State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agencies

Information Systems (IS) Acquisitions, Development, and Maintenance Policy

April/May 2014

Agenda

- Questions & Follow-Up
- Policy Workshop Overview & Timeline
- Policy Overview: IS Acquisitions, Maintenance, and Development Policy
- Risk Assessment Framework & IS Acquisitions, Maintenance, and Development Policy
- Next Steps

Questions & Follow-Up

Policy Workshop Q&As

The following questions were raised during the **Access Control** policy workshop for **all Agencies**:

Question #1 For third party hosted systems, does the third party need to be certified (e.g., SSAE 16) or provide reporting back to the Agency? Are there any mandatory requirements from DIS?

Answer #1: IS Acquisitions, Maintenance and Development and IT Risk Management policies provide guidance that Agencies need to monitor the third parties on an ongoing basis to ensure compliance with security requirements. Method and approach used is left up to the Agencies discretion.

Question #2: Will DIS be recommending an asset management software?

Answer #2: DIS has no current recommendations on the asset management software.

Policy Workshop Q&As *(continued)*

The following questions were raised during the **Access Control** policy workshop for **all Agencies**:

Question #3 When will the DIS InfoSec policies become final?

Answer #3: Policy comment period has closed. InfoSec policies are being finalized by the DIS. Agencies should not refrain from making progress as no major or substantial changes will be made based on feedback received. All policies have been posted on the DIS website under the "Policies" tab (http://dis.sc.gov/policies/Pages/default.aspx).

Question #4 When will the training materials be posted on DIS website?

Answer #4: The training materials and schedules are uploaded on the DIS website under the "Resources" tab (http://dis.sc.gov/policies/Pages/default.aspx).

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: IS Acquisitions, Development, and Maintenance Policy

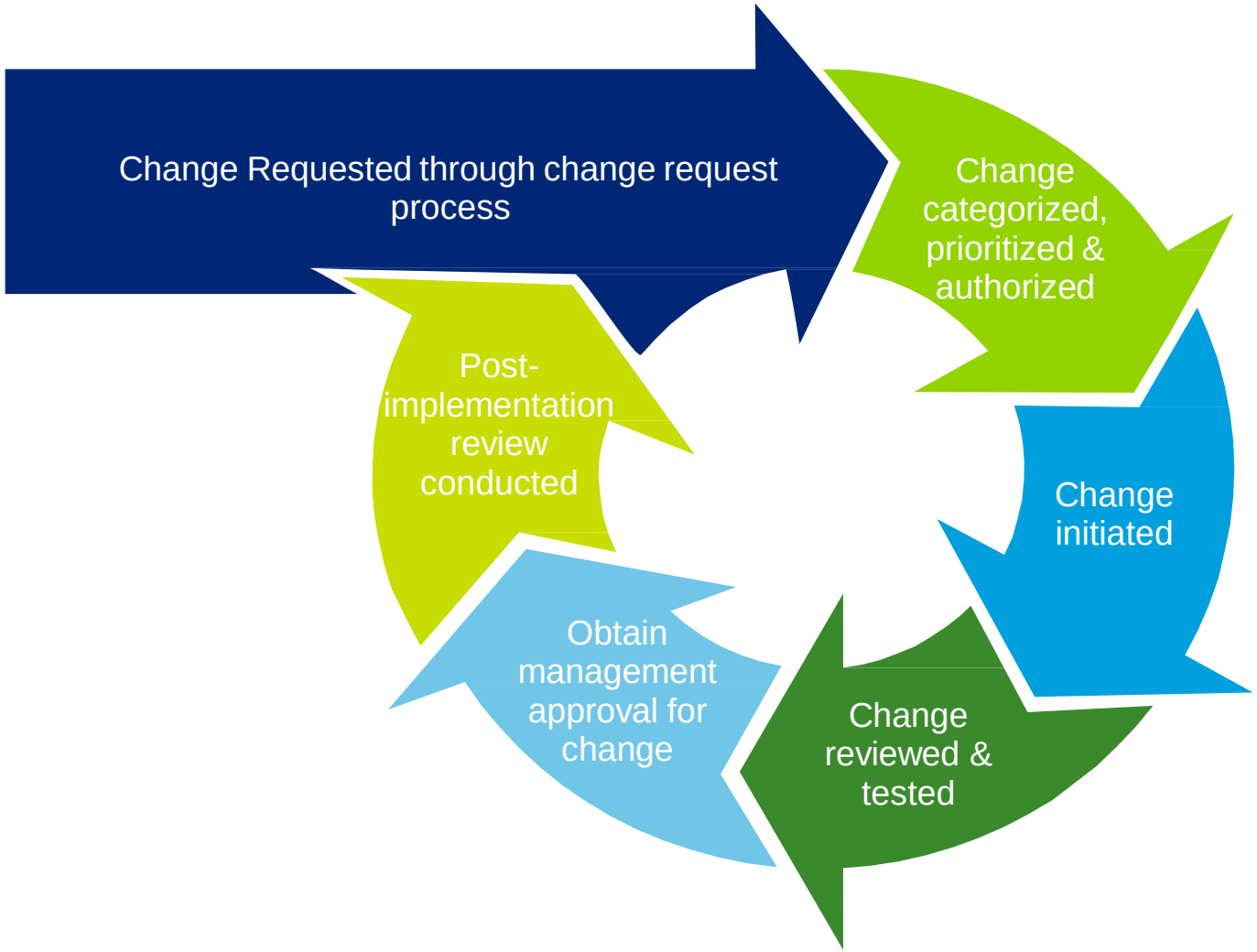
IS Acquisitions Development and Maintenance:
Key Requirements

