

# State of South Carolina – Policy Guidance and Training

## Policy Workshop

### Asset Management Policy



March 2014

# Agenda

- Introductions
- Policy Workshop Overview & Timeline
- Policy Overview: Master Policy
- Policy Overview: Asset Management
- Risk Assessment Framework & Asset Management Policy
- Breakout Groups: Gap Analysis & Process Implementation Plan of Action
- Next Steps
- Appendix

# Introductions

# Agency Key Messages

- **Policy adoption:** Each agency is expected to comply with Statewide InfoSec policies issued by the Division of Information Security (DIS).
- **Executive support:** Policies shall be approved by executive management at each Agency and disseminated to all Agency personnel.
- **Policy awareness:** Agency is expected to establish and promote awareness across its employees, contractors and partners to ensure agency-wide information security.
- **Enabling policies:** Policies will require establishment or change of processes, procedures and in some situations, organizational changes in order to be successfully implemented.

# 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
<b>Policy:</b>	<b>Policies:</b>	<b>Policies:</b>	<b>Policies:</b>	<b>Policies:</b>	<b>Policy:</b>
❖ Asset Management	❖ Data Privacy & Protection ❖ 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

# Information Security Policies

- Division of Information Security (DIS) has developed thirteen (13) information security policies to establish an information security framework across Agencies and Institutions.

South Carolina Information Security Policies	
Asset Management	Information System Acquisition, Development, Maintenance
Access Control	IT Compliance
Business Continuity Management	IT Risk Strategy
Data Privacy & Protection	Mobile Security
Master Policy	Physical & Environmental Security
HR & Security Awareness	Risk Management
Threat & Vulnerability Management	

# Policy Overview: Master Policy

## 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 Overview: *Asset Management*

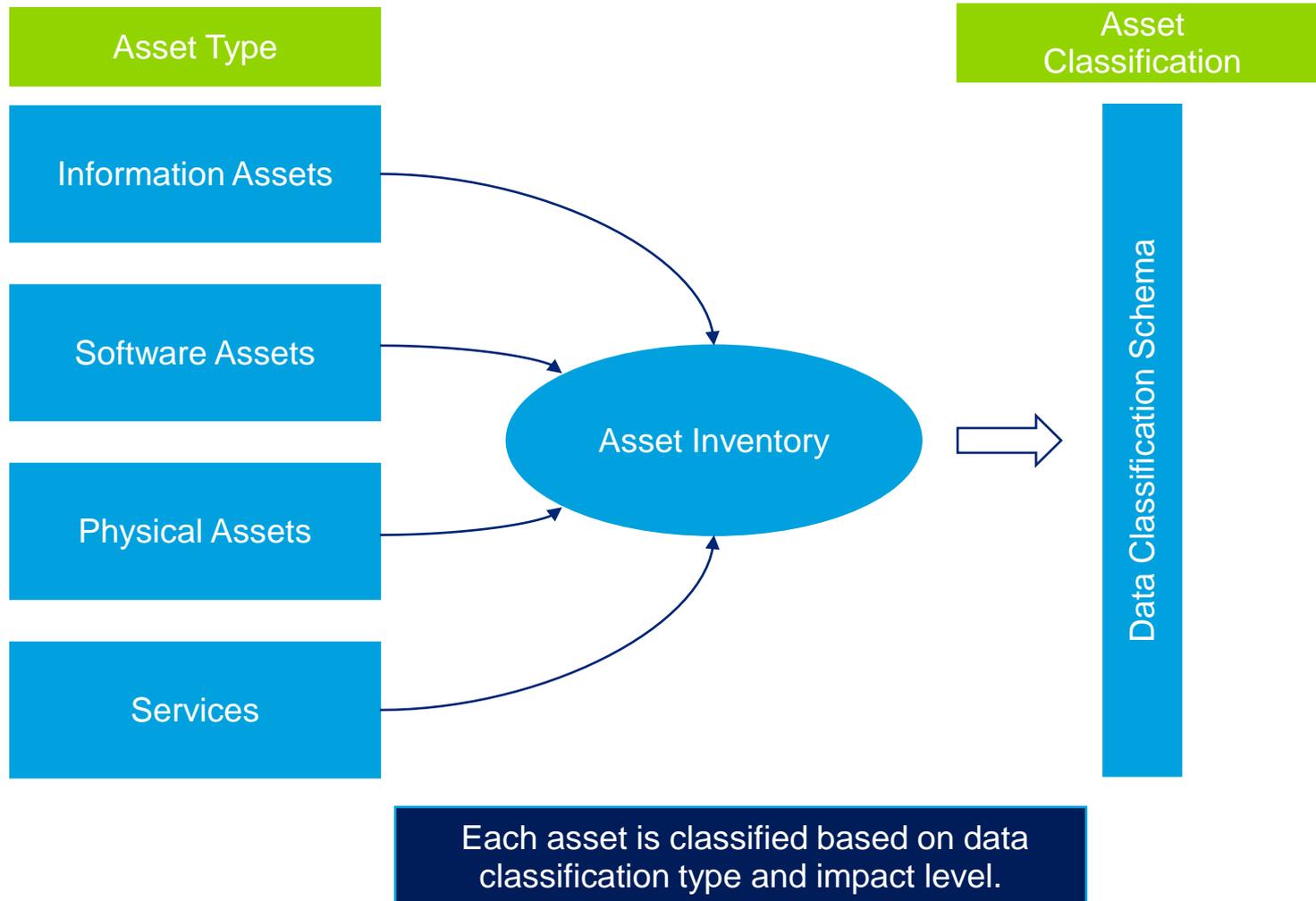
# Asset Management Policy: Key Requirements

