8-703. Security reviews; risk management.

(1) This policy is based on the NIST SP 800-53 security controls framework. Pursuant to that framework, the state must conduct an annual review of the information technology environment to ensure compliance with these standards. The security controls that are to be inspected are organized into control families within three classes (management, operational, and technical).

The state information security officer will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST SP 800-53 security controls, such that over a three-year timeframe all control areas will have been assessed. This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.

(2) Unscheduled Risk Assessments. Unscheduled risk assessments may be performed at the discretion of the state information security officer or agency information security officer, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible in nature, and are intended to review specific elements that have been identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

The security officer shall document the business area, reason for the review, scope of inspection, and dates of the review in the corrective action planning documentation. All findings and results will also be documented in the security corrective action plan.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-703.pdf