| | | | | |
|---|---|---|---|---|
| جامعة الشارقة UNIVERSITY OF SHARJAH | Policy Main Title | Information Technology | Effective Date | 30/5/2021 |
| | Policy Subject | Information technology Risk Management Methodology | Last Review date | 19/5/2021 |
| | Policy Number | IT-20 | Next Review date | 19/5/2022 |
| | Responsible Entity | IT Center | Approved By | VC for Financial & Admin. Affairs |

**Overview**

A systematic approach to information security risk management is necessary to identify enterprise needs regarding information security requirements and to align with Sharjah University Security Risk Management Framework. Information technology Risk Management should identify and mitigate risks in an effective and timely manner where and when they are needed. ISRM should be an integral part of all information security management activities.

**Scope**

The scope of this methodology documents, the information security risk assessment, identification of mitigation plans and closure of identified information security risks. The procedure is based upon the, ISO/IEC 31000 enterprise risk assessment framework. The processes documented in this methodology shall be used in performing information security risk assessments for all the services of UoS. The scope applies to all the information assets, technology infrastructure, information security practices, human resources, business processes and functions involved in managing and supporting the IT environment.

All associated information resources (information assets, people, processes etc...) that store, process and transmit data shall be included in the scope of the information technology risk management;

When defining the scope of risk assessment, the below shall considered.

1. University of Sharjah strategic objectives, strategies and policies
2. Critical Business/ Academic processes
3. Legal, regulatory, accreditation and contractual requirements applicable to UoS
4. UoS information security policy
5. Internal and external academic services offered

**Purpose**

Information Security Risk Management objectives:

1. To assess and appropriately treat the risks associated with UoS services and information assets.
2. To implement security controls on the Information systems that store, process, and transmit the university's information.
3. To enable management to make well-informed decisions based on the criticality of risks related to information security.
4. To enable the university to continually improve the risk posture of the services and information asset.

5. To ensure that a common and approved methodology is followed throughout UoS while performing Security Risk assessment on the university's services.

**Abbreviations**

ISRM - Information Security Risk Management

UoS – University of Sharjah

**Definitions**

**Availability:** Part of the Information Security Triad; availability means that information should be available when needed.

**Control:** Managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature (Note: Control is also used as a synonym for safeguard or countermeasure).

Information asset: Any information or information processing facility that has value to the organization.

**Information security:** The act of protecting information that may exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

**Inherent risk:** The susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls. Because the potential for material errors in IS areas with no controls in place is usually high, the inherent risk is usually high.

**Integrity:** Part of the Information Security Triad; integrity means that the data should not be modified without authorization, intentionally or unintentionally.

**Potential risks:** The risks that remains associated with information assets even with the presence of existing controls is commonly known as potential risks, and which requires to be treated appropriately.

**Residual risk:** The remaining potential risk after all IS security measures are applied. There is a residual risk associated with each threat.

**Risk:** Risk is the quantifiable likelihood of potential harm that may arise from a future event.

**Risk assessment:** Risk assessment is a step in the risk management process to determine the qualitative and quantitative value of risk in relation to a recognized threat.

**Risk evaluation:** Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

**Risk management:** The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect an organization's resources.

**Risk treatment:** Risk treatment – also known as risk control – describes the part of risk management in which decisions are made about how to treat risks that have been previously identified and prioritized. Options for risk treatment may include risk avoidance, risk reduction, risk transfer or risk acceptance.

**Risk Owner:** The individual or group of people in an organization with the accountability and authority to manage & treat risks.

**Threat:** Threat is the expressed potential for the occurrence of a harmful event such as an attack. It could be any party with the intent and capability to exploit vulnerability in an asset such as a malicious hacker or a disgruntled employee.

**Threat assessment:** Evaluating a threat whether it is applicable to the environment under consideration and if applicable, what would be its strength or force by which it might be affecting a service?

**Vulnerability:** A weakness in the system security procedures, system design, and implementation or internal controls, which can be triggered or intentionally exploited and result in a violation of the system's security policy.