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

- Agencies shall create an inventory of their critical IT assets.
- Asset inventories shall be inclusive of the following:
  - IT asset name/description
  - IT asset location
  - IT asset data classification
  - IT asset owner(s)
- Asset inventory shall be reviewed and updated periodically.
- Assets will be classified based on data classification type and impact level.

# Asset Management Policy

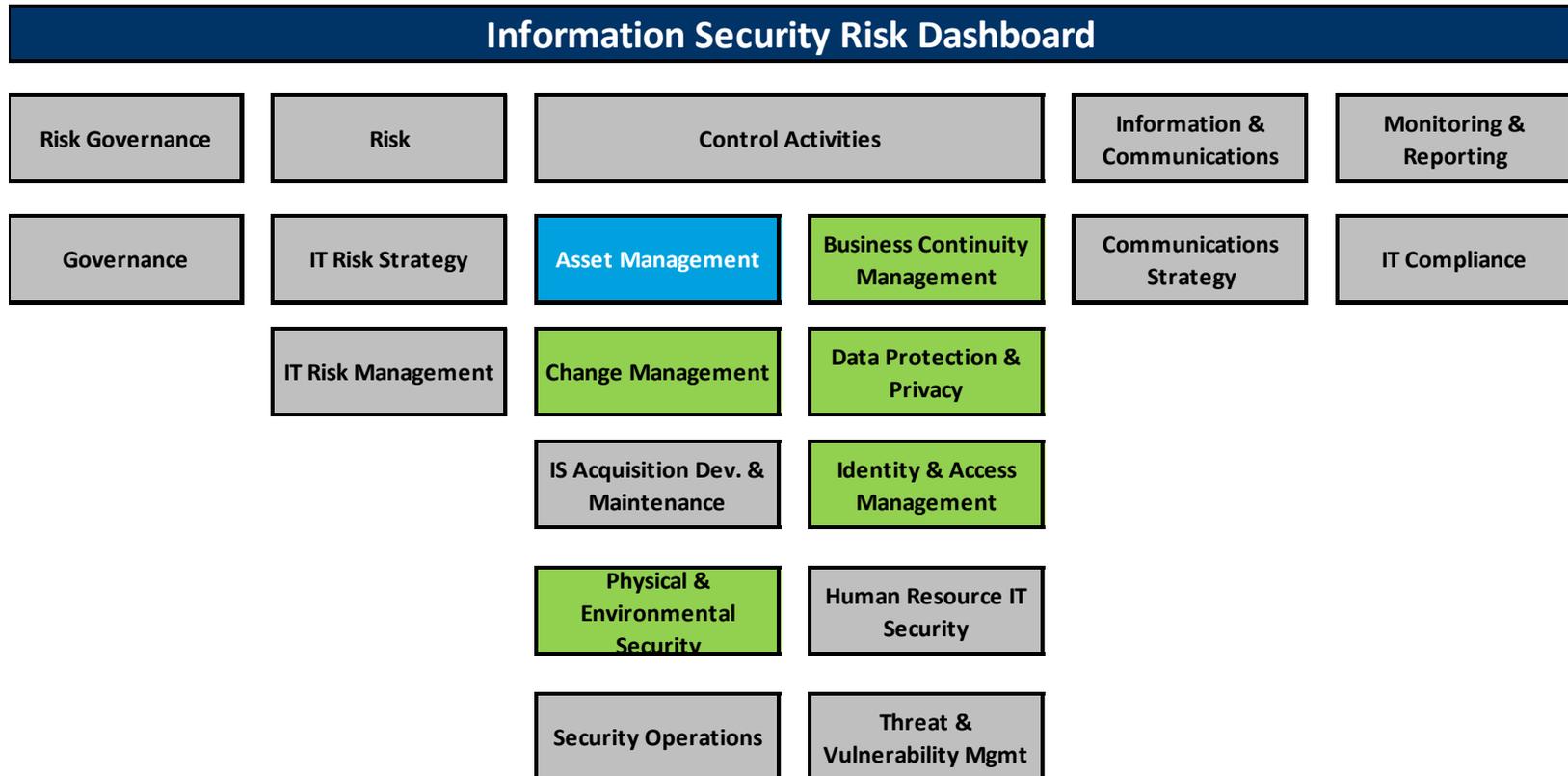
South Carolina Asset Management Policy mandates that Agencies develop an asset inventory to determine key IT assets which need to have appropriate levels of protection.



