Strategic Plan for Enterprise Security and Risk Management

Overview:

This strategic plan sets the goals and objectives of the state in the operation of its business systems related to the protection of the state's information. Today, many of the State's most critical business systems are automated. Therefore it is important to translate the business needs of the state into a strategic technology plan that details how information technology (IT) contributes to achieving the goals of providing secure and sustainable services to citizens. This plan supports the State CIO's strategic planning initiatives including, IT consolidation, Western Data Center, IT asset management, shared services, operational excellence, enterprise program management structure, unified governmental email system, IT service privatization, and state portal enhancement. The means to achieving the level of information protection driven by the business needs is supported by policies, standards, procedures (PSPs) and the technical architecture. The PSPs are the rules for operating and protecting the information. The technical architecture is the technology that is used to implement the strategic plan. Information security, risk management, compliance and business continuity measures need to be woven into the fabric of IT operations.

Listed below are the strategic Enterprise Security and Risk Management Office goals:

1. Manage risk to improve agency security posture through consolidation of IT infrastructure.
2. Support continuity of IT operations by utilizing the Eastern Data Center (EDC) and the Western Data Center (WDC) and improving business continuity planning.
3. Improve security processes by incorporating Information Technology Infrastructure Library (ITIL) process methodologies into security operations.
4. Enhance cyber incident response capabilities by expanding preventive activities, forensic services and cyber incident planning.
5. Protect the confidentiality, integrity and availability of the State's IT information by defining and implementing a consistent approach that meets legal and regulatory requirements relating to confidential and/or personal information (PI).
6. Support efforts to simplify and standardize identity management for state employees, vendors and citizens.
7. Provide State agencies with a security framework and guidance by enhancing the State Information Security Manual.

These goals are implemented in part through the deployment of information technology. Below each strategic goal is supported by the tactical approach to achieve that goal. In order to achieve these goals in an effective and efficient manner one or more initiatives may need to be defined to select and optimally deploy information security solutions.

Strategic Goal
#1. Manage risk to improve agency security posture through consolidation of IT infrastructure

Summary:

The State has a responsibility to develop, deploy, and manage business systems that contain the appropriate security controls to protect citizen information in an effective and efficient manner. Security controls need to be included in all aspects of the systems development and operational life cycle, including planning for system retirement. Agency business systems benefit from using a robust infrastructure with a layered approach to security controls, monitoring, metrics and reporting. As a system is put into operation the system security controls need to be monitored and tracked to ensure that they do not become obsolete or inadequate due to changing requirements.

Implementation Approach

- Reduce agency responsibility for operating and securing infrastructure
- Review agency automated business systems to ensure that they include adequate and appropriate risk management, security and business continuity mechanisms.
- Implement a risk based approach to secure enterprise hosting environment that includes security and audit controls.

Strategic Plan for Enterprise Security and Risk Management

- Encourage and support agency efforts for securing their applications.
- Support a risk based approach to the deployment and operation of infrastructure security controls (risk assessment and framework placement, patch and vulnerability management, incident response, etc.)
- Assess, monitor and report on the effectiveness of security controls.
- Integrate agency consolidated operations with ITS and statewide cyber incident response plans.

Strategic Goal
#2. Support continuity of IT operations by utilizing the Eastern Data Center (EDC) and the Western Data Center (WDC) and improving business continuity planning

Summary:
NC General Statute 147-33.89, Executive Order 102, and Executive Order 118 require agencies to document business continuity plans and prepare for disaster recovery from adverse events. H.B. 2436 sec. 6.10 a, b, c, d requires state agencies to identify and provide adequate backup for critical systems. The State CIO supports agency efforts to recover IT business services. The consolidation of agency IT services also requires a consolidated view of business continuity and disaster recovery needs across agencies. In order to help agencies recover and sustain IT operations under adverse circumstances a western data center was built. The need to have a consolidated view of agency plans is even more important due to the creation of the western data center. With the western data center operational, agencies need to revise their business continuity and disaster recovery plans in order to efficiently and effectively use the both data centers.

