Department of Transformation and Shared Services
State Cybersecurity Office

Standard Title: Risk Assessment Standard
Standard Version: 1.0
Effective Date: 12/19/2022

---

1. Purpose

The purpose of this Standard is to manage organizational risk by performing risk assessments so that sufficient countermeasures for mitigating risk to acceptable levels can be implemented.

2. Applicability

This standard covers all systems developed by, or on behalf of the Arkansas Division of Information Systems (DIS), that require authenticated access. This includes all development, test, quality assurance, production and other ad hoc systems.

Notations of specific control items (e.g., CJIS, FTI, PCI) only pertain to the systems that are required to comply with such regulations.

3. Definitions

Refer to the DIS Regulatory Definitions document.

4. Standard

4.1 Security Categorization RA-2

a) Categorization of information and the information system in accordance with applicable State and Federal laws, policies, regulations, standards, and guidance. NIST SP 800-60 Volumes 1 and 2 serves as a guidance for the categorization process. The security categories are based on the potential impact on the DIS should certain events occur that jeopardize the confidentiality, integrity, and availability of the information and

information systems needed by the DIS to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day to-day functions, and protect individuals. The impact to the DIS, State, personnel, and other external entities must be considered during the security categorization process.

b) System Owners shall be involved with the security categorization of an information system if they are responsible for:
    1. Any interconnected system dependencies, i.e., systems that share information
    2. A system that may inherit a security control from their respective system
c) Include the security categorization process as a part of the system development lifecycle (SDLC). The security categorizations shall be developed early in the initiation stage ensuring the planning and implementation of the appropriate security controls throughout the SDLC
d) Ensure the security categorization decision is reviewed and approved by the authorized or designated representative
e) Update documents to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments
f) The DIS, Business Owner, System Owner and supporting security liaison must assist with the development of the security categorization

4.2 Risk Assessment RA-3

a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
b) The DIS documents risk assessment results in the information security assessment report.
c) The system owner reviews risk assessment results as defined in the Regulatory Settings spreads.
d) Review risk assessment results as outlined in the regulatory spreadsheet
e) Update the risk assessment as defined in the regulatory spreadsheet or when a significant change to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

4.3 Supply Chain Risk Assessment RA-3(1)

a) Assess supply chain risks associated with DIS systems, system components, and services.
b) Update the supply chain risk assessment as defined in the Regulatory Settings spreadsheet and when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
c) Service Providers:
    1. Contractors operating information systems on behalf of the DIS
    2. Individuals accessing the DIS's information systems
    3. Outsourcing entities (e.g., cloud service providers (CSPs))
        i. Agencies need to obtain prior approval from the State CIO before contracting with cloud-hosted solutions or off-site hosting.
        ii. The DIS must ensure vendor compliance with Statewide security policies.
        iii. The DIS shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001.
        iv. Procurement language must also require, in addition to initial validation, cloud/vendor must annually provide the DIS validation of their continued compliance to State policies and procedures. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). Examples of acceptable assessment reports include Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001. CSPs must demonstrate to the State that continuous monitoring activities are in place and compliance is being met.

4.4 Vulnerability Monitoring and Scanning RA-5

a) All DIS Risk Assessment programs must include the following requirements:

1. All malware scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events.
2. Vulnerability scans in information systems and hosted applications must be performed as noted in the Regulatory Settings spreadsheet.
3. Vulnerability scanning shall include scanning for specific functions, ports, protocols and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
4. Real-time scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection
5. Scan for malware on files that are downloaded from the Internet or any other outside source, including all external media, such as flash drives, CDs, etc. shall be conducted.
6. Viruses, spyware, Trojan applications and other malicious code may cause damage to the DIS's infrastructure via Web browsers and therefore all internet traffic shall be scanned to prevent malicious code from infecting the DIS's infrastructure.
7. External computers or networks making remote connection to internal DIS computers or networks shall utilize a DIS-approved active virus scanning and repair program and an DIS approved personal firewall system (hardware or software). The DIS shall ensure that updates to virus scanning software and firewall systems are available to users. Non-DIS computers or networks making a remote connection to a public Web server are exempted.
8. The DIS shall scan their networks in order to identify any multifunctional devices (MFD)s on the network that are vulnerable and/or configured insecurely and take remediation actions.
9. Prior to commencing vulnerability scanning efforts, the following should be addressed:

