State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.3.07.01	Information Security Risk Analysis	D	12/31/2020	1 of 2

1.0 PURPOSE

This standard establishes the minimum information security risk analysis required in support of determining the proper level of security requirements for an agency.

Absolute security that assures protection against all threats is unachievable. Therefore, a means of weighing losses that may be expected to occur against the cost of the control is required.

Risk analysis offers a disciplined approach through which uncertain events can be identified, measured, and controlled to minimize loss. Risk analysis provides the basis for risk management by identifying the risk(s). Agency management then can either accept the risk(s) or select cost-effective controls and safeguards to reduce the risk(s) to an acceptable level. Risk analysis is a systematic process of evaluating vulnerabilities of a processing system, environment and data against the threats facing them.

2.0 SCOPE

This standard applies to all state agencies meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01

6.0 STANDARD

6.1 Each agency shall perform or update a comprehensive risk analysis at least biennially or when significant changes occur to the agency, office, or IT environment. The analysis shall determine potential loss, identify areas of vulnerabilities, and evaluate existing controls, with the results documented in a Risk Analysis Report.

6.2 Risks that are determined to be at acceptable levels by agency management shall be documented, identifying the risks and the reason(s) management decided to accept the risk without further countermeasures or non-acceptance of corrective recommendations.

6.3 The agency shall develop a Risk Mitigation Plan from the results of the Risk Analysis Report that shall identify the countermeasures to be implemented, the time frame for implementation, and the estimated cost that shall be submitted to the agency management for review and concurrence.

6.4 The agency shall submit a memo to the State Information Security Committee Chair indicating that a Risk Analysis has been performed and a Risk Mitigation Plan has been approved, providing the date(s) the implementation of the Risk Mitigation Plan is planned to be completed.

7.0 DEFINITIONS

None

8.0 RESOURCES

N/A

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	11/24/2020
State Chief Information Officer (CIO)	Signature on File	11/30/2020

Document History

Revision	Effective Date	Change
A	2/14/2002	Initial release
B	8/06/2012	OIS biennial review, replaces standard 4.06
C	12/26/2018	Renumbering (124 to S.3.07.01) and compliance to ADA standards
D	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)