies, boards, and commissions that contain sensitive data.
	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 authentication, authorization, and auditing of employees, contractors, customers, and other stakeholders with access to resources including data, applications, and systems.
	Cyber Threat Analytics and Intelligence	To combat cyber attacks, utilize leading industry practices and solutions to perform cyber threat analytics and gather intelligence.

Roadmap: Leading in class

Figure 18 details the activities included in the third phase of the INFOSEC program roadmap.

Figure 18: Leading in class roadmap

	Function	Description
Organization	Effective and Collaborative Governance	Establish centers of excellence for effective and collaborative governance with agencies. The centers of excellence will be used to align agency information security requirements with enterprise strategy, and to share best practices on processes, policies, procedures, and standards.
	Grow and Retain Talent	Implement talent recruitment and retention strategies including: total rewards, early talent, leadership development, succession planning and workplace customization.
	Broad Professional Development	Develop a training and professional development program leading to information security certifications for state employees in the information security field. Training is to be held on a regular basis and may include virtual instructor led training (ILT) and a semi-annual or annual security conference.
	Metrics and Monitoring	Develop a reporting mechanism such as a balanced scorecard of key performance indicators (KPIs) related to information security which is regularly distributed to relevant stakeholders (e.g. DSIT Division Director, CPO, Budget & Control Board, Agencies).
	Mature Cybersecurity Talent Sourcing Program with Local Universities	An established cybersecurity program is offered by local universities and is used as a talent pipeline for security and technical workers at the Budget & Control Board and Agencies.
Process / Policy	Automated Security Functions (Access Management, Monitoring, etc.)	Automate security functions to measure, control and help ensure confidentiality, integrity, and availability of the information processed and stored by automated information systems.
Technology	Secure Self-Healing Infrastructure	Establish a more proactive program to identify and remediate security threats and to react more rapidly when breaches do occur. Anticipate and prevent attacks when possible, but be ready to isolate and encapsulate intrusions when they do occur in order to decrease impact.
	Implement Governance, Risk, and Compliance Tools	With a view to the future, expand the regulatory compliance process to embrace automation and make effective risk-based decisions; constantly monitor/review the state's compliance posture, perform internal audits and prepare for external audits.
	Develop Agency Centers of Excellence	Establish innovative approaches to the state's shared services program and establish competency centers of excellence through security shared services to promote and mature security services.

6.3 Appendix C: Detailed budget estimates

Enterprise Security Office

The Enterprise Security Office has the responsibility for setting information security strategy, developing information security frameworks and policies, facilitating communication to employees and providing subject matter expertise. Responsibility for implementation will remain with state agencies. Further activities carried out by the Enterprise Security Office include: architecture of enterprise security technology, cyber incident response, root cause analysis, and security training. The proposed Enterprise Security Office may consist of thirty-four (34) full-time employees for which the approximate costs are detailed below. The costs include their overall annual salary and benefits, startup cost (land phone device cost, cell phone device cost, laptops, monitors, printers as well as furniture, fixtures and supplies) and operating cost (leased office space, land phone service, cell phone service, travel, training and office supplies).