i. Scanner selection – Evaluate the mandated tools for use within the respective environments
ii. The network and host-based vulnerability scanner shall provide the following capabilities:
    1. Identify active hosts on networks.
    2. Identify active and vulnerable services (ports) on hosts.
    3. Identify vulnerabilities associated with discovered operating systems and applications

b) The DIS shall implement a suite of automated monitoring tools to effectively monitor and identify vulnerabilities on networked computer servers and workstations. Vulnerability scanning tools and techniques are employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for the following:
    1. Enumerating platforms, software flaws, and improper configurations
    2. Formatting and making transparent, checklists and test procedures
    3. Measuring vulnerability impact
    4. Analyzing vulnerability scan reports and results from security control assessments
    5. Remediating legitimate vulnerabilities in accordance with an organizational assessment of risk
c) Sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the DIS to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Vulnerability Management

a) System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall, as applicable. Vulnerabilities that threaten the security of the DIS's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings:

1. Personnel shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and updates, and eliminating or disabling unnecessary services.
2. The DIS shall use where possible tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.
3. Perform scans, typically, on systems and networks known to be stable and preferably during times of least impact to the critical functionality of the system. Expect vulnerability scanning to occur during various phases of the system's life cycle.

Vulnerability Risk Ratings and Mitigation

a) Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info", or a score of 0, may be used after appropriate review.

Vulnerability Risk Rating and Mitigation timeframes		
Impact/Severity	Patch Initiated	Patch Completed
Critical-level Risk (Priority/CVSS 9.0-10.0): A vulnerability that could cause grave consequences and potentially lead to leakage of Restricted or Highly Restricted data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, and could cause functionality to cease, exfiltration of data, or an intruder to gain access to the network or IT asset.	Within 24 hours of patch release.	Within 1 week of patch release.

High-level Risk (Priority/CVSS 7.0-8.9): A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder.	Within 24-72 hours of patch detected in vulnerability management software.	Within 2 weeks of patch detection.
Medium-level Risk (Priority/CVSS 4.0-6.9): A vulnerability that should be addressed within the established timeframe. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.	Within 1 week of patch release detected in vulnerability management software.	Within 1 month of patch detection.
Low-level Risk (Priority/CVSS 0.1-3.9): A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and IT assets and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network or IT asset.	Within 1 month of patch release detected in vulnerability management software.	Within 365 days during normal maintenance cycles unless ISO determines this an insignificant risk to environment.

b) The DIS vulnerability mitigation procedures must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate personnel.
c) Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is 'high-level' and no patch is available, steps must be taken to mitigate the risk through other compensating control methods (e.g., group policy objects, firewalls, router access control lists). A patch needs to be applied when it becomes available. When a 'high-

level' risk vulnerability cannot be totally mitigated within the requisite time frame. This type of exception would follow the DIS Exception process.

d) Testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.
e) Notification shall be provided after vulnerability mitigation plans have been executed.
f) In the event of a zero-day vulnerability, a situation where an exploit is used before the developer of the software knows about the vulnerability, the DIS shall mitigate the vulnerability immediately, if possible, and apply patches as soon as possible after the vendor provides them.

Vulnerability Information Review and Analysis

a) Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis, per the DIS's policies and procedures.
b) Vulnerability information, as discovered, shall be distributed to the appropriate DIS employees, including the security office.
c) Appropriate DIS personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

Requirements for Compliance

a) The DIS must develop procedures to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in systems.
b) The DIS shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for handling patches.
c) The patching and vulnerability policy shall specify techniques the DIS will use to monitor for new patches and vulnerabilities and personnel who will be responsible for such monitoring.
d) The DIS's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.
e) A DIS process for handling patches shall include the following:
    1. Using organizational inventories

2. Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring (See http://cve.mitre.org)
3. Patch prioritization techniques
4. Organizational patch databases.
5. Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications

f) The DIS shall:
   1. develop and maintain a list of sources of information about security problems and software updates for the system and application software.
   2. establish a procedure for monitoring those information sources.
   3. evaluate updates for applicability to the systems.
   4. plan the installation of applicable updates.
   5. install updates using a documented plan.
   6. deploy new computers with up-to-date software.

g) After making any changes in a system's configuration or its information content, The DIS shall create new cryptographic checksums or other integrity-checking baseline information for the system.

