CSCU

Risk Assessment (RA)

Purpose:

The following standards are established to support policy statement 10.1 that "CSCU will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information."

Scope:

1. All Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.

2. All Connecticut State College and University institutional units' information systems.

Standard:

1. Security Categorization [NIST 800-53r4 RA2]

For All Information Systems

1.1 The Data Owner in coordination with the Information System Owner, categorizes information and the information system in accordance with the "***Information System and Data Categorization Process***";

1.2 The Information System Owner documents the security categorization results (including supporting rationale) in the system security plan for the information system; and

1.3 The ISSO reviews and approves the security categorization decision.

2. Risk Assessment [NIST 800-53r4 RA3]

For All Information Systems

2.1 The ISSO 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;

a.) Prior to information system implementation and with completed system security plan;

b.) Prior to significant changes to authorized information systems;

c.) Upon discovery of new vulnerabilities through incident response, or otherwise;

d.) At the request of Authorizing Officials, or Authorizing Official Designees, for system security plan authorization purposes;

e.) ISPO security control assessments;

f.) As needed based on CSCU CIO or CISO request.

2.2 The ISSO documents risk assessment results in the information system security plan, risk assessment report;

2.3 Authorizing Official, or Designee, review risk assessment report results;

a.) Prior to authorizing use of information system; and

b.) Prior to authorizing significant changes to already authorized information systems;

2.4 The ISSO disseminates risk assessment results to the Information System Owner, Data Owner(s), and Authorizing Officials, or their Designees, for the Information System; and

2.5 The ISSO updates the risk assessment reports biennially or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. Vulnerability Scanning [NIST 800-53r4 RA5]

For All Information Systems

3.1 The Information System Owner ensures scans for vulnerabilities in the information system and hosted applications are performed;

a.) When new vulnerabilities potentially affecting the system/applications are identified and reported; and

b.) For information systems categorized as low (L);

- Every 30 days;

c.) For information systems categorized as moderate (M);

- Every 14 days;

d.) For information systems categorized as high (H);

- Every 7 days;

3.2 The Information System Owner employs vulnerability scanning tools and techniques that must;

a.) Support SCAP version 1.2 or greater compliancy;

b.) Facilitate interoperability among tools, including;

- Asset\Inventory Management Systems;
- Security Event Management Systems;
- Incident Response Procedures;
- Patch and Configuration Management Systems; and
- Electronic Messaging and Notification systems;

c.) Automate components of vulnerability management, including;

- Updating the scanning tools vulnerability repository;
- Identify and document all platforms, and software on the information system;
- Create a vulnerability remediation schedule by prioritizing vulnerabilities based on assessed overall risk;
- Track and document remediation plans and status;
- Report results of the vulnerability management process to the Information System Owner and ISPO.

d.) Analyze identified vulnerabilities based on;

- The impact of the vulnerability on the information system;
    a. CVSS Base score: 0.0-3.9 – L
    b. CVSS Base score: 4.0-6.9 – M
    c. CVSS Base score: 7.0-10.0 - H
- Threat intelligence;
    a. Reliable, widely available exploit code is available and actively in use or no exploit code is required to exploit the vulnerability - H
    b. Functional exploit code exists, but is not always reliable and is not widely available - H
    c. Limited function proof of concept code is available but would require substantial modification for use by an attacker - H

d. A theoretical exploit exists, but exploit code is not available - M

e. Attempts to exploit the vulnerability are seen in continuous monitoring – H

f. Attempts to exploit the vulnerability are not seen in continuous monitoring – M

g. Attacks are currently reported by other organizations – H

h. Attacks are not currently reported by other organizations - M

- Exposure;

a. No compensating controls are available to reduce the likelihood of the successful exploit of a vulnerability - H

b. Compensating controls partially reduce the likelihood of the successful exploit of a vulnerability (e.g. by increasing the difficulty of successfully exploiting the vulnerability) - M

c. Comprehensive compensating controls provide close to the same effect as remediating the vulnerability - L

e.) Assign overall risk score for each identified vulnerability using;

- Impact x (Threat Intelligence x Exposure) = Overall Risk Score.

f.) Enumerate the information system platforms, software flaws, and improper configurations;

- Enumerate information system platforms using the Common Platform Enumeration (CPE);
- Enumerate information system software flaws using the Common Vulnerabilities and Exposures (CVE);
- Enumerate improper configurations based on the Common Configuration Enumeration (CCE)

g.) Formatting checklists and test procedures;

h.) Capability to readily, and automatically, update the information system vulnerabilities to be scanned: [NIST 800-53r4 RA5 (1)]

- Daily;
- Prior to a new scan;

- When new vulnerabilities are identified and reported.

i.) Capable of privileged access authorization vulnerability scanning activities.

3.3 The Information System Owner reviews vulnerability scan reports and approves and documents remediation plans;

3.4 The Information System Owner approves and documents roles, and individuals assigned to those roles, allowed to run privileged access authorization scanning activities;

3.5 The Information System Owner ensures legitimate vulnerabilities are prioritized and remediated in a timely manner in accordance with assessment of risk;

a.) For information systems categorized as low (L)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within thirty (30) days.
- Vulnerabilities identified with an overall risk score of moderate (M) or low (L) must be remediated within ninety (90) days.

b.) For information system categorized as moderate (M)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within fourteen (14) days.
- Vulnerabilities identified with and overall risk score of moderate (M) must be remediated within thirty (30) days.
- Vulnerabilities identified with an overall risk score of low (L) must be remediated within sixty (60) days.

c.) For information systems categorized as high (H)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within seven (7) days.
- Vulnerabilities identified with an overall risk score of moderate (M) must be remediated within fourteen (14) days.
- Vulnerabilities identified with an overall risk score of low (L) must be remediated within thirty (30) days.

3.6 The Information System Owner must share information obtained from the vulnerability scanning process and security control assessments with the ISPO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Refer to the Glossary of Terms located on the website.

References

ITS-04 CSCU Information Security Policy

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.