

State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agency

IT Risk Strategy



June 2014

Agenda

- Questions & Follow-Up
- Policy Workshop Overview & Timeline
- Policy Overview: IT Risk Strategy Policy
- Risk Assessment Framework & IT Risk Strategy Policy
- Deliverable Template Tips
- Next Steps

Questions & Follow-Up

Policy Workshop Q&As

The following questions were raised during the **Business Continuity Management (BCM)** policy workshop for **All Agencies**:

Question #1 – What is the DIS implementation date established for compliance for the 13 State policies?

Answer #1 – As presented during the Agency and IT Director meetings on June 4, the date established for compliance for each of the 13 policies is the following: **July 1, 2016**.

DIS Deliverable Dates:

The following dates were established by DIS for compliance with the 13 State policies:

June 30, 2014 – Roles & Responsibilities Chart

January 31, 2015 – Policy Implementation Plan of Actions (all 13 policies)

July 1, 2016 – End compliance date



**DIVISION OF
INFORMATION SECURITY**

Policy Workshops Overview & Timeline

Policy Workshop: Timeline

Objective: Conduct bi-weekly policy workshops with selected agencies to review information security policies, address implementation challenges, risks and assist on gap analysis and action plans with the Agency-designated policy champions.

March	April	May	June	July	August
Policy:	Policies:	Policies:	Policies:	Policies:	Policy:
❖ Asset Management	❖ Data Protection & Privacy ❖ Access Control	❖ Information System Acquisition, Development, Maintenance ❖ Threat and Vulnerability Management	❖ Business Continuity Management ❖ IT Risk Strategy	❖ Mobile Security ❖ HR & Security Awareness	❖ Physical & Environmental Security

Activities

- Facilitate bi-weekly Agency group workshops
- Review statewide policies
- Address key policy implementation challenges
- Conduct mini-gap analysis
- Discuss policy implementation plans

Agencies TO DOs

- Review Statewide policies and conduct mini-gap analysis
- Actively participate in breakout groups to discuss gaps and implementation challenges
- Identify remediation strategies and policy implementation plans

Policy Overview: IT Risk Strategy Policy

IT Risk Strategy: Key Requirements

Security Performance and Metrics

Information Security Metrics

- Agency shall develop, monitor and report progress on performance metrics for the following:
 - Adoption of security controls
 - Adoption of policies/procedures
 - Effectiveness of information security program
- Agency shall define performance measures to be able to support the determination of:
 - Information system security posture,
 - Demonstrate compliance with requirements
 - Identify areas of improvement.



IT Risk Strategy: **Key Requirements**

Security Performance and Metrics

Measurability of Metrics

- Metrics and/or measures collected shall be:
 - Meaningful (*S.M.A.R.T metrics*)
 - Yield impact and outcome findings
 - Provide stakeholders with the time necessary to use the results to address performance gaps

Data Management Concerns

- Agency shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

IT Risk Strategy: S.M.A.R.T. Metrics



IT Risk Strategy: **Key Requirements**

Third Party Risk Management

External Information System Services

- Agency shall direct third parties to comply with information systems requirements and employ defined security controls in accordance with applicable federal laws, regulations, directives, etc.(e.g., NIST and other State requirements such as DIS information security policies)
- Agency shall implement processes to monitor security controls compliance by third parties on an ongoing/periodic basis.

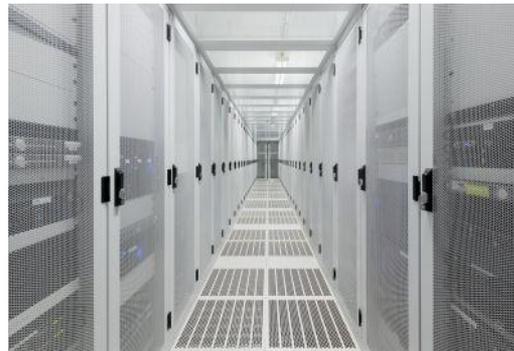
Risk Assessment

- Agency shall establish a process to conduct risk assessments on third party service providers and document the results.
- Agency shall update the risk assessments in the event of major changes in scope of services or contractual changes

IT Risk Strategy: Key Requirements

Third Party Risk Management *System Interconnections*

- Agency shall allow (data) exchange from its (internal) information systems to third party information systems by establishing Interconnection Security Agreements.
- Agency shall document third party interfaces detailing:
 - Interface characteristics (e.g., type of data input and output)
 - Security requirements (e.g., VPN connection requirement, HTTP Secure)
 - The nature of the information communicated (e.g., PHI/ PII, HIPAA, etc.).



