SOUTH CAROLINA
DEPARTMENT OF EDUCATION

TITLE OF POLICY: SC Risk Assessment Policy

SECTION: Information Security and Privacy

SUBSECTION: Information Security Framework

POLICY NUMBER: 701.3

OFFICE OF RESPONSIBILITY: CISO

EFFECTIVE DATE: May 01, 2025

THE RELEVANT DEPARTMENT OF ADMINISTRATION POLICY IS ATTACHED. BELOW IS A SYNOPSIS OF THE POLICY CONTENTS:

1. Purpose and Scope

This policy is part of the South Carolina statewide information security framework and establishes requirements for identifying, analyzing, and managing risks to agency information systems.
It applies to all state agencies and supports the broader information security and privacy program. While it provides a baseline standard, agencies must also comply with other applicable laws and regulations and may supplement this policy with organization-specific guidance.

2. Core Objective

The policy's primary objective is to ensure agencies implement a consistent and effective approach to risk management in order to:

- Identify threats and vulnerabilities
- Evaluate potential impacts to systems and data
- Inform risk-based decision-making
- Strengthen overall security and privacy posture

3. Key Policy Requirements

A. Governance and Oversight (RA-1)

- Agencies must develop, document, and maintain a risk assessment policy and supporting procedures.
- A designated official must oversee policy development, implementation, and updates.
- Policies must align with applicable laws, regulations, and standards.

B. Security Categorization (RA-2)

- Agencies must categorize systems and the information they process, store, and transmit based on sensitivity and criticality.
- Categorization results must be documented in system security plans.
- The categorization must be reviewed and approved by an authorized official.

C. Risk Assessments (RA-3)

- Agencies must conduct formal risk assessments that include:
  - Identification of threats and vulnerabilities
  - Evaluation of likelihood and potential impact of adverse events
  - Consideration of risks to systems and individuals, including those involving personal data
- Results must be documented, reviewed, and shared with appropriate personnel.
- Risk assessments must be updated periodically and whenever significant changes occur to systems or their environment.

D. Vulnerability Monitoring and Scanning (RA-5)

- Agencies must regularly monitor and scan systems and applications for vulnerabilities.
- Automated tools and standardized methods should be used where possible.
- Scan results must be analyzed, and confirmed vulnerabilities remediated based on risk.
- Agencies should share vulnerability information to prevent similar issues across systems.
- Vulnerability definitions and scanning capabilities must be kept current.

E. Risk Response (RA-7)

- Agencies must respond to identified risks and assessment findings in accordance with defined risk tolerance.
- Response actions should reflect organizational priorities and may include mitigation, acceptance, transfer, or avoidance of risk.

F. Privacy Impact Assessments (RA-8)

- Agencies must conduct privacy impact assessments before:
  - Developing or acquiring systems that process personally identifiable information
  - Initiating new collections of personal data involving multiple individuals
- These assessments ensure that privacy risks are identified and addressed early in system or program development.

4. Security and Compliance

- Must comply with FERPA, state privacy laws, and the South Carolina Public Records Act.
- Content may be considered public record and is subject to audit or disclosure.
- This policy will be reviewed annually. Violations may result in disciplinary action or loss of access.

5. Related Policies

- SC Access Control Policy Draft (702.4)
- SC Personally Identifiable Information Processing and Transparency Draft (704.1)
- SC Audit and Accountability Policy Draft (706.3)

Information Security and Privacy Policy – Risk Assessment

Division of Information Security

May 01, 2025

Revision History

Version Number	Date	Author(s)	Description
2.0	May 1, 2025	Division of Information Security	Updated for SCDIS-200 v2.0

CONTENTS

1.0 INTRODUCTION

A. Purpose

The South Carolina Statewide Information Security Program (SC Infosec Program) consists of information security policies, standards and guidelines that establish a baseline information security framework to protect the information technology systems of South Carolina state government agencies[1].

Implementing the baseline framework is critical to the development of an agency information security and privacy program. An effective information security and privacy program continually improves the overall security posture for the state, as it integrates and matures toward support of the state and organizational mission, goals and objectives.

This *Risk Assessment Policy* establishes requirements for identifying, analyzing and managing risks to an agency's information systems.

B. Authority and Responsibilities

The organizational and functional responsibilities for the South Carolina Division of Information Security (DIS) and Agency are established in the SC Infosec Program's "Master Policy."