# Risk Assessment Framework & Asset Management 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):



# Asset Management Policy: Risks & Remediation Strategies

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

Examples		
Overall Risk	Identified Gaps	Remediation Strategies
<ul style="list-style-type: none"> <li>• Over or under maintenance</li> <li>• Unidentified assets</li> <li>• Asset theft or leaks</li> <li>• Employee carelessness</li> </ul>	Critical IT assets are not clearly identified, inventoried, and are not owned by a designated asset owner.	Identify IT assets, inventory and assign asset owners.
	Designated information asset owners are not being held responsible for inventory and asset classification.	Clearly define and designate asset owners and their roles and responsibilities.
	Agency-wide asset inventory has not been implemented.	Develop and implement an asset management policy and procedure.
	Agency has not developed a risk ranking for assets.	<ul style="list-style-type: none"> <li>• Utilize data classification schema and classify data</li> <li>• Assign risk rankings to IT assets</li> </ul>

# Asset Management Policy: Challenges & Remediation Strategies for Agencies

Examples	
Sample Challenges	Potential Solutions
<p>Siloed program areas</p> <p>Identification of large volumes of assets</p>	<ul style="list-style-type: none"> <li>Collect data from assigned asset owners</li> <li>Identify a truth of source where information can be centralized</li> <li>Provide appropriate access for maintaining asset inventory</li> <li>Classify assets according to data classification schema to align with state policy</li> </ul>
Unidentified asset owners	<ul style="list-style-type: none"> <li>Classify assets per asset type</li> <li>Assign and agree on designated asset owners</li> </ul>
Inaccurately defined/classified asset data	<ul style="list-style-type: none"> <li>Align asset with the data classification schema</li> <li>Uniformly identify assets across the Agency.</li> <li>Label assets physically and digitally</li> </ul>
Continual rotation of assets within the Agency	<ul style="list-style-type: none"> <li>Implement a process that allows asset owners the opportunity to regularly update and monitor the asset inventory</li> <li>Provide appropriate access for maintaining asset inventory</li> </ul>

# Asset Management Policy: Challenges & Remediation Strategies for Agencies (cont.)

Examples	
Sample Challenges	Potential Solutions
Agency assets managed by a third party	<ul style="list-style-type: none"> <li>• Coordinate management of Agency assets</li> <li>• Define responsibilities of each party</li> <li>• Provide appropriate access for maintaining asset inventory.</li> </ul>
Not knowing what you have	<ul style="list-style-type: none"> <li>• Identify asset owners &amp; collect asset data</li> <li>• Establish and configure an asset hierarchy.</li> <li>• Identify criticality of assets based on business requirements</li> </ul>
Lack of asset management training and awareness with the Agency	<ul style="list-style-type: none"> <li>• Implement a process to train, inform and provide guidance on asset management to asset owners and employees in the Agency.</li> </ul>
Lack of resources Segregation of Duties	<ul style="list-style-type: none"> <li>• Implement process to divide responsibilities</li> <li>• Identify mitigating controls to address residual risk (i.e., secondary review or reporting mechanisms).</li> </ul>