Change Management
Configuration Change Control

- Agency shall incorporate the following recommendations for the change control process:
  - Determine the impact on the system and its functionality through change requests;
  - Implement a process to categorize, prioritize and authorize changes to the information system;
  - Formally manage changes to production environment
  - Review and test information systems after major changes to operating systems
  - Obtain management approvals
  - Perform post-implementation reviews

IS Acquisitions Development and Maintenance:
Configuration Change Control

The process below provides a graphic representation of Configuration Change Control



IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

Configuration Management

Baseline Configuration

- Agency shall manage changes to baseline configurations prior to implementing changes through:
  - Identification
  - Review
  - Security impact analysis
  - Testing
  - Approval.

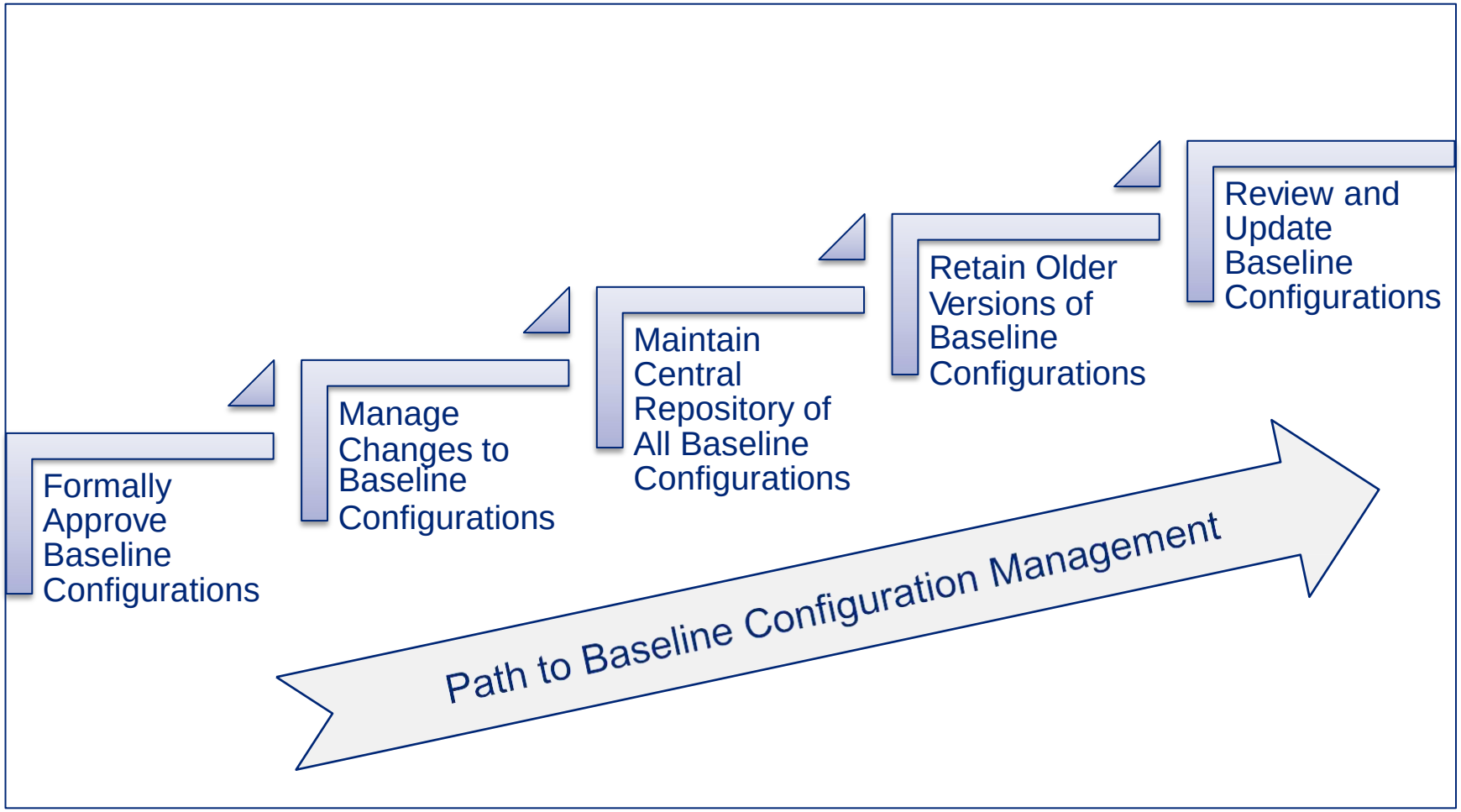
- Agency shall establish and maintain a central repository of all baseline configurations and restrict access to prevent unauthorized changes.