Enterprise Security Office - Budgetary Estimate

Position		Salary	Reoccurring Benefits	Operating Cost	One-Time Startup Cost	Reoccurring Total Cost	One-Time Total Cost
Chief Operating Officer	COO	$ 155,000	$ 48,050	$ 7,450	$ 15,000	$ 210,500	$ 15,000
Chief Security Officer	CSO	$ 150,000	$ 46,500	$ 7,000	$ 7,000	$ 203,500	$ 7,000
Admins	Admin	$ 50,000	$ 15,500	$ 7,000	$ 12,000	$ 72,500	$ 12,000
	Admin	$ 50,000	$ 15,500	$ 7,000	$ 7,000	$ 72,500	$ 7,000
Planning and Strategy	IT Security Manager	$ 100,000	$ 31,000	$ 7,000	$ 7,000	$ 138,000	$ 7,000
	IT Security Manager	$ 100,000	$ 31,000	$ 7,000	$ 7,000	$ 138,000	$ 7,000
Governance	Deputy CISO - HIPAA	$ 120,000	$ 37,200	$ 7,200	$ 9,000	$ 164,400	$ 9,000
	Deputy CISO - FERPA	$ 120,000	$ 37,200	$ 7,200	$ 9,000	$ 164,400	$ 9,000
	Deputy CISO - IRS 1075	$ 120,000	$ 37,200	$ 7,200	$ 9,000	$ 164,400	$ 9,000
	Deputy CISO - Law Enforcement	$ 120,000	$ 37,200	$ 7,000	$ 8,500	$ 164,200	$ 8,500
	Deputy CISO - Environment and Land Use	$ 120,000	$ 37,200	$ 7,000	$ 8,000	$ 164,200	$ 8,000
	Deputy CISO - Finance	$ 120,000	$ 37,200	$ 7,000	$ 8,000	$ 164,200	$ 8,000
	Deputy CISO - Higher Education	$ 120,000	$ 37,200	$ 7,000	$ 8,500	$ 164,200	$ 8,500
Enterprise Security Technology	IT Security Manager	$ 100,000	$ 31,000	$ 7,600	$ 7,600	$ 138,600	$ 7,600
	IT Security Architect	$ 90,000	$ 27,900	$ 7,100	$ 7,100	$ 125,000	$ 7,100
	IT Security Architect	$ 90,000	$ 27,900	$ 7,100	$ 7,100	$ 125,000	$ 7,100
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Manager	$ 100,000	$ 31,000	$ 7,500	$ 7,500	$ 138,500	$ 7,500
	IT Security Architect	$ 90,000	$ 27,900	$ 7,100	$ 7,100	$ 125,000	$ 7,100
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
Cyber Incident Response	IT Security Manager	$ 100,000	$ 31,000	$ 7,800	$ 7,800	$ 138,800	$ 7,800
	IT Security Architect	$ 90,000	$ 27,900	$ 7,000	$ 7,600	$ 124,900	$ 7,600
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,300	$ 92,150	$ 7,300
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,300	$ 92,150	$ 7,300
Security Training & Cyber Culture	IT Security Architect	$ 90,000	$ 27,900	$ 7,450	$ 7,500	$ 125,350	$ 7,500
	IT Security Analyst (Blended)	$ 65,000	$ 20,150	$ 7,000	$ 7,000	$ 92,150	$ 7,000
					Total	**$4,224,100**	**$ 265,900**
					Grand Total		**$4,490,000**

Salary data for positions within the Enterprise Security Office is based on the estimates provided in the Section 8 "Methodology & Definitions - Information Security Salary Estimates."

Enterprise Privacy Office

The Enterprise Privacy Office manages the protection of personally identifiable information (PII) and other sensitive information that is collected, used, transferred, and maintained by the enterprise and state agencies. The office is responsible for the analysis of sensitive data that agencies obtain, use and store within their systems as well as for subsequent classification based on the degree of protection required by federal and state laws, regulations or standards. The Enterprise Privacy Office works in close cooperation and collaboration with the Enterprise Security Office, the Division of State Information Technology and coordinates privacy matters with the agencies. Further activities include public awareness and education, incident response, mitigation of impact to citizens caused by cyber-attacks and fraud management. The proposed Enterprise Privacy Office may consist of three (3) full-time employees for which the costs are detailed below.

Enterprise Privacy Office - Budgetary Estimate

		Reoccurring		One-Time	Reoccurring	One-Time
Position	**Salary**	**Benefits**	**Operating Cost**	**Startup Cost**		
Chief Privacy Officer (CPO)	$ 120,000	$ 37,200	$ 7,000	$ 11,800	$ 164,200	$ 11,800
Deputy Chief Privacy Officer (D-CPO)	$ 100,000	$ 31,000	$ 7,000	$ 9,000	$ 138,000	$ 9,000
Deputy Chief Privacy Officer (D-CPO)	$ 100,000	$ 31,000	$ 7,000	$ 9,000	$ 138,000	$ 9,000
				Total	**$ 440,200**	**$ 29,800**
				Grand Total		**$ 470,000**

Salary data for the Chief Privacy Officer (CPO) position was retrieved from the *International Association of Privacy Professionals* which reports an average base salary of $118,367 with 223 CPOs reporting in the Southern region of the United States:

https://www.privacyassociation.org/resource_center/privacy_research/iapp_2013_privacy_professionals_salary_survey#cpo.

