State of South Carolina Information Security Analysis

Initial Assessment Overview

May 8, 2013

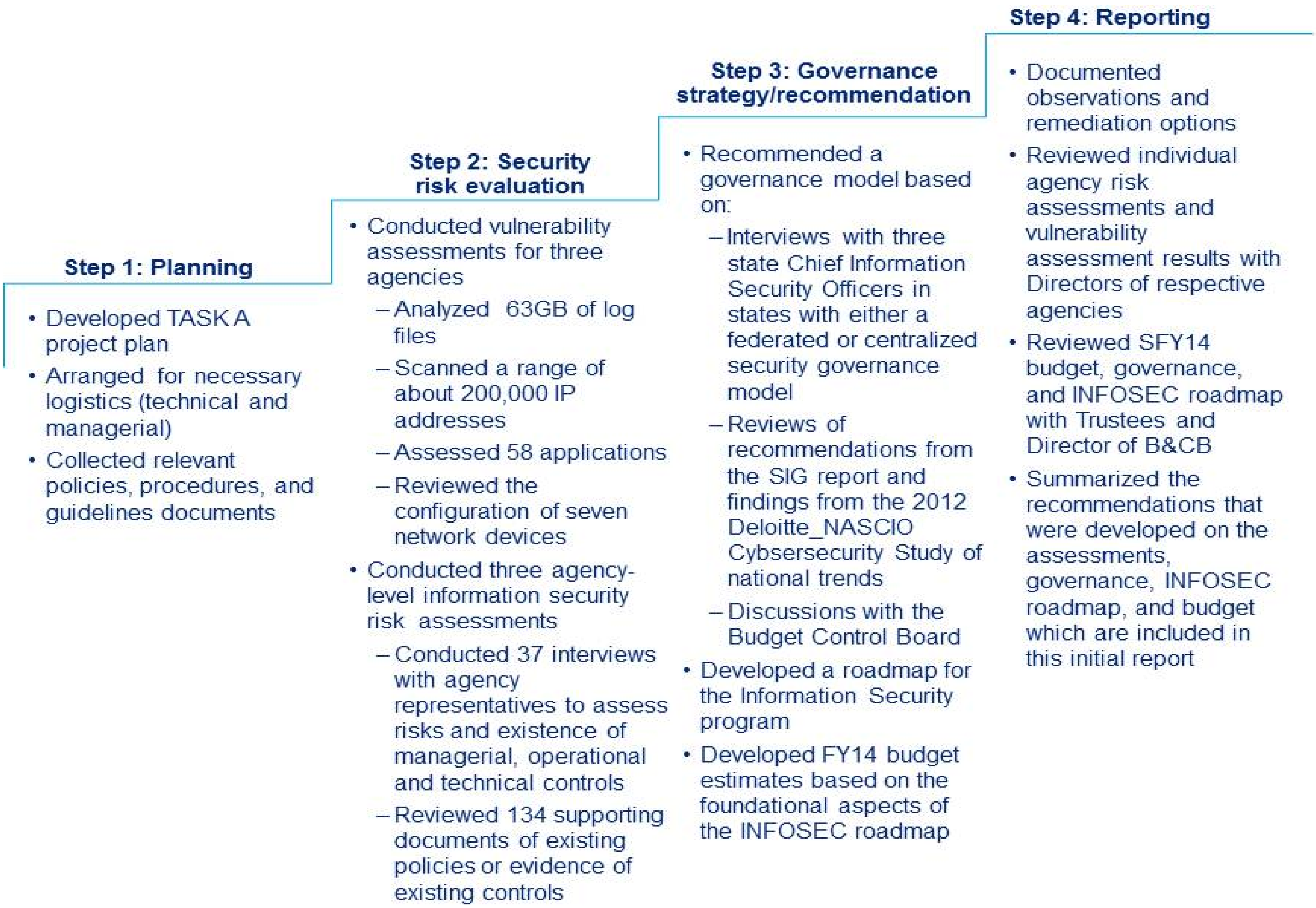
Our services were performed in accordance with the Statement on Standards for Consulting Services that is issued by the American Institute of Certified Public Accountants (AICPA). We provided to the State of South Carolina our observations and recommendations. However, our services did not constitute 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 governance presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Approach

Security Assessment Approach



Step 1: Planning

- Developed TASK A project plan
- Arranged for necessary logistics (technical and managerial)
- Collected relevant policies, procedures, and guidelines documents