- Agency shall retain older versions of baseline configurations.

- Agency shall review and update baseline configurations periodically.

IS Acquisitions Development and Maintenance: Baseline Configuration Management

The process below provides a graphic representation of a Baseline Configuration Management



IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

System Development and Maintenance

System Security Plan (SSP)

- Agency shall **ONLY** document SSPs for:
  1) Mission Critical enterprise information systems, or
  2) Systems under development

- An SSP shall describe the controls for the system life cycle: development, testing, review, approval, etc. (*NIST template can be accessed at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf*)

- If a qualifying system is modified, the documentation shall be updated accordingly.

Vulnerability Scanning

- Agency shall perform vulnerability assessments on information systems undergoing significant changes **prior** to being moved into production.

IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

System Development and Maintenance

Vulnerability Scanning (cont'd)

- Agency shall establish remediation measures to address the findings of vulnerability assessments.

- Agency shall assess, monitor and address information system-related vulnerability notifications from vendors

System and Services Acquisition Policy and Procedures

- Agency shall ensure that all IT procurement contracts protect State's interest.

System Development Life Cycle

- Agency shall implement security controls at all stages of the information system development life cycle.

IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

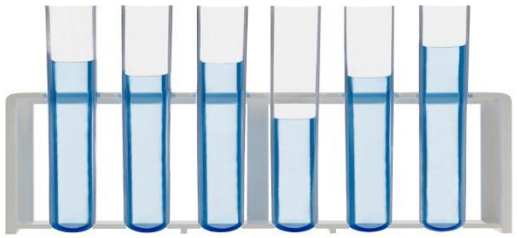
System Development and Maintenance

External Information System Services

- Agency shall monitor outsourced (i.e. third party) software development.

Developer Security Testing and Evaluation

- Agency shall establish separate development, testing, and production environments.
- Agency shall only use sanitized production data for testing purposes.
- When production data is temporarily used in testing environment, the Agency shall:
  - Obtain management approval
  - Remove post-test data
  - Document related activities



IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

System Development and Maintenance

Flaw Remediation

- Agency shall ensure correct processing of user-developed applications and information systems data.
- Agency shall apply software patches to remove or reduce security weaknesses.

Security Alerts, Advisories, and Directives

- Agency shall collect patch alerts, advisories, and directives on an ongoing basis *(frequency will be determined by the Agency*).
- Agency shall designate personnel to monitor vulnerabilities and vendors' patches and fixes.

IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

System Development and Maintenance

Software, Firmware, and Information Integrity

- Agency's upgrades to information systems due to new releases shall be based on:
  - Business requirements for the change;
  - Security of the release (e.g., the number and severity of security problems affecting this version).

