# State of South Carolina Interim Security Assessment

Deloitte & Touche LLP

**Date: October 28, 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 ..... 5**

**2 Background ..... 6**

**3 Approach ..... 8**

**4 Progress ..... 9**

4.1 Summary ..... 9

4.2 Organization ..... 10

4.3 Process/Policy ..... 11

4.4 Technology ..... 12

4.5 Fiscal year 2015 budget ..... 14

**5 Conclusion and Next Steps ..... 15**

**6 Appendices ..... 16**

6.1 Appendix A: Description of components of the roadmap ..... 16

6.2 Appendix B: Budget Summary ..... 19


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.

# 1 Executive summary

Since March 23rd, 2013, Deloitte & Touche LLP ("Deloitte & Touche") has assisted the State the South Carolina ("State") in assessing the State's information security risks and vulnerabilities, and with the development and implementation of a statewide Information Security ("INFOSEC") program. This Interim Security Assessment report provides observations by Deloitte & Touche since the issuance of the Initial Security Assessment report May 1st 2013 as well as recommendations related to the ongoing implementation of the INFOSEC program.

The State has made progress in the implementation of the INFOSEC program including information security recommendations provided by Deloitte & Touche within the Initial Security Assessment report. Notably, based on information provided by the State, it has either initiated or continued:

- Implementing a federated **information security governance model** that will be led by INFOSEC professionals, such as the State's Chief Information Security Officer (CISO) and the State's Chief Privacy Officer. Position descriptions for these and other INFOSEC leadership roles have been developed and hiring for security personnel is in process;

- Performing **agency-level risk assessments** at selected State agencies and presenting observations and remediation guidance to agency leadership. The risk assessments consisted of both technical vulnerability assessments and qualitative analyses of information security capabilities at the agencies;

- Creating and releasing an **information security self-assessment tool** to help agencies perform internal risk assessments of their organization's security posture and to help identify areas of information security risk. The self-assessment tool provides customized guidance on specific issues and remediation guidance at the agency level;

- Developing and releasing foundational **INFOSEC Policies and Recommended Technology Solutions**. During September and October, four of these INFORSEC policies were released statewide. Additional INFOSEC policies and Recommended Technology Solutions are scheduled to be released during the month of December;

- Creating and releasing a **data classification model** to categorize the State's data for more efficient use and protection. This classification schema is used to help protect against the loss or misuse of sensitive information, and to help agencies and the State prioritize investments in additional information and data security;

- Creating and posting a Request for Proposals (RFP) seeking a comprehensive, **online-based cyber-security training program for State employees**. Training for State employees can help prevent motivated aggressors from attacking government systems, stealing data and harming critical infrastructure. This training is anticipated to be available before calendar year end.

The remainder of this report provides an overview of a suggested approach for implementation of the State's INFOSEC program, current activities performed during the implementation of the program, as well as the progress made to date. It also includes recommended next steps to be taken as the State makes progress towards assisting its agencies and institutions achieving a more mature information security posture.

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.

# 2 Background

In March 2013, Deloitte & Touche was awarded a three-year contract that included two task orders (Task A and B) to assist the State with identifying and providing guidance to address information security vulnerabilities, and with implementing a statewide INFOSEC program. As part of Task A, a preliminary security assessment was conducted and on May 1, 2013, Deloitte & Touche presented results which included information security risks and areas of opportunity for improving the security posture of the State. Recommendations derived from the preliminary assessment included the following areas:

- Provide the necessary organizational, governance and financial support required to implement the foundational aspects of the INFOSEC program in FY 2014, and to further evolve and enhance the program in future years;
- Implement security technology improvements as a foundation for enterprise security improvements;
- Design and implement a governance structure for an enterprise information security organization with the authority to define, assess and enforce policy and stand up the INFOSEC program;
- Create and implement an enterprise security awareness program for state employees, and strengthen the cyber security workforce through professional development.

The State's FY13-14 Budget, approved and ratified on June 19, 2013[2], provides $10.6 million for the newly created Budget and Control Board Division of Information Security (DIS). The DIS budget included $5.8 million in recurring funds and $4.8 million in non-recurring funds. The budget created twenty one new positions within DIS, three new positions within the Privacy Office, and will better enable the State to invest in several enterprise technology solutions that will help improve the cyber security posture of agencies.