**Vulnerability assessment:** A measurement of vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount.

**Information Security Risk Management Methodology**

The Information Security Risk Methodology stages are as below:

Risk Identification

1. Identification of threats and Vulnerabilities to the services
2. Identification of current controls

Risk Analysis

1. Risk Impact value
2. Likelihood of occurrence

Risk Evaluation

1. Verify with acceptable level of risk.
2. Identify risks that need to be treated

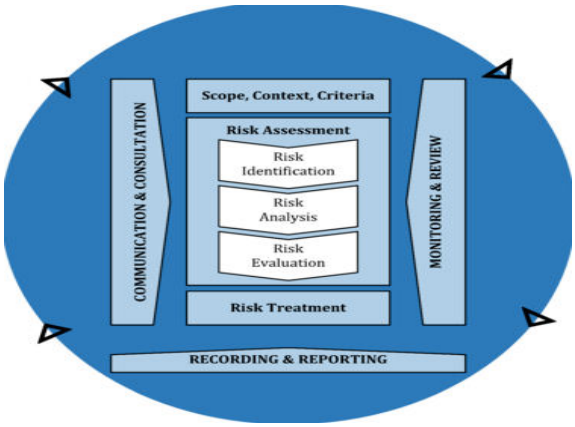
Risk Treatment

1. Mitigate
2. Transfer

3. Avoid
4. Accept

**Framework**

The information security risk management methodology of the University of Sharjah is set to identify the services and assess the risk and the risk exposure according to the academic needs. The below chart demonstrates the ISO 31000 framework and the steps to be followed for an effective information security risk management program.




**Risk Identification**

A risk is defined as a threat that has exploited a vulnerability against a service or process.

A threat is an undesirable event that could cause harm to a service or a process by violating its security.

A threat exploits vulnerability in a system, process, or procedure to launch an attack on services and processes. Threats are related to vulnerabilities because a threat without an associated vulnerability does not pose any risk to services and processes. Vulnerability level depends on complexity and current controls. All components are individually examined to identify vulnerabilities that can be exploited by threats.

The risk of an unwanted event occurring depends on the criticality of the services and processes and the threat and vulnerability present to them. The primary method for identifying risks is to address the following questions for each service or process:

a. What known threats to the asset exist and exploit the known vulnerabilities?
b. What can go wrong?

This process results in a detailed explanation of the risk context, identifying the threat and the vulnerability that could lead to its occurrence. Risks shall also be divided into the following categories:

1. Risks related to operations

2. Risks related to people
3. Risks related to information
4. Technology Risks:
    a. Software
    b. Physical assets

**Risk Analysis**

Risk assessment process includes evaluation of likelihood and severity of risk actions associated with services and processes. The actual risk analysis involves creation of various matrices and tables to arrive at a measurable value of risk. As various information securities best practices highlight, there is no right or wrong methodology of conducting the risk analysis. However, the risk methodology must be able to provide comparable and reproducible results. To assess the risks, following questions should be addressed:

1. What would be the severity if an event did occur?
2. What is the likelihood that the risk will occur?
3. What is the Risk Level, given the likelihood and severity?

**Risk Impact**

Severity or Impact is the result of successful risk action against a service or a process. It is related to their importance and criticality which is determined from the level of required protection. In simple terms, severity is the worst potential result of an event that has occurred due to a threat and vulnerability pair.

| RATING | DESCRIPTION |
|---|---|
| **Catastrophic** | Prolonged system unavailability affecting long term viability |
| | In excess of $2M loss |
| **Major** | System unavailability affecting business cycles |
| | $500,000 to $2M loss |
| **Moderate** | system unavailability but recoverable within business cycles |
| | $100,000 to $500,000 loss |
| **Minor** | System unavailabilty affects service quality |
| | $10,000 - $100,000 loss |
| **Insignificant** | System unavailability causes inconvenience |
| | < $10,000 loss |

**Likelihood of occurrence**

The Likelihood of occurrence is defined as probability of any incident occurring at a particular period of time. This is a vital parameter in determining the risk value. The threat and vulnerabilities always exist but probability of occurrence of the incident resulting from that pair finally determines the risk level and the importance to be given to the operation.

| LIKELIHOOD | | CONSEQUENCE | | | | |
|---|---|---|---|---|---|---|
| | | 1 Insignificant | 2 Minor | 3 Moderate | 4 Major | 5 Catastrophic |
| A - | Almost Certain | Medium | High | High | Extreme | Extreme |
| B - | Likely | Medium | Medium | High | High | Extreme |
| C - | Possible | Low | Medium | High | High | High |
| D - | Unlikely | Low | Low | Medium | Medium | High |
| E - | Rare | Low | Low | Medium | Medium | High |

**Risk Value**

The risk value for each threat action is calculated based on the following equation

**Risk Value = Impact Factor X Likelihood of Occurrence**

**Risk Owner**

Risk Owners are identified individuals accountable for the management of risk, to ensure that risk is under the acceptable level. They are responsible for implementing the mitigation strategy for the identified information security risks.