# Breakout Groups: Gap Analysis & Process Implementation Plan of Action

## Breakout Sessions – Gap Analysis

- Breakout groups will consist of 4-5 participants
- Training team will walk through the Gap Analysis template and select questions for each group to discuss
- Each participant will answer the Gap Analysis questions for their respective Agency's environment
- As a group, participants will discuss identified gaps and select one (1) gap to be presented to the audience.
- Allocate 15 minutes to the discussion

### **DEBRIEF**

- Present and discuss identified gaps to policy implementation.

## Breakout Sessions – Implementation Plan of Action

- Training team will walk through the Implementation Plan of Action template
- Breakout groups will use the Gap Analysis findings as the basis for the breakout discussion
- Breakout groups will design:
  - **Implementation** plan of action for the group's Agency
  - **Challenges** in implementing the State policy
- Allocate 15 minutes to the discussion

### **\*\*DEBRIEF\*\***

Present and discuss implementation plan of action for the group's gap identified.

# Next Steps

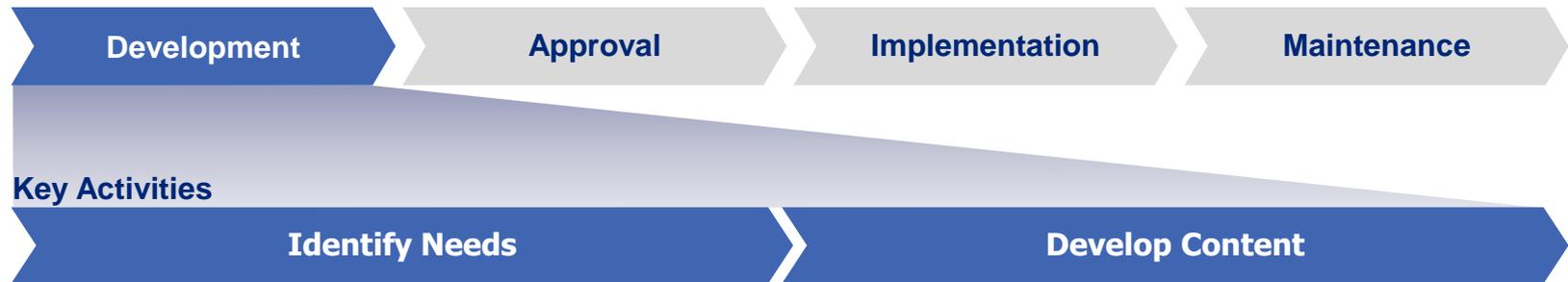
## **Next Steps**

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

# Appendix A: Policy Implementation Process

# Development Phase and Key Activities

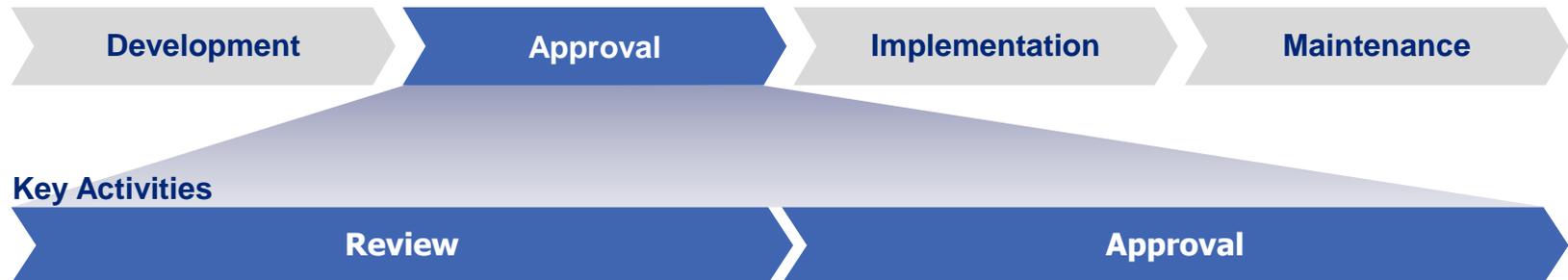
The development phase emphasizes the importance of assessing appropriate legal, regulatory, or business needs prior to the development of draft content. Content development ensures that draft policies and standards are aligned with the IT policy management framework.