As part of Task B, the Deloitte & Touche assisted the State with conducting the following INFOSEC initiatives:

- **Governance** — continued development of a federated information security governance model by creating and posting INFOSEC role position descriptions, including the Chief Information Security Officer and Chief Privacy Officer positions.
- **Risk Analysis** — conducted concurrent risk assessments at selected state agencies and presenting observations and remediation options to agencies and State leadership. These risk analyses consisted of both technical vulnerability assessments and qualitative analyses of agencies' information security infrastructure. Results were provided to the agency directors.
- **Risk Management** — developed and released an information security self-assessment tool that will help enable State agencies to internally identify, remediate, and manage information security risks identified through self assessments driven internally at each agency. The self-assessment tool domains are based on the INFOSEC framework that was developed for and approved by the State and that is currently utilized by Deloitte & Touche to perform risk assessments at State agencies.

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.

- **Information Security Policy and Recommended Technology Solutions** — created and released four new enterprise-wide information security policies; additional policies are under development and will be released over the coming months.

- **Data Classification** — created a data classification model to characterize the State's data for more efficient use and protection. This classification schema is used to protect against the loss or misuse of sensitive information, and to help agencies and the State prioritize investments in additional information and data security.

- **Training and Workforce Development** — released a Request for Proposal (RFP) seeking a broad, online-based cyber-security training program for State employees. Information security awareness is foundational for enabling the security posture of individual agencies as well as the State as a whole. In addition, Deloitte and Touche is assisting the State with development of information security professional development program and career paths. Key goals of the INFOSEC professional development program include determining the skill sets required within particular INFOSEC professional categories and specialty areas, and recommending corresponding development paths, training courses and certifications, as applicable. The objective is to provide INFOSEC professionals with continuous learning opportunities, and develop leaders that can lead a cyber-security workforce.

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.

# 3 Approach

As approved by the State during Task A, Deloitte & Touche has continued to use a four-step approach to assist the state on INFOSEC program activities.

Information security risk assessments have continued to be performed by using the risk assessment framework approved by the State. Additionally, conferences and regular meetings have been coordinated with Agency and IT Directors, State executives, and key stakeholders, such as the Executive Director of the Budget and Control Board; these meetings have been used to disseminate newly implemented security initiatives and to engage agencies and institutions of the State during the implementation of the INFOSEC program.

**Figure 1: Approach and activities performed to date (Task A and B)**

**1: Planning**

- Updated Task B project plan
- Arranged necessary logistics (technical and managerial)
- Collected relevant policies, procedures, and guidelines documents

**2: Agency Security Risk Evaluation**

- Conducted 8 vulnerability assessments
  - Scanned a range of about 215,000 IP addresses
  - Assessed 66 applications
- Conducted 9 security risk assessments
  - Conducted 69 interviews with agency representatives to assess risks and existence of managerial, operational and technical controls

**3: Program Implementation**

- Continued building new INFOSEC governance structure
  - In process of selecting State CISO
  - Created and posted position description for State CPO
- Developed new enterprise security policies and technology recommendations
- Created agency self-assessment tool to help agencies assess their current practices against potential risk

**4: Reporting**

- Documented observations and remediation recommendations
- Reviewed individual agency security risk assessments and vulnerability assessment results with directors of the respective agencies
- Reviewed and refreshed recommendations that were based on the assessments, budget, governance and INFOSEC roadmap which are included interim roadmap

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.

# 4 Progress

## 4.1 Summary

As recommended by Deloitte & Touche as part of Task A, the State has taken several steps in the areas of governance, investment in foundational aspects of the INFOSEC program, and progressing through a three-phase roadmap that includes the following dimensions:

- Organization – the State has established an enterprise information security structure
- Process/Policy – created and released new enterprise-wide information security policies
- Technology – developed a list of recommended information security solutions to address a federated model, and is in the process of acquiring enterprise information security solutions

This roadmap will help guide the State in the immediate and long term future as it seeks to enhance its information security posture.

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.