Step 2: Security risk evaluation

- Conducted vulnerability assessments for three agencies
  - Analyzed 63GB of log files
  - Scanned a range of about 200,000 IP addresses
  - Assessed 58 applications
  - Reviewed the configuration of seven network devices
- Conducted three agency-level information security risk assessments
  - Conducted 37 interviews with agency representatives to assess risks and existence of managerial, operational and technical controls
  - Reviewed 134 supporting documents of existing policies or evidence of existing controls

Step 3: Governance strategy/recommendation

- Recommended a governance model based on:
  - Interviews with three state Chief Information Security Officers in states with either a federated or centralized security governance model
  - Reviews of recommendations from the SIG report and findings from the 2012 Deloitte_NASCIO Cybsersecurity Study of national trends
  - Discussions with the Budget Control Board
- Developed a roadmap for the Information Security program
- Developed FY14 budget estimates based on the foundational aspects of the INFOSEC roadmap

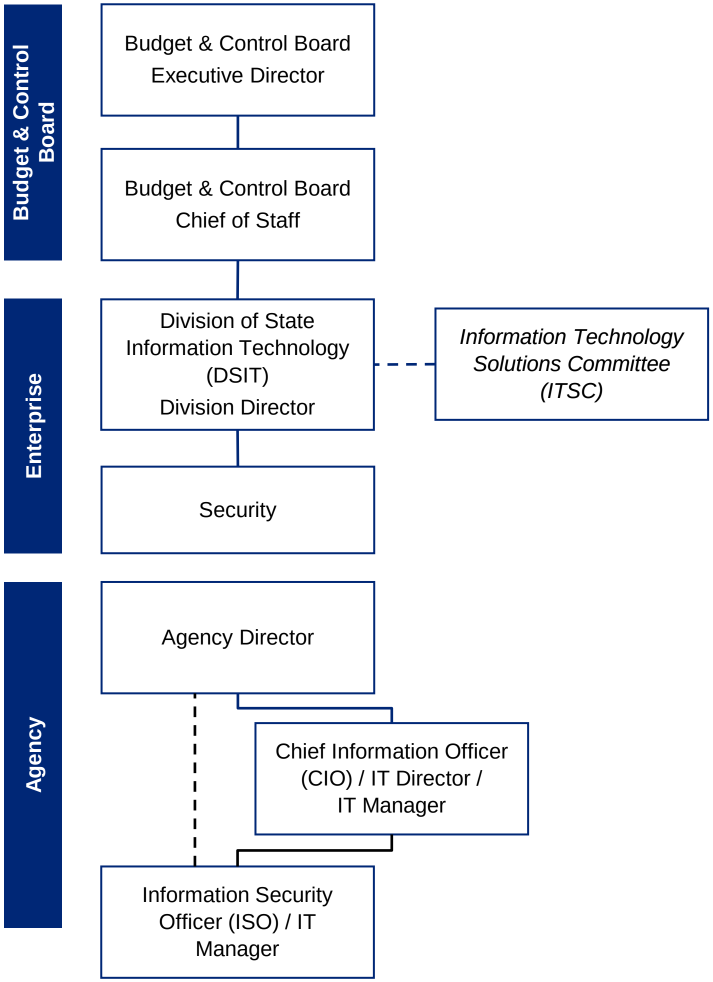
Step 4: Reporting

- Documented observations and remediation options
- Reviewed individual agency risk assessments and vulnerability assessment results with Directors of respective agencies
- Reviewed SFY14 budget, governance, and INFOSEC roadmap with Trustees and Director of B&CB
- Summarized the recommendations that were developed on the assessments, governance, INFOSEC roadmap, and budget which are included in this initial report

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

South Carolina's Decentralized Technology and Information Security Governance Structure Leads to Challenges…

Technology and Information Security Governance Structure


Budget & Control Board
Budget & Control Board Executive Director
Budget & Control Board Chief of Staff
Enterprise
Division of State Information Technology (DSIT) Division Director
Information Technology Solutions Committee (ITSC)
Security
Agency
Agency Director
Chief Information Officer (CIO) / IT Director / IT Manager
Information Security Officer (ISO) / IT Manager

Note: The ITSC is comprised of 13 members representing functional groups, 3 at-large members with knowledge in technology areas and the Deputy Division Director for Enterprise Projects at DSIT.

Note: The Security function performs continuous Information Security monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities.