- Agency shall test critical operating system (OS) changes and updates in the test environment **ONLY**.

Information Input Validation

- Agency shall test the validity of information inputs and outputs.

- Agency shall detect information system processing errors and inadvertent or deliberate activities.

IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

System Development and Maintenance

Session Authenticity

- Agency shall identify controls to:
  - Ensure session authenticity;
  - Protect message integrity in applications; and
  - Protect information transmission to and from information systems.

Release Management

Allocation of Resources

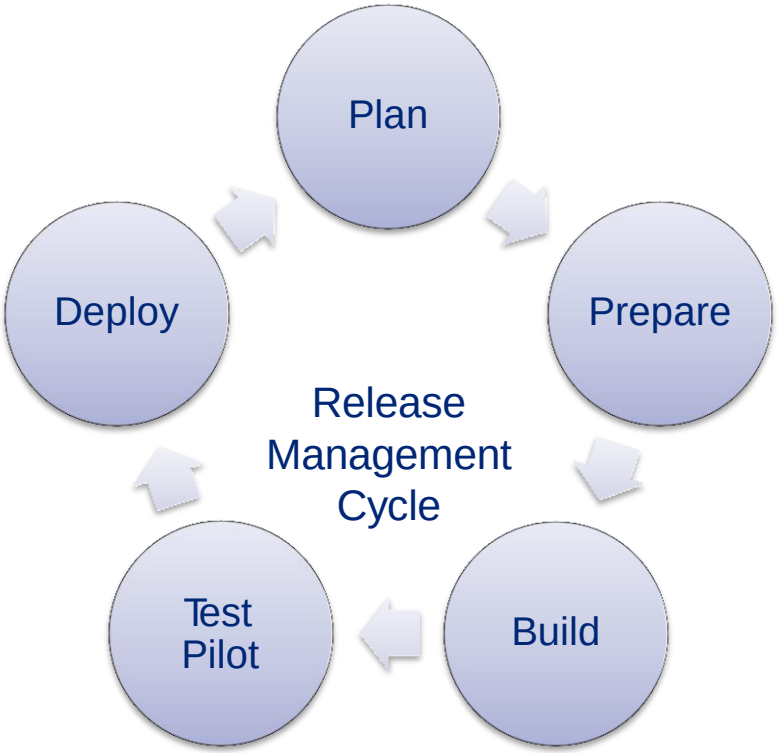
- Agency shall ensure that production-ready release packages have been deployed using the release management lifecycle.

IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

Release Management

Allocation of Resources

- Agency's release planning process shall include:
  - Resources required to deploy release;
  - Pass / fail criteria;
  - Build and test plans prior to implementation;
  - Pilot and deployment plans; and
  - Develop requirements for the release.



IS Acquisitions Development and Maintenance: Key Requirements (Cont'd)

Release Management

Information System Documentation

- Agency shall document processes for management of IT release lifecycle and release prioritization.

- Agency shall ensure that release designs are aligned with the requirements and identifying risks and potential issues.