## 4.2 Organization

In the interim public report delivered May 2013, Deloitte & Touche recommended the State consider adopting a federated information security governance model. This recommendation was based on workshops with State Budget Control Board personnel, findings from the State Inspector General's report, the 2010 and 2012 Deloitte-NASCIO cyber security studies, and the decentralized model of the State's governance model. In a federated model, the enterprise sets strategy, develops frameworks and policies, facilitates communication and provides subject matter expertise while agencies actively participate in shaping INFOSEC strategy and remain responsible for implementing specific policies and programs locally at agencies and institutions.

It is important in the federated INFOSEC model that the State is currently implementing that the executive leadership of the agencies and institutions within the State be actively engaged with the implementation of the INFOSEC program within their respective organizations. This includes

- Setting the "tone at the top" making information security a priority within their organization;
- Sponsoring the implementation of the INFOSEC program within their organization including adoption of the State's security policies, conducting risk assessments, and remediation of vulnerabilities / control gaps within their organization; and,
- Understanding the relationship among DIS, DSIT and their organization's information security function and IT function.

While DIS will support the implementation of state-wide policies and state-wide security services, the individual agencies and their respective leadership are ultimately accountable for the implementation of the INFOSEC program within their organizations. The State has also determined that cyber security awareness training for State employees is a critical component of its INFOSEC program. Training for State employees aids in the prevention of attacks by motivated adversaries who target government systems, steal data and harm critical infrastructure. Deloitte & Touche assisted the State with developing a Request for Proposal (RFP), seeking a vendor to develop and deploy an online employee cyber security awareness training program and curriculum, to be made available to agency employees.

The following summarizes the progress the State has made to date from an organizational perspective in accordance with the INFOSEC roadmap.

| Function | Current Status | Next Steps |
|---|---|---|
| Governance | • Organizational structure finalized<br>• CISO and CPO job descriptions finalized and hiring process initiated | • Develop job descriptions for other leadership positions (Deputy CISOs, COO) |
| Awareness, Training and Talent | • Developed and issued an RFP for Employee Cyber Security Awareness Training program<br>• State procurement has reviewed responses to the RFP and is in process | • Deploy awareness training program across the enterprise<br>• Develop professional development program to define training paths for INFOSEC personnel, attract new talent, and minimize rotation of personnel |

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.

| | | |
|---|---|---|
| | of selecting a vendor<br>• Information security skill set developed for statewide workforce assessment | |

## 4.3 Process/Policy

A statewide INFOSEC framework was developed based on leading practices from the National Institute of Standards and Technology (NIST), other authoritative sources, and security models from other state governments, and approved by the State. This framework provides the overall guidelines for enhancing and sustaining the State's information security posture. As agreed to with the State, Deloitte & Touche has used a multi-pronged approach to assess South Carolina's information security infrastructure based on the approved framework. Initial risk assessments have been conducted for nine agencies to date, consisting of both technical network and application vulnerability assessments (quantitative), and information security risk assessments (qualitative). Risk assessments should continue on a periodic basis to assist the State in understanding its ongoing information security risks.

In addition, the State has released a data classification schema, as suggested by Deloitte & Touche in its initial set of recommendations. The data classification schema has been made available to agencies in order to help categorize data elements collected, processed, and stored by agencies and institutions. Data will be categorized by type, location, and level of sensitivity, among other factors, which in turn will enable State agencies to better prioritize information security investments and data protection efforts. Finally, the State has released four enterprise-wide security policies since May 2013, with additional policies and recommended technology solutions to be released and disseminated to the agencies over the coming months.

The following summarizes the progress the State has made to date from a process and policies perspective in accordance with the INFOSEC roadmap.

| Function | Current Status | Next Steps |
|---|---|---|
| Security Framework | • Developed an enterprise-wide INFOSEC framework, based on information security sources, including NIST | • Develop an ongoing compliance program that measures alignment the framework |
| Security Risk Assessments | • Completed security risk assessments at nine agencies<br>• Provided individual results of assessments and remediation options to agency executive leaders<br>• Provided summary findings and remediation options to State leadership<br>• Deployed and in process of training agencies on information security self-assessment tool which is designed to | • Complete additional nine agency risk assessments<br>• Review remediation efforts of the agencies and provide recommendations for remediation assistance where needed<br>• |

