Computer Services and Information Technology

Information Technology Security

Risk Management Program

Introduction

Risk management is a process to identify, assess, manage and control potential events to provide reasonable assurance regarding the achievement of business objectives. The risk management process has five key objectives:

- Identify and prioritize risk arising from business strategies and activities
- Determine the level of risk acceptable to the university (risk appetite)
- Design and implement risk mitigation activities designed to reduce risk
- Perform on-going monitoring activities to re-assess risk and the effectiveness of controls
- Communicate periodic risk management process reports to management

The risk management process should not be treated primarily as a technical function carried out by IT staff, but as an essential management function of the university. The principle goal of the Information Technology Security Risk Management Program is to protect IT assets and the university's ability to carry out its mission in the face of potential threats to its IT assets.

Purpose

The purpose of the IT Security Risk Management Program is to:

- Comply with the Board of Regents policy (712.03 – Institutional Responsibilities), as well as other state and federal regulations, to develop, implement, and maintain a security plan with appropriate and auditable security controls;

- Provide a governance framework for understanding potential risks to IT assets based on the security plan;

- Provide guidelines for evaluating and documenting the management, operational and technical security environment of IT assets; and

- Provide management with direction, planning, and guidance in the area of information security

Scope

The scope of the IT Security Risk Management Program includes physical and logical perimeter of the SSU local-area network. The Program will assess tangible and intangible assets (e.g., people, data, facilities, technology) as well as the effectiveness of security controls (e.g., management, operational, technical).

Risk Assessment Approach

The risk assessment approach uses qualitative risk analysis techniques, relying on subjective judgment, to determine the overall risk to IT assets. Qualitative risk analysis techniques employ the product of two elements, the likelihood of an event occurring and the impact should it occur, to determine risk ratings, expressed in terms of low, medium and high.

The risk assessment approach follows the Control Objectives for Information and Related Technology 4.1 (COBIT) framework. Other risk management frameworks referenced include:

- National Institute of Standards and Technology (NIST)
- Capability Maturity Model (CMM)

Phase 1 - Identify and Understand IT Strategy

A fundamental element of risk assessment is to gain an understanding of the business objectives and to determine how IT is used to support the achievement of those objectives. Defining an IT universe provides an inventory of key computing environment components to determine which IT areas pose a business risk. IT universe elements are classified under five categories:

- *Strategic* - high-level goals, aligned with and supporting its mission
- *Operations* - effective and efficient use of IT resources
- *Compliance* - compliance with applicable laws and regulations
- *Reporting* - reliability of reporting
- *Data Classification* – the level of sensitivity (confidential, sensitive, public)

Phase 2 – Inherent Risk Assessment

Risk is defined as the likelihood of an event occurring and the potential impact it may have on the achievement of business objectives should it occur. Inherent risk is the risk related to the nature of an objective before internal controls are applied. Based on the ISO/IEC 27002 framework, the likelihood and impact are assessed for each identified risk and calculated using a weighted matrices approach with a rating scale, expressed in terms of low, medium and high.

Each identified risk is assigned a risk response that determines how the risk will be handled:

- *Accept* – acknowledge the risk's existence, but take no preemptive action
- *Reduce* – implement internal controls to mitigate the risk
- *Transfer* – share the risk (e.g., insurance, third-party contract)
- *Avoid* – eliminate the condition that allows the risk

Identified risks assigned a "high" risk rating may not have a risk response of "accept". Acceptable risks must be supported by a validated business case and reviewed in conjunction with the risk assessment cycle.

Phase 3 – Internal Control Assessment

An effective internal control environment provides reasonable assurance regarding the effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations. Internal control activities are actions, supported by policies, which help to increase value and reduce risk.

Phase 4 – Residual Risk Assessment

Residual risk is defines as the risk remaining after internal controls have been applied. Based on the residual risk identified from the control activity, the likelihood and impact are calculated using a weighted matrices approach with a rating scale, expressed in terms of high, medium and low.

Phase 5 –Risk Assessment Results

Results from the risk assessment are expressed using a heat map showing the inherent risk levels of the IT universe across four domains: strategic, operational, compliance and reporting, using the following risk ratings:

High Risk	🟥
Medium Risk	🟨
Low Risk	🟩

Phase 6 – Risk Mitigation and Monitoring

Risk mitigation involves evaluating and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Based on a cost-benefit analysis, the recommended control will be prioritized and assigned to a responsible party for implementation. Risks will be monitored based on a 3-year review strategy:

High Risk	Reviewed annually
Medium Risk	Reviewed every 2 years
Low Risk	Reviewed every 3 years