Salary data for the D-CPO positions are based on the salary of the IT Security Manager role in the Section 8 “Methodology & Definitions - Information Security Salary Estimates.”

The costs include their overall annual salary and benefits, startup cost (land phone device cost, cell phone device cost, laptops, monitors, printers as well as furniture, fixtures and supplies) and operating cost (leased office space, land phone service, cell phone service, travel, training and office supplies).

Awareness, Training and Talent

The purpose of the Awareness, Training, and Talent area is to enhance the State’s talent and develop additional skills in information security. The initiatives will grow and mature the State’s information security workforce and increase the security awareness of the state government employees with regards to information security. These initiatives include the following:

- End user awareness and training program
- Training and professional development
- Annual security conference
- An internship and campus recruiting program

By completing these initiatives, the state will be able to enhance the skill set of employees while reducing the risk of a data breach through learning and education.

End User Awareness and Training Program

Provide the State’s approximately 50,000 employees who have access to Information Technology computing devices with relevant information security training to decrease the number of security incidents. The budgetary estimate includes the online security awareness training licenses as well as administration and customization expenses.

Security Awareness Training - Budgetary Estimate

Position	Reoccurring
Licenses for 50,000 Seats	$ 200,000
Administration and Customization	$ 150,000
Grand Total	**$ 350,000**
Variables:	
Number of Seats	50,000
Annual Licensing Cost per Seat	$ 4

Training and Professional Development

Develop a training and professional development program leading to Information Security certifications for state employees that work in Information Security or are involved in handling sensitive state data. Training should be held on a regular (i.e. monthly or quarterly) basis and may include vendor-led seminars and (virtual) instructor led training. Training should be tracked and provided at a minimum on an annual basis. The budgetary estimate includes costs associated with this program, including travel, facilities and logistics.

Training - Budgetary Estimate

Position	Reoccurring
Travel, facility, logistics, etc.	$ 50,000
Grand Total	**$ 50,000**

Annual Security Conference

Conduct an annual security conference for state employees from the Enterprise Security Office, Enterprise Privacy Office, Division of State Information Technology as well as Agency Information Security and Agency Privacy Officers. The security conference is held at a central location and may span multiple days educating the employees on security topics (e.g. Data Leakage Protection, Cloud Computing risks, Regulatory updates, etc.) The budgetary estimate includes costs associated with this conference, including travel, facilities and logistics.

Annual INFOSEC Budgetary Estimate

Position	Reoccurring
Travel, facility, logistics, etc.	$ 20,000
Grand Total	**$ 20,000**

Internship and Campus Recruiting Program

Establish an internship and work-study program to create a pipeline of early talent to work in Information Security. The budget may be used to scale the program to other areas of the organization (e.g., Division of State Information Technology) and increase the number of students in subsequent years. These students gain work experience, become familiar with the State's operations and may eventually become future full-time employees.

Campus Recruiting Program - Budgetary Estimate

Position	Reoccurring	One-Time
Consultant	$ -	$ 150,000
Student Salaries	$ 50,000	$ -
Total	**$ 50,000**	**$ 150,000**
	Grand Total	**$ 200,000**

Information Security Salary Estimates

The salary data used in this budget are based on two salary research reports.

Report 1: *2012 Mercer Salary Study of Information Technology Positions*.

The *2012 Mercer Salary Study of Information Technology Positions* uses percentiles (10th, 25th, Median, Mean, 75th, 90th) to account for differences in labor cost of Metropolitan Statistical Areas within the United States. However, the report does not provide guidance into which category Columbia, SC falls.

Report 2: *2013 ComputerEconomics IT Salary Report*.

The *2013 ComputerEconomics IT Salary Report* is an annual cross-industry survey which takes into account private and public sector salaries. The report uses percentiles (10th, 25th, Median, 75th, 90th) to account for differences in labor cost of Metropolitan Statistical Areas within the United States. While Columbia, SC is listed as a separate Metropolitan Statistical Area (MSA), salary data from 39 comparable MSA's such as Cedar Rapids, IA, Wichita, KS, Columbia, MO, Fargo, ND, Sioux Falls, SD and Knoxville, TN were taken into account to increase the salary sample size and receive a higher degree of accuracy.