IT Risk Strategy: **Key Requirements**

Third Party Risk Management

Use of External Information Systems

- Agency shall establish terms and conditions for Service Level Agreements (SLAs) with third parties owning, operating, and/ or maintaining external information systems, including:
 - Controls to access information systems from third party information systems;
 - Controls for processing, storing, or transmitting of data using third party information systems.

IT Risk Strategy: Key Requirements

Third Party Risk Management

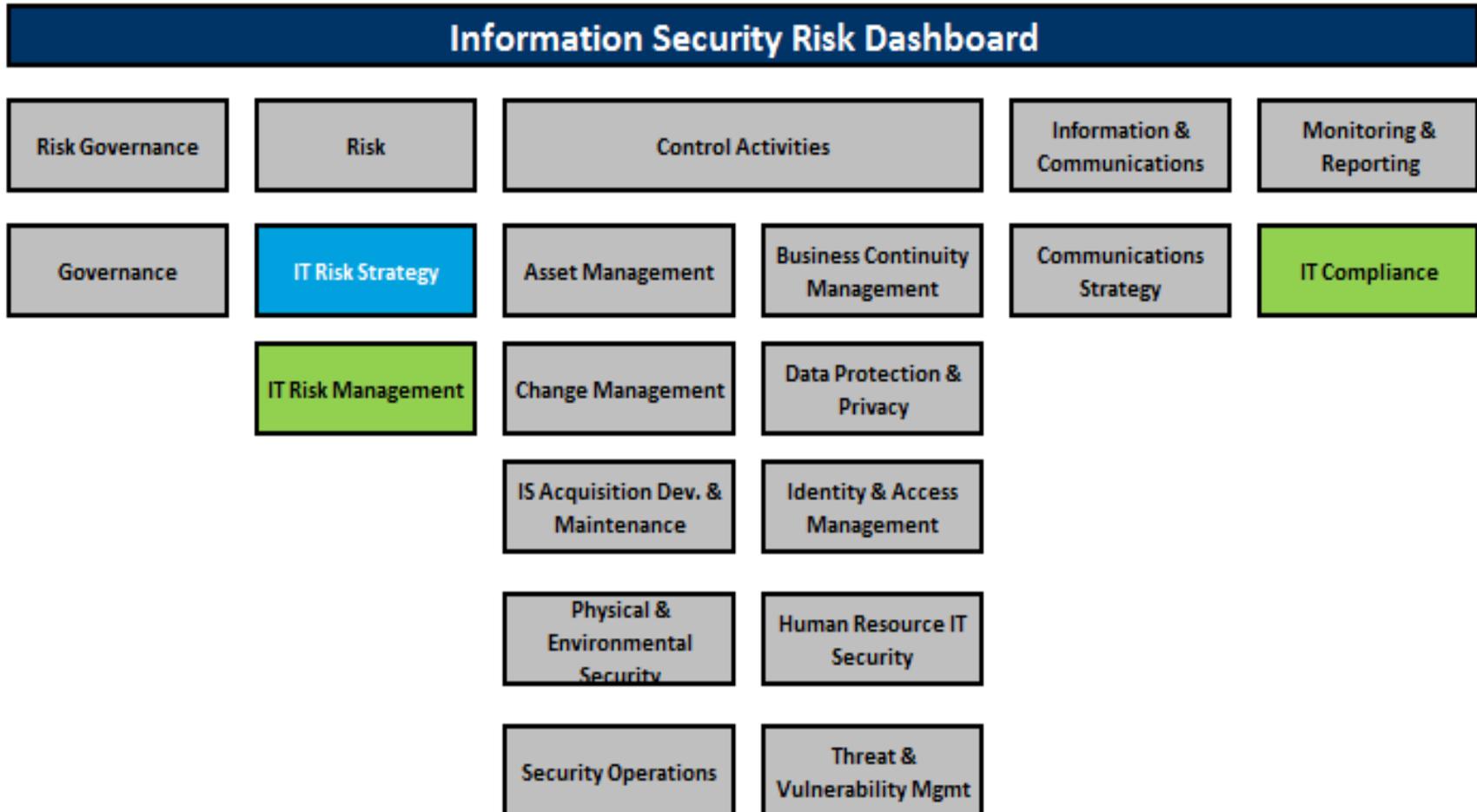
Information Sharing with Third Parties

- Agency shall share personally identifiable information (PIIs) with third parties only for authorized purposes as mandated in the established SLAs (or Interconnection Security Agreement)
- Agency shall establish the required SLAs (or equivalent agreement) and develop ground rules for the sharing of data with third parties.
- Agency shall inspect and evaluate proposed new instances of sharing sensitive data to assess if the sharing is authorized or whether additional public notice is required within the Agency

Risk Assessment Framework & IT Risk Strategy Policy

Risk Assessment Framework

The Risk Assessment Framework, based on the National Institute of Standards and Technology (NIST 800-53), was used as the basis to assess risk across the State Agencies using the fifteen (15) security domains (noted below):



IT Risk Strategy Policy: Risks & Remediation Strategies

Risk assessments conducted with State Agencies uncovered a number of risks in environments with inadequately implemented Access Control Policy and procedures. Remediation strategies were created to help Agencies address gaps and implement necessary safeguards.