Implementation Approach
- Define and deploy a standardized consistent approach for using the features and functions of the business continuity planning (BCP) tools to provide both agency and enterprise views to support consolidation of recovery services.
- Train and support agencies on business continuity management including the features and functions of the standardized BCP tool set.
- Support agency use of Business Impact Analysis (BIA) to identify their risks and requirements for using both the eastern and western data centers.
- Support agency use of the Living Disaster Recovery Planning Software (LDRPS) to incorporate both the eastern and the western data center into their business continuity and disaster recovery plans in an effective and efficient manner.
- Assess, review and analyze revised agency IT business continuity plans.
- Prepare statewide reports on critical backup and recovery of systems.

Strategic Goal
#3. Improve security and risk management processes by incorporating Information Technology Infrastructure Library (ITIL) process methodologies into security operations

Summary:
The State has a responsibility to maintain the operational availability, confidentiality, and integrity of information processed by systems. ITIL, the *de facto standard* used in the IT industry encompasses the foundation for IT Service Management (ITSM). ITIL is a transformative process built on best practices or recommendations that implement a shift from a strict focus on technology to a focus on delivering highly available services. Spanning the entire ITIL framework are the essential security, risk and business continuity controls necessary to ensure availability of services while protecting citizen and employee information in an effective and efficient manner. ITS business systems benefit from using a standardized methodology that has imbedded within its core functionality a layered approach to security controls, monitoring, metrics and reporting.

Strategic Plan for Enterprise Security and Risk Management

Implementation Approach

- Provide detailed, ongoing support by participating in teams developing, implementing and managing the elements of Service Support and Service Delivery.
- Participate in the development and implementation of availability management processes and procedures to support a consistent approach to risk and business continuity management
- Convert the internal security processes to an ITIL framework based on regulatory requirements, State standards and policies, best practices and practical experience in operating security in a State agency.
- Apply the six security measures as defined within the ITIL framework – preventative, detection, reductive, repressive, and corrective and evaluation – to implementation and daily operations.
- Monitor Critical Success Factors (CSFs) with developed Key Performance Indicators (KPIs) to achieve and maintain confidentiality, integrity and availability values.
- Ensure Operational Level Agreements (OLAs) and Service Level Agreements (SLAs) are defined, negotiated and maintained to support key security, risk management and compliance services.
- Define and implement evaluation processes to verify compliance, to respond to inappropriate use and to measure the effectiveness of security, risk and business continuity measures.

Strategic Goal

#4. Enhance cyber incident response capabilities by expanding preventive activities, forensic services and cyber incident planning

Summary:

The state has a responsibility to take a proactive approach to preventing cyber security incidents as well as a responsibility to effectively respond to cyber security incidents. The ability to disseminate timely warnings to constituent agencies and other ITS customers is paramount in this effort. Providing a centralized source for this information ensures consistency and eliminates the need for duplicated efforts across state government. When a cyber security incident occurs or misuse of state network and computer resources takes place, the ability to investigate the root cause and collect evidence is an essential part of cyber security incident response. In many cases the collection and preservation of evidence is necessary to meet legal and regulatory requirements and/or agency policy. Using a dedicated forensics lab with qualified staff to provide this service ensures the state is following standard evidence collection practices. The evidence gathered in this manner may be used in various legal proceedings or released to the appropriate law enforcement authorities without a subsequent need for the evidence to be re-processed.

Implementation Approach

- Maintain up to date cyber incident management plan.
- Review agency incident management plans.
- Serve as State of North Carolina representative to the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Encourage state, local, and university participation in NC-ISAC and MS-ISAC activities
- Provide timely updates on new cyber security threats through e-mail notifications, security web portal, and other means as required to protect the state's network and computer resources.
- Integrate NC-ISAC Security Web Portal with statewide MC-ISAC and dedicated US-CERT portal for North Carolina.
- Support statewide business continuity planning for information security.
- Provide yearly incident management training to constituent agencies and customers.
- Provide computer forensic services to state agencies.
- Maintain a database of cyber security incidents.
- Provide statistical information and monthly reports to ITS management, the State Auditor and North Carolina Attorney General.
- Provide security advisory services to agencies.

