State of Louisiana

Division of Administration

Information Security Program

CHARTER

Office of Technology Services

Date Published: 12, 09, 2015

Charter Contents

Executive Sponsors

State Chief Information Officer
Dep. State Chief Information Officer
Director of Human Capital Management
Asst. Commissioner of Administration – Facility Planning & Control
Asst. Commissioner of Administration – Management & Finance
Asst. Commissioner of Administration – Procurement
Division of Administration, General Counsel
Commissioner of Administration

Program Owner

Dustin Glover, Chief Information Security Officer

Introduction

This charter defines the Information Security Strategy, Purpose, Scope, and Components of the Information Security Program; and management roles and responsibilities, including the role of the Chief Information Security Officer (CISO) and the Information Security Team (IST).

Statewide Information Security Strategy

The State of Louisiana and its operational Agencies are entrusted with sensitive and confidential information including, but not limited to, Criminal Justice Information (CJI), Protected Health Information (PHI), Federal Tax Information (FTI), and Personally Identifiable Information (PII) and acknowledges the responsibility and steps required to protect that information. As such, the State has adopted an Information Security Strategy intended to align information security with operational strategy; to comply with applicable legal and regulatory requirements; to achieve industry standards; to manage, monitor, and mitigate information security risks and incidents; to optimize information security investments; to manage information security resources efficiently; and to monitor the ongoing effectiveness of the Information Security Program.

Information Security Program

Purpose and Scope

In order to implement the Information Security Strategy, the Division of Administration has developed and implemented an Information Security Program. The scope of the Program includes all people, processes, technologies, and environmental factors involved in the creation, use, destruction, storage, restoration, management, and governance of information and information assets. Additionally, the Program is designed to provide for the availability, integrity, authentication, confidentiality, and non-repudiation of information systems and information assets.

Program Components

Information Risk Management
Identify and manage information security risks and align Information Security Strategy with the operational needs of the State.

Information Security Program Development
Create and maintain a program to implement the Information Security Strategy.

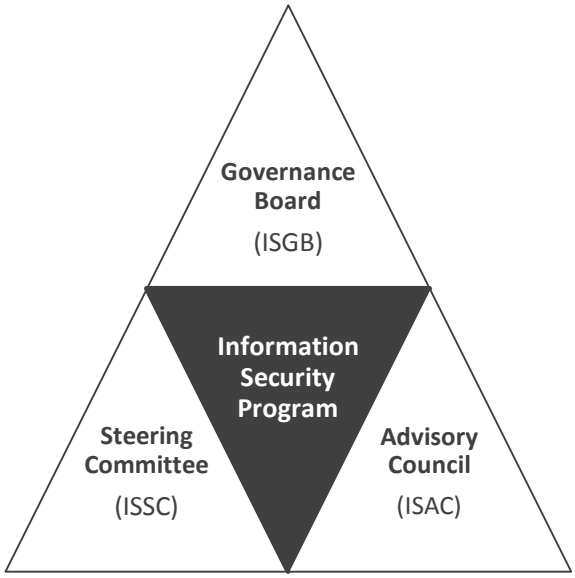
Information Security Program Management
Oversee, direct, and monitor information security activities to execute the Information Security Program.

Incident Management & Response
Plan, develop, and manage appropriate capabilities and measures to detect, respond to and recover from information security incidents.

Information Security Governance
Establish and maintain a governance structure to provide for accountability and assurance that the Information Security Strategy is aligned with the operational needs of the State and consistent with applicable law, regulations, and industry best practices.

Information Security Governance

Governance Structure



Roles and Responsibilities

Information Security Governance Board (ISGB)

The ISGB is responsible for confirming that the State:

- Aligns the Information Security Strategy with the State's operational strategies.
- Manages information security risks through appropriate risk tolerance levels and risk policies.
- Assigns priority for information security activities and investments.
- Requires reporting of security activity costs and security breaches.
- Monitors the effectiveness of security measures.
- Manages, assigns, and monitors resources utilization.
- Oversees security process integrations within the State.
- Monitor regulatory compliance.
- Oversees the incident management and reporting of security breaches.
- Confirms information security processes utilize and produce effective metrics.

Meetings: The ISGB meets quarterly.

Membership: The ISGB is comprised of members of the Division of Administration's Executive Staff and Agency Leadership. Additions and changes to the membership of the ISGB may be proposed and approved by the ISGB.

