Policy Title: Information Technology Services – IT Risk Management and Assessment Policy

Policy Number:

Established: March 2019

Approved by:

Last Approval Date:

Revision Date:

Position Responsible for Maintaining and Administering the Policy: Executive Director, Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

Policy Statement

The University of Windsor engages in a wide range of activities, both on and off campus, all of which give rise to some level of risk. As such, this Policy will require IT Services to:

- Embed risk management into the mission critical or other core IT systems
- Incorporate risk management aspects into planning activities and resource allocation decisions related to IT Services
- Manage IT risk and leverage opportunities in accordance with best practices
- Regularly re-assess the risk appetite of the University and effectiveness of IT risk management activities

Purpose

The University has established standard processes for IT risk management, including:

- Identification
- Analysis
- Evaluation
- Treatment

The approach to IT risk management allows risks to be correctly prioritized across all of the University's identified IT operations in order to bring awareness to potential issues and / or enable the organization to establish effective controls.

In summary, the IT Risk Management and Assessment Policy seeks to compliment other existing established University controls.

Scope

This Policy applies across the University for any IT services / products identified as critical for business continuity and / or services that contain / process inherently risky or confidential data. Consequently, this Policy applies to all administrative and academic units of the University that access or use identified IT services and applications.

Principles:

1. IT risk management explicitly addresses uncertainty, while creating and protecting value
   Risk is the effect of uncertainty and may have both positive and / or negative impacts on the outcome, which should be considered when identifying the required risk management to explicitly address this uncertainty. Risk management is expected to create and protect organizational value and as such, the resources necessary to mitigate risk should be less than the perceived consequences of inaction.

2. Risk management is tailored to IT Services processes
   As risk is an inherent part of the activities of IT Services, risk events will be considered within the context of the identified risk appetite when identifying mitigation strategies

3. Risk management is based on best available information and is responsive to change
   For any potential risk event, the risk will be managed in accordance with available information on the perceived consequence should the event occur and the probability of that occurrence. As the internal and external environment change, current risks will be reviewed and any new risks that are identified will be appropriately managed.

4. Risk management is inclusive and transparent
   Risk management activities will involve the necessary key stakeholders to reflect representative views, assure accountability and to facilitate the change required to meet identified goals

Responsibilities:

1. Information Technology (IT) Services has the responsibility to:
   - Enforce this Policy and is authorized to set specific / related guidelines and protocols
   - Oversee IT risk management activities within established guidelines of the IT Services Leadership Team
   - Assist with the creation of appropriate IT risk management procedures and measurement methodologies
   - Coordinate the monitoring of key IT risks and where appropriate, report on key risks and potential treatment plans to the appropriate University body
2. Client areas have the responsibility to:
   - Be aware of this Policy and take appropriate measures to ensure compliance
   - The extent required, manage and / or delegate responsibility for particular risks assigned for their respective areas
   - Actively identify risks and report them to their supervisor, especially during periods of change to processes or operational practices
   - Comply with all identified / approved risk treatment plans
3. IT Steering Committee has the responsibility to:
   - Regularly review this Policy
   - Provide feedback and guidance on this Policy
   - Approve amendments to this Policy

Exceptions to Policy

The Executive Director, IT Services may determine that certain situations or circumstances require exceptions to this Policy in order to best serve the interests of the University. Such requests should be communicated in writing to the Executive Director, IT Services and should include the exact nature of the exception and, if appropriate, the time period during which the exception should be granted.

Cross-References

None

Definitions

None

Procedures

Procedures for IT Risk Management and Assessment have been identified in the Appendix. In specific instances across the University where supplemental, more restrictive policies or procedures have been instituted, these more stringent requirements must be followed.

Review Process for Policy

This Policy will be reviewed at least every three (3) years. There may be certain circumstances that may cause for the review of the Policy prior to that date: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by Senior Management or the Board of Governors to review the Policy.