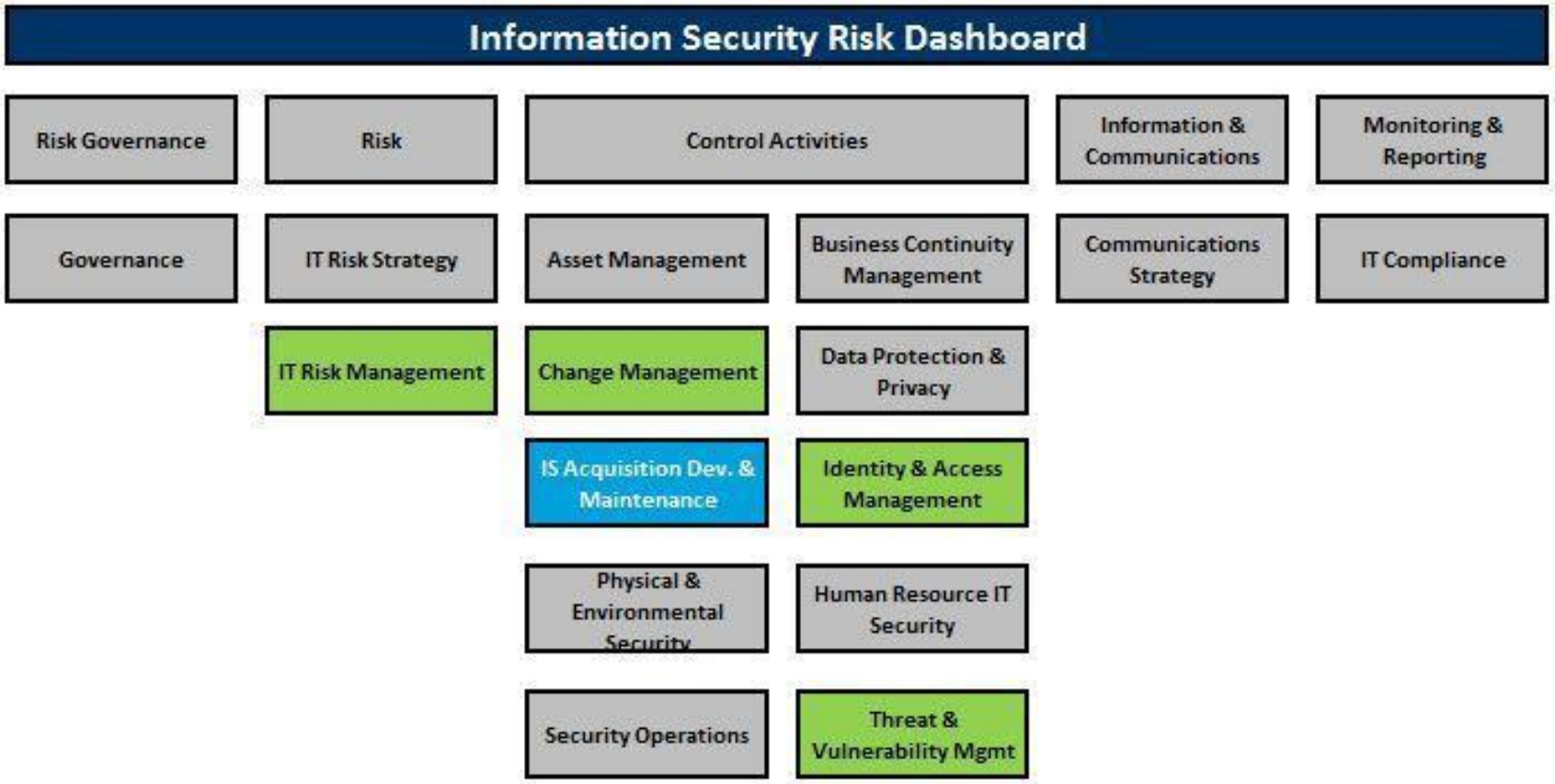
Security Engineering Principles

- Agency shall use the change request process to deploy releases into production.

Risk Assessment Framework & IS Acquisitions, Maintenance, and Development 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):



IS Acquisitions, Development, and Maintenance 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
• Sensitive data exposure during code testing • Technical risk to security posture of Agency • Lack of developer training leads to sub-standard code development	Agencies do not conduct code reviews and peer reviews prior to making changes to the production environment	Establish code review and peer review procedures in the system development life cycle
	Agencies have not established an enterprise-wide Systems Develop Life Cycle (SDLC)	Establish a enterprise-wide SDLC
	Production data is copied into development environments without proper security considerations	Establish three environments - production, test and development to conduct code testing
	Developers are not provided information security trainings such as secure coding practices or secure development standards	Provide code developers with training related to 'industry best practices' related to secure coding practices and development standards

IS Acquisitions, Development, and Maintenance Policy:
Challenges & Remediation Strategies for all Agencies

Examples	
Sample Challenges	**Potential Solutions**
Collecting Performance Metrics	• Develop a process to collect software metrics and which is approved by management • Request end-user participation in the collection of metrics
Lack of a structured communications process	• Establish a structured communication process to solicit inputs from end users • Encourage period 'debriefs' between the developer community and the end user.
Segregation of Duties	• Establish separate roles for code development and code review
Securing code post approval, however, prior to implementation in the production environment	• Code ready for production could be secured in a test server prior to its release to production • Access to this server can be restricted only to authorized personnel
Emergency changes to production software	• Develop an emergency change management process involving only the required number of authorized personnel. • Ensure all such changes are reviewed and approved by a member of the security team (i.e., information security officer or equivalent) and approved by an authorized individual (i.e., IT director or equivalent)

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