As of 09/01/2015 the ISGB Members:

1. State Chief Information Officer (ISGB Co-Chair)
2. Chief Information Security Officer (ISGB Co-Chair)
3. General Counsel
4. Assistant Commissioner – Procurement
5. Assistant Commissioner – Facility Planning and Control
6. Director, Office of State Human Capital Management
7. Director, Office of Planning and Budget
8. Agency Deputy Executive Director (3) (Alternating 2 year terms)

Information Security Steering Committee (ISSC)

The ISSC is responsible for assisting the ISGB and CISO with implementing and maintaining the Information Security Strategy and Information Security Program. The core functions of the ISSC include:

- Managing security strategy and integration efforts
- Operational support and service integration
- Assist with identifying emerging risks
- Promoting security practices
- Identifying compliance issues
- Reviewing and advising on the adequacy of security initiatives to service the operational needs of the State
- Assist with identifying of critical processes and assurance
- Directing Assurance integration efforts
- Require monitory and business case studies of security initiatives

Meetings: ISSC meets monthly.

Membership: The ISSC is comprised of members of the Division of Administration's Office of Technology Services (OTS) Executive Leadership Team. Additions and changes to the membership of the ISSC may be proposed and approved by the ISSC.

1. Deputy Chief Information Officer (ISSC Co-Chair)
2. Chief Information Security Officer (ISSC Co-Chair)
3. Chief Technology Officer
4. Chief Data Officer
5. Director of Data Center Operations
6. Director of Application and Data Management
7. Director of Network Services
8. Director of End User Computing
9. Director of Agency Relationship Management
10. Director of Project Management

Information Security Advisory Council (ISAC)

The ISAC is responsible for advising the CISO on any emerging information security risk(s) and statewide program effectiveness. The core functions of the ISSC include:

- Communicate identified, emerging, or potential information security risk(s)
- Identifying upcoming changes in federal or state regulatory or compliance related information security requirements
- Reviewing and advising on the adequacy of security initiatives to service the operational needs of the State
- Assist with identifying of critical processes
- Identify opportunities to address information security risk(s) with consistent, efficient, and standardized methods

Meetings: ISAC meets bi-annually or as needed.

Membership: The ISAC is comprised of subject matter experts from various state, federal, or local entities selected by the CISO or ISGB. Additions and changes to the membership of the ISAC may be proposed by any member of the ISAC, ISGB, or ISSC and approved by the CISO.

1. Chief Information Security Officer (ISAC Chair)
2. Information Security Team
3. Representative(s) from Out of Scope Agencies. (Higher Education, Enforcement Agencies, Etc.)

Chief Information Security Officer (CISO)

The CISO is responsible for the development, maintenance, and implementation of the Information Security Program. The CISO leads the Information Security Team (IST) and works with various State Offices, Agencies, assurance functions, and internal or external parties to implement, monitor, and execute the Program. The CISO is empowered and authorized to take appropriate steps and actions to successfully manage the Program and respond to security incidents while working closely with Legal, Compliance, and Human Resources Offices as appropriate.

The core responsibilities of the CISO are:

Governance

- Develop, in conjunction with the ISGB, the Information Security Strategy.
- Develop, oversee, implement, and maintain the Information Security Program and related initiatives.
- Align, in conjunction with the ISGB, the Information Security Strategy with the operational strategy of the State.
- Liaise with agency leadership and process owners to support ongoing alignment and verify risk and operational impact assessments are conducted and that risk mitigation strategies are being implemented.
- Assist in identifying current and potential legislation and regulatory requirements affecting information security.
- Monitor utilization and effectiveness of information security resources by developing and implementing monitoring and metrics.
- Direct and monitor information security activities.
- Liaise with other assurance providers (e.g., Internal Audit, Louisiana Legislative Audit, External Auditors, Compliance Counsel, Privacy Officer, etc.) regarding information security.
- Provide assurance for proper response and reporting of information security incidents.
- Define information security roles and responsibilities throughout the State.
- Working with ISGB, establish reporting and communication needed to support the Information Security Program.

Information Risk Management

- Establish and maintain processes for information asset classification and ownership.
- Implement a systematic and structured information risk assessment process.
- Confirm operational impact assessments are conducted periodically.
- Verify threat and vulnerability evaluations are performed on an ongoing basis.
- Identify and periodically evaluate information security controls and countermeasures for mitigation of risk to acceptable levels.
- Integrate risk, threat, and vulnerability management into operational life cycle processes (e.g., project management, development, procurement, and employment life cycles).
- Report significant changes in information security risk to appropriate levels of management on both periodic and event-driven basis.