When the *2012 Mercer Salary Study of Information Technology Positions* data was compared to the data from the *2013 ComputerEconomics IT Salary Report,* there was sufficient data correlation to use the 25th percentile of the *2012 Mercer Salary Study of Information Technology Positions* and the median of the *2013 ComputerEconomics IT Salary Report* as input data for a proposed salary estimate.

To retrieve the proposed salary estimate, the average between the data of the *2012 Mercer Salary Study of Information Technology* and *2013 ComputerEconomics IT Salary Report* was used and rounded to an even number.

Five IT positions were investigated:

- Chief Information Security Officer (CISO): The highest level executive dedicated to IT security who is responsible for the organization's development and enforcement of security policy and strategy. Oversees the selection, development, deployment, monitoring, maintenance and enhancements of the organization's security technology.
- Deputy Chief Information Security Officer (D-CISO): Responsible for the delivery of IT security services and functions. Liaisons between the CISO and the Agencies.
- IT Security Manager: Manages the development and delivery of IT security standards, leading practices, architecture and systems to implement information system security across the enterprise.
- IT Security Architect: Develops and implements enterprise information security architectures and solutions. Serves as a security expert in application development, database design, network and/or platform efforts, helping project teams comply with enterprise and IT security policies, industry regulations, and leading practices.
- IT Security Analyst (Blended across Associate, Intermediate, Senior levels): Performs procedures asked to implement the safety of Information Systems Assets and to protect systems from intentional or inadvertent access or destruction.

(Position descriptions retrieved from *2012 Mercer Salary Study of Information Technology Positions*)

Salary for Budgetary Estimate		***1. 2012 Mercer Salary Study of Information Technology***					***2. ComputerEconomics 2013 IT***		
Role	Salary			10%	25%	Mean	Tab	25%	Median
CISO	**$ 150,000**	Chief Info Security Officer		$ 121,400	**$ 150,400**	$ 172,800	CISO	$ 120,662	**$ 153,076**
D-CISO	**$ 120,000**	IT Security Director		$ 110,700	**$ 123,700**	$ 140,600	CISO	**$ 120,662**	$ 153,076
IT Security Manager	**$ 100,000**	IT Security Manager		$ 92,500	**$ 101,600**	$ 113,800	Managers	$ 71,726	**$ 90,994**
IT Security Architect	**$ 90,000**	Information Security Architect		$ 83,000	**$ 89,200**	$ 105,900	Architect	$ 68,596	**$ 88,700**
IT Security Analyst (Blended)	**$ 65,000**	Analyst	Associate	$ 44,400	$ 48,300	$ 56,900	Analyst		**$ 66,557**
			Intermediate	$ 54,500	$ 60,550	$ 71,675			
			Senior	$ 72,500	$ 79,450	$ 91,175			
			Blended	$ 57,133	**$ 62,767**	$ 73,250			

Technology Vulnerability Remediation Estimates

The technology data used in this budget is based on a five (5) step approach.

Step 1: Identify Technology Needs

The information security risk and vulnerability assessment identified technology gaps at the institution and two agencies which were reviewed as part of the initial assessment.

Step 2: Determine Technology Solution

Based on the technology gaps detected, research reports from Gartner, International Data Corporation (IDC), and Forrester were utilized to identify leading-in-class and cost-effective technology solutions to address serious information security gaps and vulnerabilities.

Additionally, Deloitte corroborated with the Information Security team at the Division of State Information Technology (DSIT) to understand the enterprise security needs of the state.

Step 3: Define Assumptions

The following assumptions were used to develop the budget estimates:

- 10,000 Remote Users
- 50,000 - 60,000 State Employees
- 3 - Year Initial Contract

Step 4: Obtain Vendor Quotes

Based on the assumptions in Step 3, Deloitte obtained quotes from technology vendors as well as DSIT's procurement department who helped Deloitte understand the state procurement process and the current list of state preferred vendors.

Step 5: Contingency Estimates

A 20% contingency for procurement and administrative overhead was added to the overall technology budget. This also accounts for the fact that quotes from the technology vendors may not contain all the necessary information that may increase the pricing.