OIS Risk Assessment Process [1]

Information systems and processes have become critical to the success of organizations. University of Colorado (CU) relies on information systems for every aspect of its operations including academics, management, research, and infrastructure. The diverse nature of university operations requires handling various types of data including sensitive information such as student records, faculty and staff records, financial records, research data, and health information.

An important step in protecting the university information assets is to understand the risk they are subjected to, and address those risks appropriately based on business needs, cost-benefit considerations, regulatory and legal requirements. Risk assessment is a critical component of organizational risk management. Risk assessments conducted by OIS aim to identify, prioritize, and estimate risk to organizational functioning, assets and individuals from the operation of information systems and processes.

The CU OIS Risk Assessment and remediation process is based on NIST (SP 800-30 Rev1, 800-37, 800-39, 800-53, 800-60), SANS, and ISACA guidelines. It is important to remember that every risk assessment is different in nature and customizations will be made to the assessment and remediation process on a case-by-case basis. However, this page describes the general process that will be followed for conducting risk assessments.

The following steps outline the OIS Risk Assessment process:

1. **Define Risk frame including purpose, scope, boundaries, data flows, system/process encironment, owners, assumptions, constraints, and expectations from the assessment.**
2. **Identify Threat sources and events.**
3. **Identify Vulnerabilities based on Pre-disposing conditions, threat capability and control analysis.**
4. **Determine Likelihood based on Threat Event Occurance and Vulnerability level.**
5. **Impact Determination.**
6. **Risk Determination.**
7. **Risk Assessment Report and Recommendations.**

1. Risk Frame

Defining the Risk frame accurately is essential to the success of the assessment. This step ensures that all the relevant entities initiating or affected by the assessment are on the same page with regards to scope, purpose, and expectations from the assessment. Another component of this step is to get a general characterization of the system or process and the necessary stakeholders. After an initial meeting with the information system/process owner, all the stakeholders will be informed of the beginning of the assessment.

Purpose and Scoping questions along with an in-person meeting with the stakeholders of the assessment will be used to address the first step. The following is a sample of Purpose and Scoping questions. These will be revised to address unique nature of individual cases.

Purpose and Scoping Questions

- What is the purpose of the assessment?
- What is the scope of the assessment?
- What is the mission of the organization?
- Who are the system/process owners/authorizing officials?
- Who are the users of the system/process?
- What is the primary purpose of the system/process in relation to the mission?
- Are there policies, standards or guidelines that address the mission and system/process?
- What is the Security Category (Criticality and Sensitivity) of the System with regards to Confidentiality, Integrity and Availability?
- How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?

- Overview of the system/process? (Network diagrams, flowcharts, architectural representations, etc.)
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g. student, financial, personnel, research and development, medical, command and control)?
- Where specifically is the information processed and stored? What are the types of information storage?
- Could a system or security malfunction or unavailability result in injury or death?

2. Threat and Events

OIS Risk assessment will evaluate the existing Technical, Operational and Management

Controls.

These controls contribute to defense against the various threats that information systems, processes, and assets are subjected to. Threats can be explained in the context of a threat source (Adversarial, Accidental, Structural and Environmental) and associated threat events (Access sensitive information through network sniffing, accidental spilling or mishandling of sensitive information by authorized user). The framing of the assessment will include expectations related to the threat sources against which the assessment is conducted. OIS will use the threat source and event information primarily from NIST SP 800-30 Rev 1. However, information from other sources such as REN-ISAC, industry bulletins and technology vendors may also be used for this purpose.

3. Vulnerabilities and Pre-disposing Conditions

The primary purpose of this step in the assessment is to understand the nature and degree to which the organization is vulnerable to the threats identified in the previous step. Vulnerabilities can exist in all types of controls (technical, operational, and management). Control analysis (non-existent, ad-hoc, implemented, documented, monitored) therefore plays an important role in understanding the degree of vulnerability to the threats thereby influencing the likelihood determination. OIS will work with the necessary stakeholders and through a rigorous process which may include interviews, questionnaires, scans, process and architectural analyses determine the state of vulnerabilities that could be exploited by the threat sources. Predisposing conditions that exist within the organization (including business processes, information systems and environments of operations) can contribute to the likelihood that one or more threat events initiated by threat sources result in severe adverse impact to university assets and resources. Based on the capability of threat sources and control analysis, the following are the three vulnerability levels:

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

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

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.

