State of South Carolina – Policy Guidance and Training

Policy Workshop

Data Protection and Privacy Policy

April 2014

Agenda

- Questions & Follow-Up
- Policy Workshop Overview & Timeline
- Policy Overview: Data Protection and Privacy Policy
- Risk Assessment Framework & Data Protection and Policy
- Next Steps

Questions & Follow-Up

Questions Raised: Guidance

The following questions were raised during the previous policy workshop for the Large Agency Group:

Question #1: Do the Agencies need to develop new policies (if those are lacking in their environment) or make sure that relevant processes are documented and in alignment with State InfoSec policies?
Answer #1: Agencies may choose any method which documents and implements secure processes that align with DIS Policies. This should include the review of current process documentation for inclusion of security provisions, and potentially creation of additional process documentation where secure processes are not otherwise described. Replication of the entire DIS Policy framework at the agency level is not required.

Questions Raised: Guidance

The following questions were raised during the previous policy workshop for Medium Agency Group:

Question #1: Agencies are not getting clear guidance regarding exceptions to the DIS project completion deadlines. Can DIS take responsibility of sharing such exceptions to the Agency and IT Directors?

Answer #1: The only deadlines established by DIS are:

- **June 30, 2014** for agencies to establish roles and responsibilities for performing the work that is due by the next deadline.
- **January 31, 2015** to complete the gap analysis and establish a plan of action for remediation.

If an Agency is unable to meet a deadline, it is responsible for notifying its stakeholders and DIS (informationsecurity@bcb.sc.gov).

Question #2: Do the Agencies need to develop new policies (if those are lacking in their environment) or make sure that relevant processes are documented and in alignment with State InfoSec policies?

Answer #2: Agencies may choose any method which documents and implements secure processes that align with DIS Policies. This should include the review of current process documentation for inclusion of security provisions, and potentially creation of additional process documentation where secure processes are not otherwise described. Replication of the entire DIS Policy framework at the agency level is not required.

Questions Raised: Guidance

The following questions were raised during the previous policy workshop for Small Agency Group:

Question #1: Agencies are interested in providing further comments on the InfoSec policies. What is the cutoff date and how can they go about commenting?
Answer #1: Policies are expected to be out of draft by mid-April. Policies may be further revised by DIS as prudent to address critical needs. A regular policy review cycle has not yet been established. Comments may be submitted at any time, for draft or final versions of policies to DIS by e-mail at informationsecurity@bcb.sc.gov.

Question #2: Do the Agencies need to develop new InfoSec policies (if those are lacking in their environment) or ensure that processes are documented in alignment with State InfoSec policies?
Answer #2: Agencies may choose any method which documents and implements secure processes that align with DIS Policies. This should include the review of current process documentation for inclusion of security provisions, and potentially creation of additional process documentation where secure processes are not otherwise described. Replication of the entire DIS Policy framework at the agency level is not required.

Master Policy: Key Requirements

Master Policy key requirements include the following which need to be established in the Agency environment:

- Agencies shall plan for their implementation of the Information Security Program. Implementation date: **June 30, 2014**.
  - Establish roles, responsibilities, management commitment
  - Resource planning and budgeting
  - Establish a plan of action for implementation
- Agencies shall develop internal procedures for policy management. Implementation date: **January 31, 2015**.
  - Identify security objectives, risk-based approach
  - Consult subject matter experts as needed
  - Establish a schedule for periodic review