Examples

Overall Risks	Identified Gaps	Remediation Strategies
<ul style="list-style-type: none"> • Unmanaged third party access • Lack of protection to confidential or restricted Agency data • Unclear metrics that lead to improper Agency decisions 	An agency-wide information security strategy does not exist.	Develop an IT Risk strategy for the Agency
	An agency-wide enterprise risk assessment framework has not been established	Establish an enterprise risk assessment framework
	Many agencies have not documented enterprise architecture design	Agencies are required to document the enterprise architecture design
	Third parties are not risk-ranked (e.g., transaction volume, data type, and contract length, etc.)	Define relative risks with third parties (e.g., risk ranking, transaction volume, data type and contract

IT Risk Strategy Policy : Challenges & Remediation Strategies for All Agencies

Examples	
Sample Challenges	Potential Solutions
Developing and establishing meaningful metrics	<ul style="list-style-type: none"> • Understand the current environment and what raw data is readily available for metrics • Use the S.M.A.R.T methodology to develop meaningful metrics • Identify to whom the metrics established will be shared and reported • Determine how the metrics can drive change, remediation efforts and/or training requirements within the Agency
Knowing what Agency data is being shared with third-parties	<ul style="list-style-type: none"> • Use and complete the data inventory tool to help identify the data that being externally communicated to third parties • Review existing SLA (or ISA) agreements with third parties • Align missing State requirements to the existing SLA (or ISA) or establish new agreements with third parties to ensure data is protected

IT Risk Strategy Policy : Challenges & Remediation

Strategies for All Agencies

Examples	
Sample Challenges	Potential Solutions
Controlling third party vendors in your IT environments	<ul style="list-style-type: none">• Establish clauses and acceptable use policies for the use of Agency data/assets by vendors into the third party contract (SLA)• Govern the level of control for the vendor/contractor access point (such as restricting use to specific locations, utilizing VPN, etc.)• Examine and oversee that vendor devices are patched and have antivirus to better protect the Agency data.• Control vendor access to information systems and make sure they are strictly regulated (e.g. to specific servers or subnet as opposed generic access or through the use of VDIs [Virtual Desktop Infrastructure])

Deliverable Template Tips

Gap Analysis: Tips & Guidance

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
InfoSec Policy has been reviewed and approved	Has the InfoSec Policy been reviewed and			

- Be DETAILED!!
- Consider using *'Partial'* to answer questions
- The *'Comments'* column should be used to document current environment and notes
- For identifying and finalizing gaps:
 - Consider both **process** and **documentation** gaps separately (and document both types)
 - Gaps should be detailed enough to read and understand independently when transferred to the implementation plans
 - You can have multiple gaps per question
- Consider using Gap Analyses as a process improvement exercise as well
- The Gap Analyses are meant to be filled out once as a point in time exercise
- Not all gaps will be identified with a 'No' response

Policy Implementation Plan of Action: Tips & Guidance

Action Plan						
Related Policy Clause	Current Gaps	Implementation Challenges	Implementation Strategy	Lead	Status	Due Date
SAMPLE ENTRY 1.1	SAMPLE ENTRY Asset inventory is not updated	SAMPLE ENTRY Process has not been	SAMPLE ENTRY <ul style="list-style-type: none"> Define process for 	SAMPLE ENTRY John Doe	SAMPLE ENTRY IP	SAMPLE ENTRY 3/30/2014

- Implementation Plans are meant to be living, breathing documents (even through the July 1, 2016 implementation date).
- Copy finalized gaps from Gap Analyses directly to ‘*Current Gaps*’ column
- Consider using long, medium and short-term implementation strategies
- There should be multiple, detailed bullets once an implementation strategy is finalized.
- Recommendations:
 - *Documentation* gaps should be separated (different lines) from *process* gaps.
 - Merge rows (where applicable) or transfer implementation plan to Excel
 - Identify unique ‘*due dates*’ for each bullet of the strategy
- A sample, short-term strategy could be as simple as ‘Waiting for State solution for Patch Management’ (your detailed strategy to close the gap would be identified after the DIS/DTO has announced the available solution).

Next Steps

Next Steps

1. Develop or update Agency's InfoSec policies to align with published State policies
2. Conduct Policy Gap Analysis
3. Develop Policy Implementation Plan of Action
4. Develop processes to enable the implementation of InfoSec Policies
5. Promote Agency-wide InfoSec policies awareness
6. Coordinate with DIS on training and guidance