Strategic Plan for Enterprise Security and Risk Management

- Test the state's capabilities to prepare for, protect from, and respond to the effects of cyber attacks by participating in the Department of Homeland Security (DHS) national cyber exercises and other testing activities.

Strategic Goal
#5. Protect the confidentiality, integrity and availability of the State's information by defining and implementing a consistent approach that meets legal and regulatory requirements relating to confidential and/or personal information (PI)

Summary:

There are many legal and regulatory requirements for handling information that is classified by law as confidential and/or personal information, (PI). Security breaches involving such data often contain requirements for disclosure and/or penalties. Effective October 1, 2006 state agencies must disclose security breaches when PI is involved. Executive branch agencies must report security breaches to the Enterprise Security and Risk Management Office. It is important that agencies understand and are prepared to meet these requirements.

Implementation Approach

- Support agency use of encryption technologies and other security tools.
- Incorporate PI requirements into the statewide cyber incident plan.
- Raise agency awareness through training.
- Identify critical systems with confidential/PI data and update the incident management plan
- Define and apply consistent communications protocols for confidential/PI data.
- Remind agencies when reporting a cyber incident that they need to take appropriate actions if confidential/PI data is involved.
- Encourage state and local government agencies to provide mobile data encryption by using the statewide contract for mobile data encryption products and related services

Strategic Goal
#6. Support efforts to simplify and standardize identity management for state employees, vendors and citizens

Summary:

The state must consistently identify who has access to state IT resources, authentication, and what they can do once they have such access, authorization. Strong identity management mechanisms are a foundational element of risk management and information security. Legal and regulatory requirements increasingly require strong forms of identity management. Users of identity management systems need to a have a consistent means of interfacing with state resources through simplified sign on processes that minimizes user confusion while simultaneously enforcing the application of strong and consistent policies and procedures. User access needs to be defined based on their roles in the business process. The business of the state must expand from state employees to service citizens and vendors for critical business functions that require strong identification and authorization.

Implementation Approach

- Support an enterprise approach to identity management though the NCID service offering.
- Define and update state and ITS agency PSPs related to identity management.
- Support efforts to integrate various platforms with enterprise identity management service offerings, including but not limited to badge systems, RACF, wireless networks, etc.
- Support implementation of dual factor authentication (begin with systems and database administrators) by integrating use of certificates, tokens, smartcards, biometrics, etc.
- Support state efforts to understand and comply with federal requirements.

Strategic Plan for Enterprise Security and Risk Management

- Monitor and report on compliance with legal and regulatory requirements.
- Review agency project plans for appropriate identity management approach.
- Engage the Technology Planning Group (TPG) and agency staff in the identity management process.

Strategic Goal
#7. Provide State agencies with a security framework and guidance by enhancing the State Information Security Manual

Summary:

The State continues to build and maintain the State Policy, Standards and Procedures (PSPs) framework to ensure that all agencies have a common baseline of PSP's within the ISO27002/NIST standards framework. PSP's are created and/or updated as needed. Agencies need help in identifying gaps and tailoring their agency policies within the State framework to meet their own unique requirements. In this way the State can ensure that all agencies have a common baseline of PSP's integrated with the state level framework. The ISO27002 standard is internationally recognized and is used by the National Institute of Standards (NIST) and others. The State CIO has adopted and follows a standards/policy review and rollout process to make the latest statewide manual available to agencies. As new and/or revised policies are approved, they are rolled out to all executive branch agencies with appropriate training materials provided. All approved security policies and standards that are not classified by law as 'confidential' are posted in the Statewide Information Security Manual which is on the State CIO's web site. As part of the annual review of security standards required under GS 147.33.110, the ESRMO reviews the statewide security standards, industry standards and best practices and seeks suggestions from agencies subject to the standards.

Implementation Approach

- Provide for regular updates to the security manual content for security, risk management, business continuity planning, including new policies for new technologies such as cloud computing and social media.
- Train agencies on state security manual.
- Engage the agency staff in the security manual review process.
- Perform security standards gap analysis.
- Follow process established by the State CIO related to enterprise standards.
- Assess agency PSP compliance, monitor and track deviations.
- Encourage agencies to complete complimentary agency level PSPs.