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

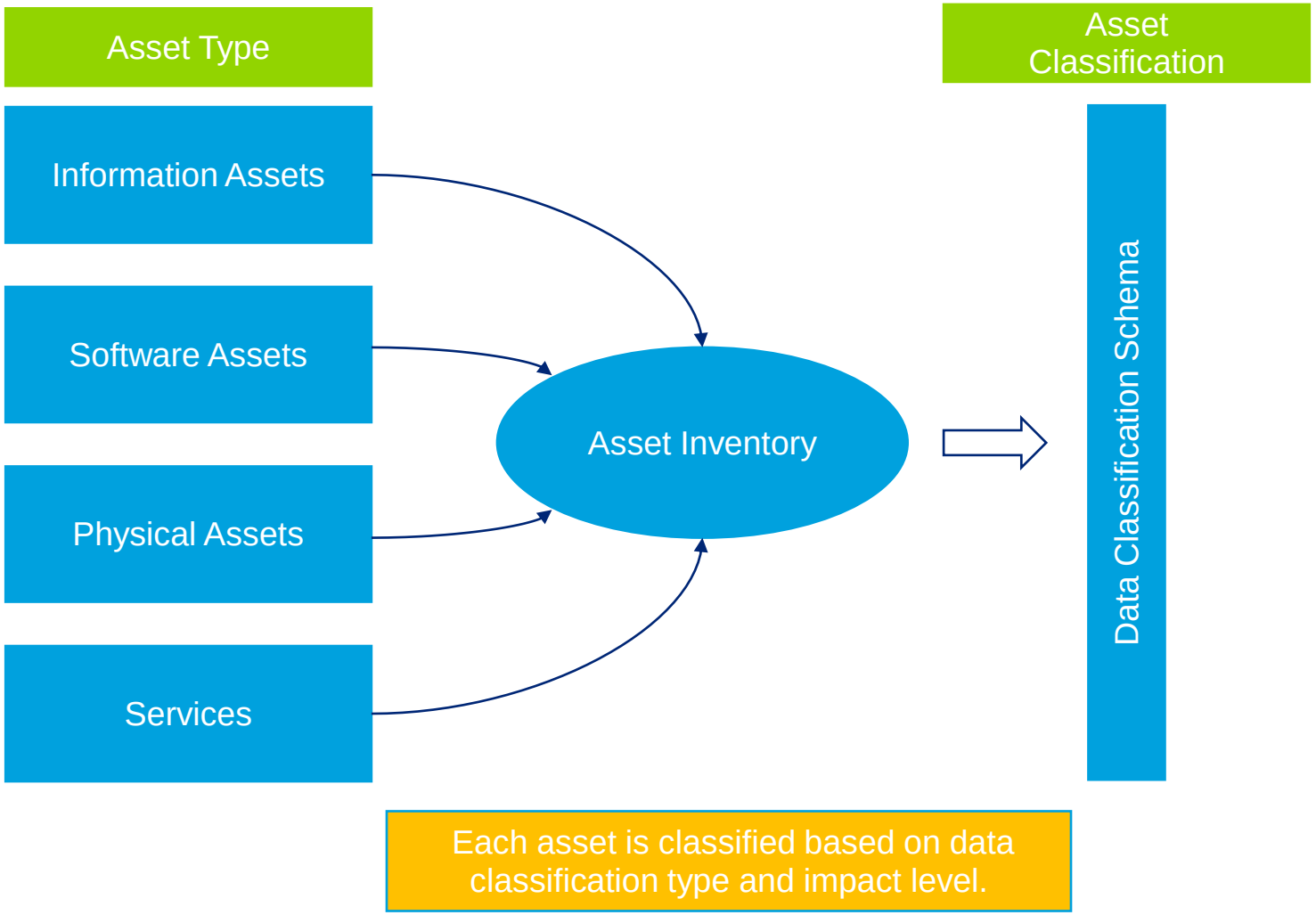
Agencies TO DOs

- 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: Data Protection and Privacy Policy

Asset Management Policy

South Carolina Asset Management Policy mandates that Agencies develop an asset inventory to determine key IT assets which need to have appropriate levels of protection.



Data Classification: Overview

Why Classify Data?

- Agencies can not expect to adequately protect data if they do not know:
  - What type of data exists in the Agency
  - Where is it stored
  - What value does it have to the Agency
  - Who should have access to data
  - How to use data

Which Data Classification Schema to Use?