Challenges

- South Carolina does not have standard statewide technology or Information Security policies. There is no state entity with the authority and responsibility to provide technology or security leadership, standards, policies, and oversight.
- Information Security procedures and protocols have been largely uncoordinated and outdated, exposing the State to greater risks of internal and external cyber-attacks on Information Technology (IT) infrastructure and data records. There are no standards against which agencies are measured, nor are there recurring processes to perform systematic risk assessments.
- Agencies are conducting mission critical Information Security activities but uneven staffing, skill, and experience does not leave room to be proactive in an environment of increasing vulnerability and threat. Lack of employee awareness training and a culture of complacency creates ongoing exposure.
- Agencies have a significant variety of software, hardware and information which increases the number of exposure points and leads to higher expenses, thus diverting money from underfunded areas such as Information Security staffing and training.
- Agencies have a degree of skepticism and distrust toward the Division of State Information Technology (DSIT) owing to a history of friction, primarily related to the cost of services provided. These historical trust issues impair DSIT's ability to "drive" any change initiatives.

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Assessment Recommendations

Approach to Determining an Appropriate Information Security Governance Model for the State

Reviewed:

Inspector General Report

Draft Legislation S.334

Governance Models in other States

2012 Deloitte-NASCIO Cybersecurity Study

Interviewed:

Chief Information Security Officers (CISOs) from Other States

Michigan

Minnesota

Pennsylvania

Conducted:

Workshops

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Foundational Elements of the Information Security Program

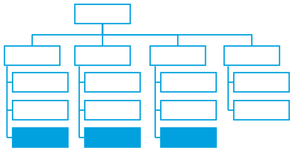
An effective information security program requires collaboration across the foundational functions

	Privacy	Information Security	Technology & Security Operations
Role	Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. A privacy function in government determines what data needs to be protected.	Information security is the practice of defending classified and protected information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.	The technology function provides and operates the technical infrastructure and security infrastructure in accordance with the policies defined by the Information Security function.

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Governance Models: Decentralized, Federated, Centralized

Decentralized Model



Agencies operate with full autonomy while attempting to maintain global standards in order to meet specific (but limited) enterprise requirements.

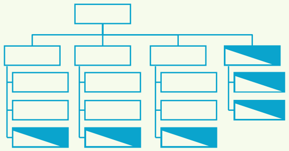
Benefits

- Flexibility for agencies to run their operations.
- Ability to respond efficiently to specific requirements.

Challenges

- Lack of common roles, responsibilities and information across the enterprise.
- Inconsistent definition and application of processes, standards and policies.
- Higher expenses due to redundancy of software, hardware and information.
- Highest risk due to many additional exposure points.

Federated Model



The enterprise sets strategy, develops frameworks and policies, facilitates communication and provides subject matter experience while agencies remain responsible for the implementation.

- ← Control → +

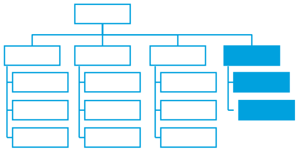
Benefits

- Enterprise sets strategy, policy and framework to reduce risk, support collaboration and develop centers of excellence.
- Representation from the agencies improves decision making.
- Lower incremental costs due to combination of existing and new resources.
- Agencies are responsible for their security, keeping control close to the source.

Challenges

- Slower decision making as ownership is distributed throughout the enterprise.
- Agencies may not prioritize security or may not be able to find people with the required skill sets.

Centralized Model



The enterprise provides a single point of control for decision making with agencies reporting directly to the central entity.

Benefits

- Enterprise establishes, controls, and enforces policies and standards.
- Improved oversight of Information Security within the organization.
- Increased speed of decision making due to single point of control and accountability.
- Greater degree of control over the creation and distribution of information.