- Evaluate business needs or business requirements
  - Assess requirements and impact; legal, regulatory
  - Assess for overlaps and conflicts with other policies and standards
  - For new requirements determine the appropriate hierarchy level (policies or standards)
- Designate owner to drive content development
  - Consult with subject matter resources as needed;
  - Conduct impact assessment to determine key dependencies, length of implementation, and costs
  - Draft content for appropriate hierarchy
  - Create or update existing policies or standards as necessary
  - Prepare draft for review and approval

# Approval Phase and Key Activities

The review and approval of IT policies and standards is necessary to ensure that the appropriate content has been incorporated and that adequate assessments (e.g., impact, mapping to risks and controls library) have been performed prior to policies or standards implementation.



- Identify potential areas of issues or concerns
- Send policies or standards back to owner with feedback
- Update draft policies or standards to address feedback
- Resubmit policies or standards for final review and approval
- Review authoritative sources by mapping policies or standards control statements to risk and controls library. Update risks and controls library (if required)

- Decision made to approve, revise, or cancel proposed policies or standards
- Document justification for revision or cancellation
- Define effective date
- Approved policies or standards submitted for implementation

# Implementation Phase and Key Activities

Implementation ensures that change control over documents is appropriately enforced, IT policies and standards are published in a central repository, and that expectations due to policies or standards changes have been adequately communicated to affected parties.



# Maintenance Phase and Key Activities

Maintenance ensures that historic versions of IT documents are retained, periodic review of policies and standards is performed, and monitoring for exceptions is conducted.



# Policy Implementation Drivers

An information security program is a foundational component of the overarching strategy to protect sensitive information, resources, and data. The program plays a key role in establishing a baseline of controls that should be implemented across the Agencies.

Four key drivers for developing an information security program include:

<p style="text-align: center;"><b>Risk Management</b></p> <ul style="list-style-type: none"> <li>▪ Baseline expectations across the organization for IT domains</li> <li>▪ Define and communicate management's risk tolerance</li> <li>▪ Measure and monitor compliance with IT risk</li> </ul>	<p style="text-align: center;"><b>Standardization</b></p> <ul style="list-style-type: none"> <li>▪ Standardize IT processes and requirements</li> <li>▪ Define key aspects of IT management</li> <li>▪ Reduce IT development and implementation costs</li> </ul>
<p style="text-align: center;"><b>Alignment</b></p> <ul style="list-style-type: none"> <li>▪ Align IT goals and objectives with the business</li> <li>▪ Increase awareness of IT requirements across the enterprise</li> <li>▪ Align with legal, regulatory and industry requirements</li> </ul>	<p style="text-align: center;"><b>Integration</b></p> <ul style="list-style-type: none"> <li>▪ Consistently manage IT processes and technologies</li> <li>▪ Integrate IT requirements into operational processes</li> <li>▪ Provide a mechanism to enforce IT requirements</li> </ul>

**Despite various drivers leading organizations to develop a robust IT policies and standards program, implementation and management challenges exist**

# Appendix B: References

# References

## ISO 55000: Standards for Asset Management

- ISO 55000 – Overview, principals and technology
- ISO 55001 – Management systems – Requirements
- ISO 55002 – Management systems – Guidelines for the application of ISO 55001

## PAS 55: Optimal management of physical assets

- Part 1 – Specification for the optimized management of physical infrastructure assets
- Part 2 – Guidelines for the application of PAS 55-1

## Asset Management Standards:

- E2604-09 – Standard Practice for Data Characteristics of Equipment Records
- E2812-11 – Standard Practice for Uniform Data Management in Asset Management Records Systems
- E2132-11 – Standard Practice for Inventory Verification: Electronic and Physical Inventory of Assets