4.5 Update Vulnerabilities to Be Scanned RA-5(2)

a) For all systems, update the system vulnerabilities to be scanned prior to a new scan, or when new vulnerabilities are identified and reported.

4.6 Breadth and Depth of Coverage RA-5(3) (CJIS Only)

a) For CJIS systems, the DIS shall employ vulnerability scanning procedures that can identify the information system components scanned and vulnerabilities checked.

4.7 Privileged Access RA-5(5)

a) If automated scanning tool functionality is used, it must be able to perform credentialed scans. To the extent possible, credentials should be compliant with organizational policy.

b) Credentialed scanning must be performed on all information systems and network devices (including appliances).
c) The DIS must maintain and provide changes to the system accounts to support credentialed scanning.

4.8 Public Disclosure Program RA-5(11)

a) The DIS must have a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.
b) Critical features include:
    1. Publicly discoverable channels and policies
    2. Explicit authorization of good-faith security research
    3. Absence of non-disclosure as a condition of authorization of testing in public programs
    4. Timeline-driven Coordinated Vulnerability Disclosure (CVD) practices

4.9 Risk Response RA-7

a) DIS will address and mitigate any risks presented by one of the following:
    1. Implementing new controls
    2. Strengthening existing controls
    3. Accept risk with appropriate justification or rationale, sharing of or transferring risk, avoiding risk, or rejecting risk
b) For those risks that cannot be mitigated immediately a plan of action and milestones entry will be required for tracking of mitigation.

4.10 Privacy Impact Assessments RA-8 (FTI Only)

Conduct privacy impact assessments for systems, programs, or other activities before:

a) Developing or procuring information technology that processes personally identifiable information; and
b) Initiating a new collection of personally identifiable information that:
    1. Will be processed using information technology; and
    2. 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, ten or more individuals, other than

agencies, instrumentalities, or employees of the federal government.

c) Supplemental Guidance: A privacy impact assessment must be conducted specifically for new systems used to process, store, or transmit FTI.

4.11 Criticality Analysis RA-9

a) For systems categorized as Moderate, or higher
    1. Identify critical system components and functions by performing a criticality analysis for, system components, or system services and document the analysis in the System Security Plan.

b) NOTE: Criticality Analysis is an end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s).

5. Authority

Refer to the DIS Regulatory Definitions document.

6. Roles & Responsibilities

RACI is an acronym derived from the four key components: Responsible (R), Accountable (A), Consulted (C), and Informed (I).

	Roles					
Activities	Project Risk Manager	Designer	Initial Risk Owners	DPM Management	Risk Management Support Group	Capital Investment Planning & Dev
Risk Planning	A	C		C		C
Risk Identification	A	R	R/C	I		
Risk Analysis	A	R	C			
Quantitative Risk Analysis	A	R	C	C		

Risk Response Planning and Action Plan Development	A	R/C	R/C	I		
Risk Monitoring and Control	A/R	C	C	C	C	
Lessons Learned Documentation	C	C	C	I	A/R	

7. Compliance

This control shall take effect upon publication. Compliance is expected with all DIS controls. Employees not following this DIS control are subject to the standard DIS disciplinary procedures.

If compliance with this control is not feasible or technically possible, or if deviation from this control is necessary to support a business function, applicable entities shall request an exception through the DIS Exception Request procedure.

8. Related Documentation

Risk Assessment Procedures
Policy_RA_Risk Assessment
SCSO_Exception Request Procedure
SCSO_Regulatory Definitions
SCSO_Regulatory Settings

9. Revision History

This standard shall be subject to review according to the Regulatory Spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
12/16/2022	Moved from Draft to Final	Greggari Tucker, Deputy Chief Information Security
12/19/2024	Annual Review. Update of “Related Documentation”.	Raymond Girdler, State IT Security Specialist