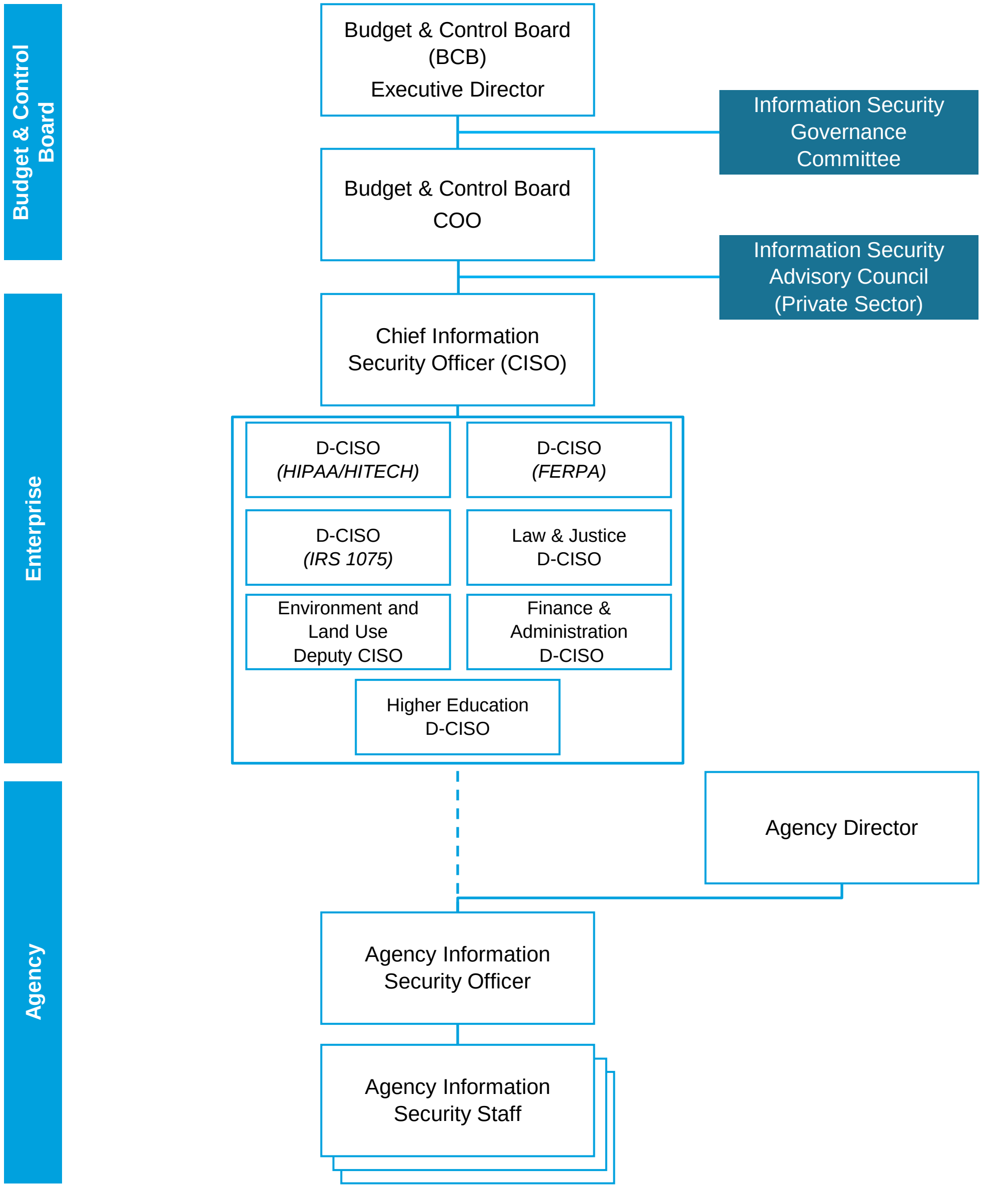
Challenges

- Difficult to implement effectively in a highly decentralized organization.
- Risk of poor decision making due to lack of agency representation.

■ Decision making
□ Proposed model

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Governance Model: Reporting of Security Functions



Budget & Control Board

Enterprise

Agency

Budget & Control Board (BCB) Executive Director

Information Security Governance Committee

Budget & Control Board COO

Information Security Advisory Council (Private Sector)

Chief Information Security Officer (CISO)

D-CISO *(HIPAA/HITECH)*

D-CISO *(FERPA)*

D-CISO *(IRS 1075)*

Law & Justice D-CISO

Environment and Land Use Deputy CISO

Finance & Administration D-CISO

Higher Education D-CISO

Agency Director

Agency Information Security Officer

Agency Information Security Staff

Description

- Consider establishing the role of **Chief Information Security Officer (CISO)** at the Enterprise level. This role would report administratively to the Chief of Staff of the Budget & Control Board.
- Consider establishing the role of seven **Deputy Chief Information Security Officers** roles at the Enterprise level. Each Deputy CISO would serve as a subject matter specialist in a certain field and as the primary point of contact for a State Agency for their respective field. These roles would report administratively to the Chief Information Security Officer.
- The Agency **Information Security Officers (ISO)** would report administratively to the Director of their Agency with the Deputy Chief Information Security Officer responsible for the Agency providing input on hiring and performance reviews. The Agency ISO would also have a secondary reporting relationship to the CISO.
- The Agency **Information Security Officers** are not required to be a full-time position and may also report to other positions like Agency CIOs and not directly to the Agency Director.

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Roadmap Recommendations

	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

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.

Fiscal Year 2014 Budgetary Estimate

	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	*Primarily accounted for by Task B activities*	
	Security risk assessments		
	Data classification		
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**

This presentation is intended solely for the information and internal use of the State of South Carolina, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this draft presentation.