C. Scope

Organizations shall comply with the SC Infosec Program's policies, standards and guidelines. Implementation of the SC Infosec Program's policies, standards and guidelines is not meant or intended to replace, supersede or otherwise nullify agency compliance requirements identified in other applicable federal, state, local, agency or institutional regulations, policies, or guidance. Likewise, compliance with the SC Infosec Program's policies, standards and guidelines does not convey compliance with other regulatory requirements agencies may have for information security.

Organizations may implement policies, standards and guidelines "as-is," but are encouraged to develop additional agency or institution-specific guidance to address unique components of their business operations.

[1] The term "Agency" will be used to refer to SC state government agencies as described in the SC Infosec Program's "Master Policy."

2.0 RISK ASSESSMENT POLICY STATEMENTS

A. Policy and Procedures [RA-1]

NIST CSF Reference: GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03

1. Agencies shall develop, document and disseminate:
    a. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines.
    b. Procedures to facilitate the implementation of the *Risk Assessment Policy* and the associated risk assessment controls.
2. Agencies shall designate an official to manage the development, documentation and dissemination of the risk assessment policy and procedures.
3. Agencies shall review and update the current risk assessment policy and procedures at defined frequencies and following defined events.

B. Security Categorization [RA-2]

NIST CSF Reference: ID.AM-05, ID.RA-04, ID.RA-05

1. Agencies shall categorize the system and information it processes, stores and transmits.
2. Agencies shall document the security categorization results, including supporting rationale, in the security plan for the system.
3. Agencies shall verify the authorizing official ,or authorizing official designated representative, reviews and approves the security categorization decision.

C. Risk Assessment [RA-3]

NIST CSF Reference: GV.RM-06, GV.RM-07, GV.SC-03, GV.SC-09, GV.SC-10, ID.AM-05, ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.IM-01, ID.IM-02, ID.IM-03, DE.AE-07, RS.AN-08

1. Agencies shall conduct a risk assessment, including:
    a. Identifying threats to and vulnerabilities in the system.
    b. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction of the system, the information it processes, stores, or transmits, and any related information.
    c. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.
2. Agencies shall integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk

assessments.

3. Agencies shall document risk assessment results.
4. Agencies shall review risk assessment results.
5. Agencies shall disseminate risk assessment results to designated personnel or roles.
6. Agencies shall update the risk assessment according to a defined frequency or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

D. Vulnerability Monitoring and Scanning [RA-5]

NIST CSF Reference: GV.SC-10, ID.RA-01, ID.RA-08, ID.IM-01, ID.IM-02, ID.IM-03

1. Vulnerability Monitoring and Scanning [RA-5]:
   a. Agencies shall monitor and scan for vulnerabilities in the system and hosted applications according to a defined frequency and when new vulnerabilities potentially affecting the system are identified and reported.
   b. Agencies shall employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
      (1) Enumerating platforms, software flaws and improper configurations.
      (2) Formatting checklists and test procedures.
      (3) Measuring vulnerability impact.
   c. Agencies shall analyze vulnerability scan reports and results from vulnerability monitoring.
   d. Agencies shall remediate legitimate vulnerabilities in accordance with an organizational assessment of risk.
   e. Agencies shall share information obtained from the vulnerability monitoring process and control assessments with designated personnel or roles to help eliminate similar vulnerabilities in other systems.
   f. Agencies shall employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
2. Update Vulnerabilities to be Scanned [RA-5 (2)]:

   Agencies shall update the system vulnerabilities to be scanned.

3. Privileged Access [RA-5 (5)]:

   Agencies shall implement privileged access authorization to defined system components for defined vulnerability scanning activities.

E. Risk Response [RA-7]

NIST CSF Reference: GV.OC-05, GV.RM-01, GV.RM-03, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-03, GV.SC-09, GV.SC-10, ID.RA-05, ID.RA-06, ID.IM-01, ID.IM-02, ID.IM-03, RS.AN-08

Agencies shall respond to findings from security and privacy assessments, monitoring and audits in accordance with organizational risk tolerance.

F. Privacy Impact Assessments [RA-8]

NIST CSF Reference: ID.RA-04

Agencies shall conduct privacy impact assessments for systems, programs or other activities before:

1. Developing or procuring information technology that processes personally identifiable information.
2. Initiating a new collection of personally identifiable information that:
    a. Will be processed using information technology.
    b. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more individuals, other than agencies, instrumentalities or employees of the state government.