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.

| | | |
|---|---|---|
| | better enable agencies to measure their own information security posture | |
| Security Policy | • Designed and released four new enterprise-wide security policies:<br>o Asset Management<br>o Human Resources and Security Awareness<br>o Risk Management<br>o Information Systems Acquisition, Development, and Maintenance | • Release additional enterprise-wide security policies and associated Recommended Technology Solutions over the next three months<br>• Monitor and evaluate polices on an as-needed basis |
| Data Classification | • Deployed and provided training on an initial IT asset management tool to assist agencies with identification of systems within their organization that contain data<br>• Established an enterprise-wide data classification schema and delivered it to agencies | • Pilot sensitive data discovery tool to assist with data identification and subsequent classification<br>• Determine appropriate security measures based on data classification |
| Agency Risk Profiles | • Established risk profile categories for each agency, along with an information security framework for each category<br>• Created an information security self-assessment tool to help agencies auto-classify internal information security risks | • Based on the risk levels observed, determine appropriate ongoing security measures for each agency |

## 4.4 Technology

In conjunction with the analysis of the State's information security infrastructure and capabilities, Deloitte & Touche recommended several technologies to enhance and sustain the State's information security capabilities. The State has made progress toward fulfilling these recommendations and is currently of evaluating, procuring, designing, and implementing the solutions described below.

The vulnerability assessments being conducted at individual agencies provide the opportunity to develop recommendations for agencies' particular information security needs. A strong INFOSEC infrastructure depends on designing the program to meet agency as well as enterprise objectives.

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.

The following summarizes the progress the State has made to date from a technology perspective in accordance with the INFOSEC roadmap.

| Function | Current Status | Next Steps |
|---|---|---|
| Secure network engineering | • Identified and distributed enterprise information security solutions for access controls and protect against malicious threats | • Establish and implement a distributed enterprise solution |
| Data protection | • Identified the different types of sensitive data within the State environment<br>• Developed and delivered asset management guidance and data classification schema | • Perform a data discovery exercise to identify the presence of sensitive data, and employ the appropriate level of data protection |
| Threat monitoring and control | • Identified information security solutions to enhance the current IT security monitoring and reporting capabilities of the State | • Enhance threat monitoring to include cyber threat analytics and gathering intelligence |
| Periodic vulnerability assessment and remediation | • Conducted vulnerability assessments to help identify, analyze and mitigate infrastructure and current application vulnerabilities | • Establish a program to track the remediation of future vulnerabilities identified during periodic vulnerability assessments |

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.

## 4.5 Fiscal year 2015 budget

This section provides an overview of the budget estimate for implementing the proposed strategies and recommendations for fiscal year 2015 (see Figure 2).

Leading information technology, security and privacy salary benchmark reports were consulted as part of formulating the budget estimates for FY15 and local comparisons and adjustments were taken into account in deriving budget estimates for establishing the INFOSEC organization. Deloitte & Touche reviewed the draft budgetary estimates and underlying assumptions with representatives from the Budget & Control Board, who confirmed the information used and gathered during the budget development process. The estimated budget includes estimates for annual salary and benefits for new personnel, as well as operating expenses which include landline and cell phone service, travel, training and office supplies.

The security technology initiative budgets for FY15 were derived from estimates and assumptions with input from State personnel. Software, hardware, licenses, and maintenance costs are included as part of the technology budget. The Recommended Technology Solutions included in the budget are targeted toward enterprise level assets, 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

**Figure 2: State fiscal year 2015 budget estimate**

| | Activity | State FY 2015 Budget Estimate |
|---|---|---|
| Organization | • Enterprise Security Office | $3,336,400 |
| | • Enterprise Privacy Office | $440,200 |
| | • Awareness, Training and Talent | $1,124,000 |
| Technology | • Enterprise Technology | $15,987,366 |
| | | Grand Total: $20,887,966 |

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.

