8020.S001 Information Security Risk Management – Risk Assessment Standard

Implements:	CSU Policy #8020.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8020.0.shtml

Introduction

A campus must develop a process for assessing risks to its information assets. These assessments must be based on established severity and likelihood criteria and managed through ongoing evaluation and review activities.

1.0 Risk Assessment Criteria

Each campus must use a risk assessment model based on established criteria (see Appendix A). The campus must not alter the severity or likelihood classifications contained in Appendix A, but the campus may add criteria and/or numeric weighting based on its unique environment or circumstance.

2.0 Formal Risk Assessment Process

2.1 Establish Criteria

Each campus must establish and document two forms of formal risk assessment criteria. These criteria must be adequately communicated to campus departments:

- Criteria for situations in which a formal risk assessment must be performed (i.e. HIPAA, PCI, protected level 1 data, etc.).
- Criteria for situations in which a formal risk assessment may be necessary as determined by the ISO. If a project meets this criteria then the ISO must be notified about the proposed information asset change or acquisition. The ISO will determine whether a formal assessment needs to be performed.

2.2 Identify Formal Risk Asessment Methodology

Working with the procurement, project teams, change management groups and others as appropriate, campuses must establish and maintain a process for identifying information assets on which established criteria is used to determine if a formal risk assessment is required.

2.3 Required Elements of Formal Risk Assessment

Recognizing that risk assessment activities may vary depending on the nature of the risk being assessed, the following elements must be included:

a) Review Frequency

Formal risk assessments must identify a review cycle to ensure that risk management remains appropriate and effective. The length of the review cycle must comply with all applicable laws, policies, standards, and contracts. (For example, the length of the review cycle for PCI and HIPAA risk assessments must not exceed two years.) The review cycle for systems which were identified as "critical" must not exceed three years.

b) Risk Exposure
Each formal risk assessment must use the established risk assessment criteria (See Appendix A) to establish a risk exposure for the identified system, process, asset, etc.

c) Documentation and Retention
Written records of the formal risk assessment and supporting materials must contain sufficient detail to facilitate periodic review and must be retained for a minimum of 3 years.

d) Approval
The campus ISO is responsible for approving the formal information security risk assessment.

3.0 Informal Risk Assessment Process

Informal risk assessments may be used for those systems, assets, processes, etc. not considered critical to the organization and/or which fail to meet the criteria for formal risk assessment. Records of informal risk assessments may be in the form of email or other notes and should contain a statement of the dependencies, premises and facts upon which the opinion is based.

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
0.1	11/25/14	Macklin	First draft – ISAC development team	All
0.3	2/6/14	Macklin	Incoroprated team comments	2
.4	3/10/15	Macklin	Incorporated team comments	2
.5	4/28/15	Luvisi	Incorporated CISO comments	2.3
.6	4/29/15	DeCato	Made Cosmetic changes like font type and size	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
6/3/15	Perry (CISO)	Reviewed: Submitted to ITAC/ISAC. Review Timeframe: 6/11/15 until 7/11/15
7/13/15	Perry (CISO)	Approved for Posting

------APPENDIX A-------------------

Severity Scale (derived from SANS)

Critical - May allow full access to or control of the application, system, or communication including all data and functionality.

- The attacker is not limited in access after execution, they may be able to escalate privileges.
- Possible disclosure of 500 or more records containing sensitive or confidential information.
- Allows modification or destruction of all critical/sensitive data.
- Total shutdown of a critical service or services.

High - May allow limited access to or control of the application, system, or communication including only certain data and functionality.

- The attacker can access the sensitive data or functionality of a user, either limited to a specific piece of data and/or a specific user.
- An outside attacker can execute arbitrary code at the level of the user.
- Ability for a user to access unauthorized functionality.
- Allows limited modification or destruction of critical/sensitive data, either limited to a specific piece of data and/or a specific user.
- Severe degradation of a critical service or services.
- Exposure of sensitive system or application information that provides implementation details that may be used to craft an exploit.
- Breach may be difficult to detect.

Moderate - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Weaknesses that can be combined with other vulnerabilities to have a higher impact.
- Disclosure of information that could aid an attacker.
- Any vulnerability that can hinder the detection or investigation of higher impact exploit.
- Fines greater or equal to $10,000 and less than $50,000.

Low - May indirectly contribute to unauthorized activity or just have no known attack vector. Impact may vary as other vulnerabilities or attack vectors are identified.

- Deviation from a recommended practice or emerging standard.
- May be the lack of a security process or procedure to govern or manage security related activities.
- No direct exposure of data.
- Fines less than $10,000.

- Would not contribute to the exposure of confidential information.
- Would not enable alteration of stored records.
- Would not impact the availability of critical campus systems.

Likelihood Scale

Very High - Exposure is apparent through casual use or with publicly available information, and the weakness is accessible publicly on the Internet.

- Can be exploited by large anonymous population (Any Internet host).
- Vulnerability can be exploited from the general Internet.
- Possible with only publicly available information.
- No specific attack skills are required, such as general user knowledge.

High - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

- Can be exploited by extended campus population (students, guests)
- Can be exploited by anyone that can reach the network, no authentication required.
- Vulnerability can only be exploited from related networks to which the organization does not control access. (vendors)
- Simple (easily guessable) authentication may be required for exploit.
- Possible with limited knowledge of target configuration.
- Basic attack skills are needed, such as an automated attack (i.e. there exists a metasploit module, or known attack)

Moderate - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

- Can be exploited by a limited and known population.
- Vulnerability can be exploited through the internal company network or client connection only.
- Simple authentication is required for exploit.
- Vulnerability requires a user to be 'tricked' into taking some action (e.g. a targeted phishing message or a request to go to a website and download a file).
- Possible only with detailed internal information or reasonable guessing.
- Expert technical knowledge is needed such as knowledge of available attack tools.

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.

- Threat source is employee
- Vulnerability can be exploited through the internal campus network only.
- Single strong authentication is required for exploit.
- Possible only with a significant amount of guesswork or internal information.
- Vulnerability can be exploited with local physical access only and resources have physical access controls, but are still accessible to a large number of people.

Negligible - The threat-source is part of a small and trusted group or controls prevent exploitation without physical access to the target or significant inside knowledge is necessary, or purely theoretical.

- Small and trusted population.
- Vulnerability can be exploited with local physical access only and resources have strong physical access controls.
- A series of strong authentications or multi-factor authentication are required for exploit.
- Possible only with a significant amount of likely detectable guesswork or tightly controlled internal information.
- Attack is theoretical in nature and no known exploit or potential of exploit is currently proven or expected.

Risk Exposure Mapping

		Severity			
		Critical	High	Moderate	Low
Likelihood	Very High	Critical	Critical	High	Moderate
	High	Critical	Critical	High	Low
	Moderate	High	High	Moderate	Low
	Low	Moderate	Moderate	Low	Low
	Negligible	Low	Low	Low	Low