Information Security Program Development and Management

- Develop, maintain, and manage plans to implement the Information Security Strategy while providing clear visibility to the specific activities being performed within the Information Security Program.
- Establish, communicate, and maintain information security policies, and verify that processes and procedures are performed in a compliant manner.
- Confirm the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
- Develop the information security resources, including people, processes, and technology.
- When applicable, working with the CIO and Dep. CIO, identify and manage internal and external resources (e.g., finances, people, equipment, systems) required for the execution of the program.
- Develop processes to ensure applicable contracts and agreements contain the necessary information security controls (e.g., outsourced providers, residents, third parties).
- Identify opportunities to integrate information security requirements within the State's operational processes and life cycle activities.
- Provide Information Security advice and guidance (e.g., risk and analysis, control options) to the State.
- Ensure alignment between the Information Security Program and other assurance functions.
- Design, develop, and manage processes to provide information security awareness, training, and education to the appropriate audiences.(e.g., process owners, users, OTS resources).
- Define and establish metrics to evaluate the effectiveness of the Information Security Program
- Verify any Information Security Program compliance issue or other variance is resolved in a timely manner.
- Monitor, measure, validate, and report on the effectiveness and efficiency of information security controls and program compliance.

Incident Management and Response

- Develop and implement processes to prevent, detect, respond, and recover from information security incidents.
- Establish clear escalation and communication processes including lines of authority during incident response.
- Develop and maintain incident response plans to ensure timely response, reporting, and remediation.
- Establish the capability to investigate and analyze information security incidents in order to determine root cause (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process in accordance with Incident Management & Response Policy to communicate with internal parties and external organizations (e.g., media, law enforcement, residents).
- Integrate information security incident response plans with the State's disaster recovery and operational continuity plans.
- Periodically test and refine information security incident response plans.
- Manage the response to information security incidents.
- As needed, conduct reviews of systems, applications, networks, or processes related to previous information security incidents to ensure remediation actions are working as designed.
- Develop corrective actions, reassess risk, and establish monitoring mechanisms as needed.

Information Security Team (IST)

The IST is comprised of specifically selected OTS resources at various operational levels with the primary responsibility of performing operational information security functions. Lead by the CISO, the IST works with applicable OTS and Agency resources to develop, implement, communicate, and apply the Information Security Policy to State Systems and Data. As needed the IST is authorized to add, modify, or remove safeguards and controls to improve the information security posture of the State.

The core responsibilities of the IST are:

- Provide guidance, support, direction, and authority for all information security activities for the State in accordance with and in support of the Information Security Program.
- Employ a series of layered technical and non-technical safeguards and controls leveraging manual or automated processes and procedures in order to protect the State's information and information assets.
- Enforce the information security policy and provide direction for all information security activities for the State in accordance with and in support of the Information Security Program.
- Engage and work with various State agencies, offices, assurance functions, and internal and external parties as needed for managing the program.
- Take appropriate steps and actions for managing and responding to information security incidents, policy violations, forensics and investigations, internal or external exploits, threats and vulnerabilities.
- Provide management direction in line with operational goals and objectives and relevant law and regulations, demonstrate support for, and commitment to information through the maintenance and implementation of the Information Security Policy across the State.

Additionally, in accordance with the Information Security Program and Policy, the IST will implement, manage, validate, and monitor relevant information security controls for:

- Identity and Access Management
- Information Security Risk Management
- Incident Management
- Data Center Security
- Network Communications and Device Security
- Configuration Management
- Data Sanitization
- Vulnerability Management
- Audit Logging and Event Monitoring
- Information Asset Management
- Information Security Training and Awareness
- Data Protection and Encryption Requirements

Information Security Officer (ISO)
The CISO will assign specific members of the IST to serve as an ISO. An ISO will assist in leading Information Security Program initiatives related to specific regulatory environments. An ISO will also function as a dedicated resource for agencies to assist with planning, audits, incident response, data protection, disclosure, notifications, and ensure regulatory requirements are implemented in a verifiable manner.

Minimally, an individual ISO shall be assigned for the following Restricted Data types:

- Federal Tax Information (FTI)
- Protected Health Information (PHI)
- Criminal Justice Information (CJI)

Changes and Amendments

Changes and Amendments to this Charter may be proposed by any member of the ISGB.
The ISGB will review and approve the proposed changes or amendments.

Approval

By signing below, you are indicating your approval of the Information Security Program effective 12/09/2015

Program Owner	Signature	Date
Dustin Glover, CISO		12/4/2015

Executive Sponsor	Signature	Date
Richard "Dickie" Howze, *CIO*		12/7/15
Neal Underwood, *Dep. CIO / OTS COO*		12/7/2015
Ron Jackson, *OSHCM, Director*		12-9-2015
Jan Cassidy, *Asst. Commissioner*		12/8/2015
Scott Johnson, *General Counsel*		12/7/2015
Stafford Palmieri, *Commissioner of Administration*		12/7/2015

Document Revision Log

Name	Date	Action
Dustin Glover, *CISO*	05/01/2015	• Created Draft
Dustin Glover, *CISO*	08/03/2015	• Finalized Draft
Dustin Glover, CISO	10/21/2015	• Updated with initial OGC recommendations
Dustin Glover, CISO	12/04/2015	• Updated Executive Sponsors based on leadership change.