- To provide consistency in data management, agencies shall classify data according to the State of South Carolina Data Classification Schema: http://dis.sc.gov/schema/Pages/default.aspx

Data Protection and Privacy Policy: Key Requirements

Data Protection and Privacy Policy key requirements include the following which need to be established in the Agency environment:

- Regardless of the format (electronic or hard-copy), all information assets should be classified into one of the following categories:
  - Public
  - Internal Use
  - Confidential
  - Restricted
- If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.
- Media sanitization shall be documented, tracked and reviewed for both electronic and non-electronic media prior to disposal, release or reuse.
- Media sanitization equipment and procedures shall be tested at least annually.

Data Protection and Privacy Policy: Key Requirements

Data Protection and Privacy Policy key requirements include the following which need to be established in the Agency environment:

- Physical destruction or digital wiping shall be tracked and performed on all devices before disposal.
- Agencies shall define and follow an acceptable use policy for employees.
- Agencies shall implement encryption mechanisms to protect confidential and restricted data
- Agencies shall conduct a Privacy Impact Assessment (PIA) for any system that handles Personal Identifiable Information (PII), per NIST 800-53 Rev. 4 (Appendix J, AR-2 Privacy Impact and Risk Assessment) requirement.
- Agencies shall provide confidentiality agreements to all employees and business partners (i.e., contractors, vendors or any third party entities).
- The agency shall designate personnel responsible for data privacy.

Data Protection and Privacy Policy

South Carolina Data Protection and Privacy Policy mandates that Agencies define the different categories for the data regardless of form whether it is electronic, hard copy, or intellectual property.

Public

Information intended or required for sharing with the public

- Brochures
- Press releases
- Website material

Internal Use

Non-sensitive information that is used in daily operations of an agency

- Work phone numbers
- Policies
- Interagency communication

Confidential

Sensitive information in use by an agency

- Information security plans
- Personally Identifiable Information (PII)

Restricted

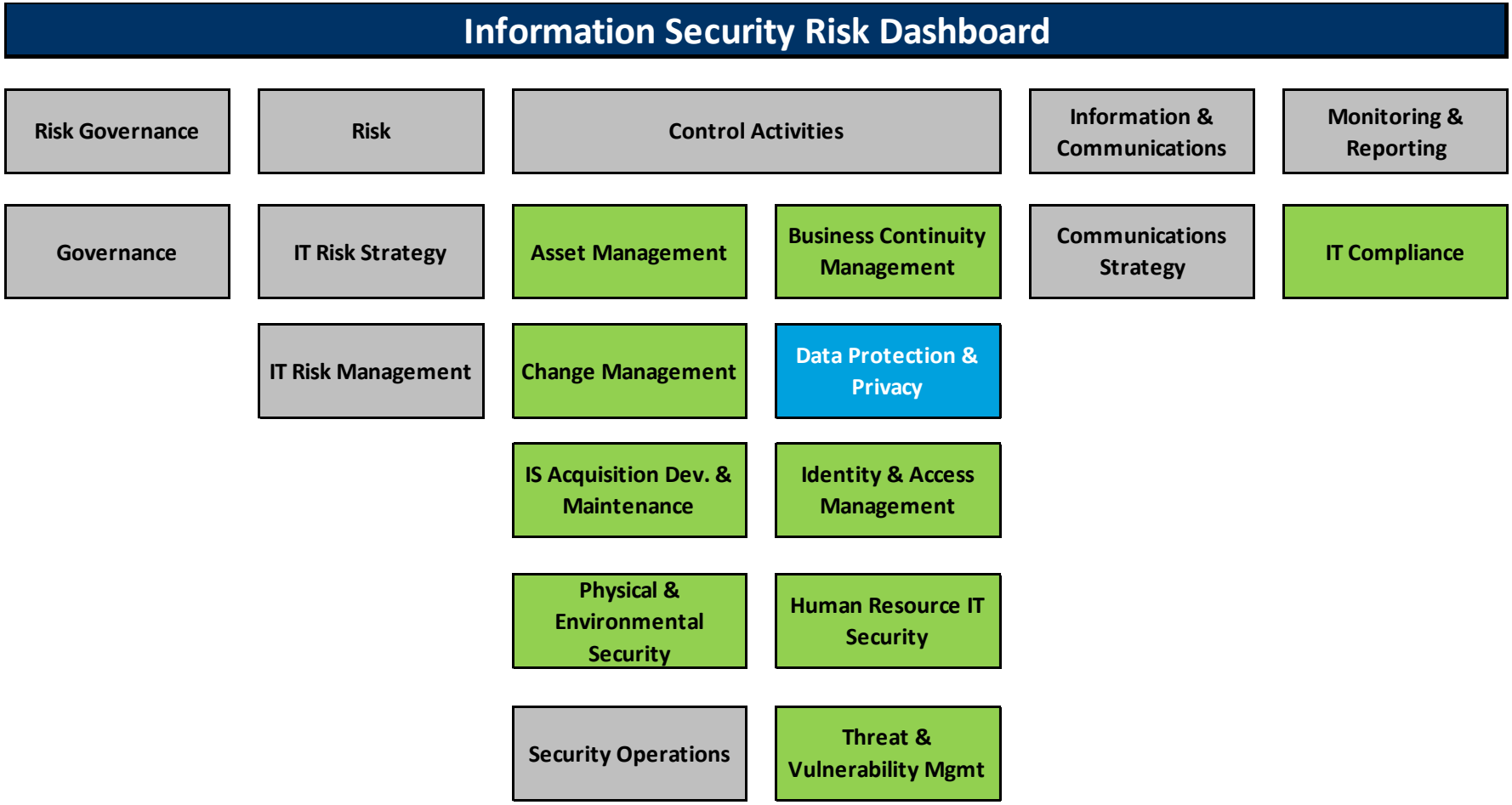
Highly sensitive information protected by statutory penalties

