STATE OF ALABAMA

Information Technology Guideline

GUIDELINE 606G1-00: RISK ASSESSMENT AND MITIGATION

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its life cycle. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

OBJECTIVES:

- Provide guidelines for performing routine risk assessments of the State of Alabama computing environment to address external and internal threat agents.
- Provide risk mitigation options and methodology.

SCOPE:

The guidelines in this document apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

GUIDELINES:

RISK ASSESSMENT

Based on the recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Systems, State of Alabama risk assessment processes should follow these nine steps:

SYSTEM CHARACTERIZATION:

All State of Alabama information systems and the networks that provide system-to-system communication establishes the risk assessment boundaries for this risk management policy. The risk assessment process shall encompass the entire system processing environment including, but not limited to, the information system mission, hardware, software, system interfaces, personnel access, system and data criticality, and the level of protection required to maintain system and data integrity, confidentiality, and availability.

THREAT IDENTIFICATION:

The risk assessment shall evaluate the security posture of State of Alabama information systems and networks against common threat elements to include: computer, human, environmental and nature.

VULNERABILITY IDENTIFICATION:

The risk assessment, utilizing security checklists and vulnerability assessment toolsets, shall be used to identify vulnerabilities within the State of Alabama information systems and networks and associate

the vulnerability with an identified threat category. The security checklist shall, at a minimum, cover the Management, Operational and Technical security control areas.

CONTROL ANALYSIS:

The risk assessment shall evaluate the effectiveness of current technical and non-technical security controls. The control analysis will review the preventative and detective characteristics of the security controls.

LIKELIHOOD DETERMINATION:

Based on the threat element motivation, vulnerability type and existing control measures, a Likelihood Rating will be assigned to the vulnerability as Low, Medium or High. The following Likelihood Level definitions will be applied:

Table 1: Likelihood Level Definitions

Likelihood	Definition
High	The threat source is highly motivated and sufficiently capable and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

IMPACT ANALYSIS:

The risk assessment will provide, based on the loss of confidentiality, integrity and availability, what impact is possible to the State of Alabama information system. The impact will be ranked in a Low, Medium and High level.

Table 2: Impact Level Definitions

Impact Level	Definition
High	Exercise of the vulnerability may: (1) result in the highly costly loss of major tangible assets or resources; (2) significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human death or serious injury.
Medium	Exercise of the vulnerability may: (1) result in the costly loss of tangible assets or resources; (2) violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human injury.
Low	Exercise of the vulnerability may (1) result in the loss of some tangible assets or resources, or (2) noticeably affect an organization's mission, reputation, or interest.

RISK DETERMINATION:

The risk assessment will utilize these three attributes in making a final risk determination to the information system or network:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The risk level matrix, table 3 below, shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories.

Table 3: Risk Level Matrix

Threat Likelihood	Impact Level		
	Low (1)	Medium (5)	High (10)
High (10)	Low 10	Medium 50	High 100
Medium (5)	Low 5	Medium 25	Medium 50
Low (1)	Low 1	Low 5	Low 10

High Risk: If an observation or finding is evaluated as a high risk (>50 to 100), there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

Medium Risk: If an observation is rated as medium risk (>10 to 50), corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

Low Risk: If an observation is described as low risk (1 to 10), the system's owner must determine whether corrective actions are still required or decide to accept the risk.

Depending on the organization's requirements and the granularity of risk assessment desired, some assessments may include additional likelihood or impact levels such as Very Low or Very High to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

CONTROL RECOMMENDATIONS:

In order to reduce risk to an acceptable level, the risk assessment will provide risk remediation recommendations based on these factors:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

RESULTS DOCUMENTATION:

A detailed report shall be prepared for senior management following the conclusion of the risk assessment. The report will describe the threats and vulnerabilities, measure the risk, and provide recommendations for control implementation.

RISK MITIGATION

Based on the recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Systems, the State of Alabama organizations shall utilize the following risk mitigation options and methodologies:

RISK MITIGATION OPTIONS:

Risk Assumption:

Accept the potential risk and continue operating the IT system, or implement controls to lower the risk to an acceptable level.

Risk Avoidance:

Avoid the risk by eliminating the risk cause and/or consequences (e.g., forgo certain functions of the system or shut down the system when risks are identified).

Risk Limitation:

Limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).

Risk Planning:

Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.

Research and Acknowledgment:

Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.

Risk Transference:

Transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

RISK MITIGATION METHODOLOGY:

Prioritize Actions:

Based on the risk levels presented in the risk assessment report; the implementation actions will be prioritized. When allocating resources, top priority will be given to risk items with a High risk ranking first; Medium risk ranking second; then the Low risk ranking items. These High risk vulnerability/threat pairs will require immediate corrective action.

Evaluate Recommended Control Options:

During this step, the feasibility of the recommended control options shall be analyzed. The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific State organization and their IT system. The goal is to select the most appropriate control option for minimizing risk.

Conduct Cost-Benefit Analysis:

To aid management in making a decision on what risk mitigation option to employ, a cost-benefit analysis will be conducted.

Select Control:

On the basis of the results of the cost-benefit analysis, management will determine the most cost-effective control(s) for reducing risk to the affected IT system or network. The controls selected

should combine technical, operational, and management control elements to ensure adequate security for the IT system, network and organization.

Assign Responsibility:

Identify personnel who have the appropriate expertise and skill-sets to implement the selected control and assign responsibility. If in-house personnel are not available, then contractors may be used.

Develop a Safeguard Implementation Plan:

A safeguard implementation plan will be developed. The plan should, at a minimum, contain the following information:

- Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- Recommended controls (output from risk assessment report)
- Prioritized actions (with priority given to items with High risk levels
- Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- Required resources for implementing the selected planned controls
- Lists of responsible teams and staff
- Start date for implementation
- Target completion date for implementation
- Maintenance requirements

Implement Selected Control(s):

Depending on the specific situations, the implemented controls may lower the risk level but not eliminate the risk entirely. All residual risk will be documented in a Residual Risk Report and provided to management.

SUPPORTING DOCUMENTS:

- Information Technology Policy 606: Risk Management

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
606G1-00	09/01/2011	Replaces Standards 670-01S1 and 670-01S2