# 5 Conclusion and Next Steps

The implementation of a state-wide INFOSEC program is an evolutionary process which requires a long-term commitment of funding, and both legislative and executive leadership support. It is important to understand that the security assessments conducted, policies released and technology adopted to date, have not identified all State and agency security vulnerabilities and will not combat all threats. However, to date, the State has made progress towards the establishment of a statewide INFOSEC program. This report provides an overview of the progress made to date as well as the next steps in further refining and supporting the program. Deloitte & Touche has continued 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 out-year funding estimates.

The following timeline provides an overview of remaining activities within the scope of the INFOSEC program:

**Figure 3: INFOSEC program timeline**

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.

# 6 Appendices

## 6.1 Appendix A: Description of components of the roadmap

The figures included in this appendix show the three stages of the INFOSEC program roadmap, which include foundation, evolve, and leading in class stages. Current state for each of the domains is noted in section “4 Progress” within this report.

**Roadmap: Build foundation**

Figure 4 details the activities included in the foundation building phase of the INFOSEC program roadmap.

**Figure 4: Build foundation roadmap**

| | Function | Description |
|---|---|---|
| Organization | Governance | • Establish Organization: Finalize organizational structure and secure funding.<br>  • COO, CISO, and Deputy CISOs: Develop job descriptions and hire resources.<br>  • CPO: Develop job descriptions and hire resources.<br>  • 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.<br>• Training and Professional Development: Professional training for security and technical workforce at the state.<br>• Cyber Security State Workforce Development Program: Define career paths for state employees that work in information security, attract new talent, and minimize the rotation of personnel. |
| 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 schema. The schema forms the foundation for discovering and understanding the data agencies hold and defines the degree of protection required. |
| 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. |

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.

## Roadmap: Evolve

Figure 5 details the activities included in the evolve phase of the INFOSEC program roadmap.

### Figure 5: 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. |

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.

### Roadmap: Leading in class

Figure 6 details the activities included in the third phase of the INFOSEC program roadmap.

## Figure 6: 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. |
| Organization | Grow and Retain Talent | Implement talent recruitment and retention strategies including: total rewards, early talent, leadership development, succession planning and workplace customization. |
| Organization | 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. |
| Organization | 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). |
| Organization | 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. |
| Technology | 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. |
| Technology | 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. |

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.

## 6.2 Appendix B: Budget Summary

Figure 7 provides a summary overview of the budget estimates for the implementation of the information security strategies.

### Figure 7: Budget Summary

| | Activity | State FY2015 Budget Estimates | Future Recurring Budget Estimates |
|---|---|---|---|
| Organization | • **Enterprise Security Office** | | |
| | • COO Office | $210,500 | $210,500 |
| | • CISO Office | $203,500 | $203,500 |
| | • Planning and Strategy | $276,000 | $276,000 |
| | • Governance | $821,600 | $821,600 |
| | • Enterprise Security Technology | $1,139,300 | $1,139,300 |
| | • Cyber Incident Response | $458,000 | $458,000 |
| | • Security Training and Cyber Culture | $227,500 | $227,500 |
| | • **Enterprise Privacy Office** | $440,200 | $440,200 |
| | • **Awareness, Training and Talent** | | |
| | • End User Awareness and Training Program | $350,000 | $350,000 |
| | • Training and Professional Development | $504,000 | $504,000 |
| | • Annual Security Conference | $20,000 | $20,000 |
| | • Cyber Security State Workforce Development | $250,000 | $250,000 |
| Technology | • **Enterprise Technology and Remediation** | | |
| | • Foundational - Secure Network Engineering | $1,510,866 | $1,143,866 |
| | • Foundational - Data Protection | $970,000 | $470,000 |
| | • Foundational - Threat Monitoring and Control | $4,914,500 | $1,019,500 |
| | • Foundational - Continuous Vulnerability Assessment, and Remediation | $1,637,000 | $287,000 |
| | • Evolve - Agency Security Shared Services | $675,000 | $525,000 |
| | • Evolve - Continuity Vulnerability and Threat Management | $2,445,000 | $875,000 |
| | • Evolve - Expand Data Protection | $665,000 | $40,000 |
| | • Evolve - Identity and Access Management | $255,000 | $180,000 |
| | • Evolve – Cyber Threat Analytics and Intelligence | $2,915,000 | $2,665,000 |
| | | **20,887,966** | **12,105,966** |

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.