- Data received from the Internal Revenue Service (IRS)
- Personal Health Records (PHR)

Risk Assessment Framework & Data Protection and Privacy 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):



Data Protection and Privacy Policy: Risks & Remediation Strategies

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

Examples		
Overall Risks	Identified Gaps	Remediation Strategies
• Loss of critical data • Loss of reputation • Unauthorized access to confidential data • Statutory / regulatory penalties • Lack of employee awareness	Agencies do not have a data classification policy	Develop and implement a single, broad data classification model using the Statewide Data classification schema
	Agencies do not have comprehensive, documented listings of their interfaces and data exchanges with third parties	Create a detailed document listing of interfaces and models of data exchange with third parties
	Agencies do not have a structured approach to escalate instances of security breaches	Implement a structured approach to escalate instances of security breaches
	Agencies do not have adequate controls over the type of data transferred on to removable devices	Provide employees with training on best practices in data handling and storage

Data Protection and Privacy Policy: Challenges & Remediation Strategies for Agencies

Examples	
Sample Challenges	**Potential Solutions**
Lack of user education and awareness	• Publish and inform employees of the state data classification schema • Develop data classification awareness training for users • Enforce an understanding of the asset inventory and the data held within them (i.e. PII, FTI, PHI, PCI, CJIS, FERPA)
Lack of expertise in data classification	• Determine what data resides within the asset • Use the data classification decision process • Confirm the data classification using the potential impact table
Lack of resources (non-data classification)	• Identify third-party entities to help with disposal and sanitization • Define responsibilities of both parties • Develop a service-level agreement for the Agency

Data Protection and Privacy Policy: Challenges & Remediation Strategies for Agencies

Examples	
Sample Challenges	**Potential Solutions**
Over protection of data (i.e. classify everything as confidential or restricted).	• Understand the state data classification schema • Realign the assets and classification within the Agency
Lack of adequate controls for data protection	• Utilize basic encryption methods, e.g., Public Key Encryption • Utilize encrypted disk and flash memory drives for data at rest and data transfers • Implement access controls based on the data classification type
Lack of data sanitization procedures	• Identify the type of data to be sanitized (i.e., typically, confidential and restricted) • Sanitize the data at source • Develop and document data sanitization procedures for uniform compliance throughout the Agency

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