As a rule of thumb, it is assumed that the risk owners will put in effort to treating the risk by applying the right controls before looking at other treatment options. Each identified risk shall be assigned to a Risk Owner, who shall be responsible to ensure that appropriate mitigation strategy, controls and treatment plans are implemented for the risk, to reduce it to an acceptable level.

**Risk Treatment**

Risk Treatment planning is a process of deciding the steps that needs to be taken to reduce threats and take advantage of the opportunities discovered during the risk analysis. The detailed risk mitigation plans / strategies are generally developed for those risks which have high probability of occurrence or which can cause severe impact to the business.

The strategy for treating the risk falls into one of the following categories:

1. Accept Risk: Not to set any new / additional controls
2. Mitigate Risk: New / additional controls to reduce the likelihood of its occurrence or its impact
3. Transfer Risk: Outsourcing or insuring against a risk to compensate for its repercussions if it occurs
4. Avoid Risk: Cancelling the process or service in order to avoid the risk

The objective is to identify the high-risk threats and introduce countermeasures to reduce the likelihood or the severity. The risk management strategy should include plans for implementation and deployment of the identified countermeasures.

**Risk Acceptance**

While finalizing an approach to treat the risk encountered, it is important to have a criterion based on which an informed decision can be taken by the management to suitably treat the risks encountered and decide as to how the organization should respond to the risks encountered. Thus, based on the criteria given below, the risk found initially or the residual risk remaining after the implementation of controls can be suitably treated.

The risk value outcome has been categorized on the basis of criticality as shown and referred to as the risk rating. It is advisable to take appropriate risk mitigation actions on the basis of risk ratings.

| RATING | LEGEND |
|---|---|
| EXTREME | Improved actions, resources and strategies are required to be implemented IMMEDIATELY to reduce, transfer or control the level of risk |
| HIGH | Existing actions, resources or strategies must be modified AS SOON AS POSSIBLE to reduce, transfer or control the risk |
| MEDIUM | Take actions to reduce where benefit exceeds cost and / or continue to implement actions, resources and strategies to prevent and/or reduce the level of risk |
| LOW | MAINTAIN current actions, resources and strategies to prevent the escalation of the level of risk |

**Residual Risk**

The risk needs to be effectively treated which results in the reduction of the risk to an acceptable level, with minimal adverse impact. Practically, no information system is risk free, and not all implemented controls can eliminate the risk they are intended to address, or reduce

the risk level to zero. The risk remaining after the implementation of new or enhanced controls is the residual risk.

**Periodicity of Conducting Risk Assessment**

Risk assessment needs to be conducted periodically at least once a year to:

1. Identify the new risks
2. Identify the severity level of existing risks
3. Evaluate the effectiveness of implemented controls
4. Identify the need for new controls or adjusting/removing existing controls

The periodicity may depend on the following factors:

1. Frequency of changes in the infrastructure
2. Frequency of changes in business environment
3. Statutory requirements
4. Compliance requirements
5. Monitoring and Incident Analysis

**Continual Improvement**

In order to ensure the effectiveness of the Information Risk Management Framework, the continual improvement of the process is essential.

The Corrective and Preventive actions procedures need to be considered along with the information security policies and procedures, security objectives, audit results, analysis of monitored events and management review. As the university matures in terms of risk management, the acceptable risk value can be increased to a higher level to increase the level of security and to trigger the continual improvement process.

**Review of the Risk Management Framework**

This Information Risk Management Framework shall be reviewed at least once a year to suitably address the acceptable levels of risk and ensure the effectiveness of the framework to reflect the requirements of the operations.

The reviews will include adequacy and effectiveness of the Risk Assessment Methodology and Risk Treatment Strategies with regard to any identified significant changes in the university, changes in technology, changes in business / academic objectives and processes, changes in identified threats and changes in legal and regulatory situation. This information Risk Management Framework shall also be reviewed whenever there is a major change to the infrastructure and whenever there is a major incident.

The relevant committee shall conduct annual review of residual risks and arrive at an acceptable risk level for the period. Such reviews will include changes in the organization, changes in technology, changes in business objectives and services and processes, changes in identified threats and changes in legal and regulatory environment.

**References**


ISO 27001:2013 Information Security Management System Requirements.
ISO 31000:2018 Enterprise Risk Assessment Framework
ITIL V3.