4. Likelihood Determination

The Likelihood determination is made based on a combination of occurrence of threats and degree of vulnerability to those threats. OIS categorizes threat occurrences in the following manner to determine likelihood:

High: Threats have been observed frequently in higher education, healthcare and other relevant industries within the last 3 years

Moderate: Threats have been observed occasionally in higher education, healthcare and other relevant industries within the last 3 years

Low: Threats have been observed rarely in higher education, healthcare and other relevant industries within last the 3 years

Based on the nature of the assessment, OIS will use qualitative or semi-quantitative technique to determine likelihood. The analysis of likelihood will be represented by three levels (High, Moderate, and Low). The semi-quantitative analysis will rely on a scale of 1-10 with 1 being the lowest level of likelihood of an adverse impact and 10 being the highest.

5. Impact Determination

Impact determination plays a crucial role to determining the level of risk. Impact will depend on the Security categorization of the information system and the information type involved. For any information type, a level of impact is assigned to each of three security categories. Following definitions are defined for security categories:

Confidentiality— "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.

Integrity — "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.

Availability— "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

The impact levels are defined as low, moderate and high. E.g. of Security Category for a funds control system could be represented as Security Category funds control = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (2) result in major damage to organizational assets; (3) result in major financial loss; or (4) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

CU uses the following as guides for defining impact:

- Financial – direct or indirect monetary costs to the institution where liability must be

transferred to an organization which is external to the campus, as the institution is unable to incur the assessed high end of the cost for the risk; this would include for e.g. Use of an insurance carrier
- Reputation – when the impact results in negative press coverage and/or major political pressure on institutional reputation on a national or international scale
- Safety – when the impact places campus community members at imminent risk for injury
- Legal – when the impact results in significant legal and/or regulatory compliance action against the institution or business.

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (2) result in significant remediation cost to the university.

CU uses the following as guides for defining impact:

- Financial – direct or indirect monetary costs where liability is transferred to the campus as the business unit/school is unable pay the assessed high end cost for the risk
- Reputation – when the impact results in negative press coverage and/or minor political pressure on institutional reputation on a local scale
- Safety – when the impact noticeably increases likelihood of injury to community member(s)
- Legal – when the impact results in comparatively lower but not insignificant legal and/or regulatory compliance action against the institution or business.

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (2) result in minor damage to organizational assets; (3) result in minor financial loss; or (4) result in minor harm to individuals.

CU uses the following as guides for defining impact:

- Financial – impact results in direct or indirect monetary costs to the institution where business unit/school can solely pay the assessed high end of the cost for the risk
- Reputation – when the impact has a nominal impact and/or negligible political pressure on institutional reputation on a local scale
- Safety – where the impact has nominal impact on safety of campus community members
- Legal – when the impact results in none or insignificant legal and/or regulatory compliance action against the institution or business.

For the purposes of semi-quantitative analysis a scale of 1-10 will be used with 1 being the lowest level impact and 10 being the highest.

6. Risk Determination

Risk is determined from the combination of likelihood and impact. The following are the levels of risk which will be included in the final assessment report. OIS will work with the necessary stakeholders to draft a risk mitigation plan and/or risk acceptance document.

High Risk: There is a strong need for corrective measures. A corrective action plan must be put in place as soon as possible. The system/process owner needs to make a decision on accepting the risk or initiating a corrective action plan within 30 business days of the formal submission of the report.

Moderate Risk: Corrective actions are needed and a plan must be developed to incorporate these actions within a defined reasonable period of time.

Low Risk: Corrective actions are recommended

7. Risk Assessment Report and Recommendations

The last step in the process is the preparation of a risk report that contains the findings from the assessment, the level of risk and the recommended controls to mitigate the risk. OIS will deliver the report to the information system/process owner or their designee. Depending on the level of risk, OIS will work with the stakeholders to implement a mitigation plan and/or obtain a risk acceptance statement.

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/ois-risk-assessment-process