Process for Communicating Policy

The Policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

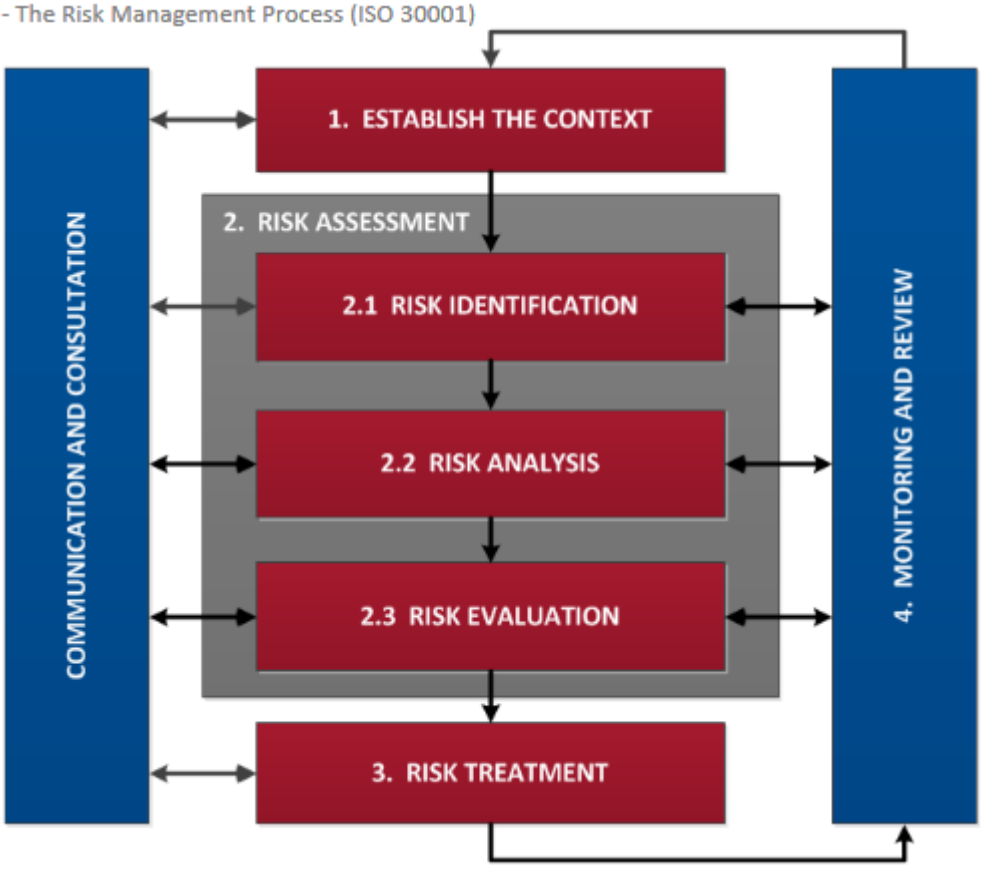
Contact Information

Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the Policy was developed, as per the contact information at the introduction of the Policy.

Appendix

The IT Risk Management and Assessment Policy utilizes the ISO 30001 process as outlined in Figure 1.

Figure 1 - The Risk Management Process (ISO 30001)



1. Establish the Context

   IT Services will establish context by articulating objectives and defining the parameters to be considered when managing IT risks, as well as set the scope and risk criteria for the balance of the process

2.1 Risk Identification

Risk identification requires reasonably foreseeable risks that have the potential to have meaningful impact on IT services to be identified. A risk is any event or action that has an uncertain effect that may impact on the objectives of the Department or University. Risks can arise as much from the possibility that opportunities will not be realized as they do from the possibility that threats will materialize, errors be made and / or damage will occur. All University Staff within the scope of this Policy should report any identified risks to their supervisor or via established project / activity processes.

In general, two types of risks will be identified:

1) Project

   These risks are generally associated with significant change or project activity and are normally identified at the commencement of the new activity or project. These risks may also be reviewed in a more formal manner as part of transition activities to operations.

2) Ad-Hoc (Operational)

These risks may be identified by staff during their normal University work. When risks are identified in this manner, staff must report them to a designated risk owner (i.e. Supervisor, Manager) who in turn shall:

- Determine whether immediate action is necessary to reduce the risk, and if safe to do so, carry out this action
- Document and report the risk as is required based on type / magnitude of risk

All identified risks will be tracked within the designated IT Services Service Management system. As a minimum, the following information regarding the risk shall be captured:

- The description of the risk, preferably a short, meaningful title such that the risk can readily be referred to in the future
- The causes of the risk
- The assigned risk owner

In addition, the following information if known, shall be included:

- The category of the risk
- Details regarding the existing controls in place to manage the risk, including temporary controls that are being used to manage the risk until further action is taken
- The inherent risk rating determined from the assessment of the potential consequences and likelihood for the risk

2.2 Risk Analysis

Risk analysis involves developing an understanding of the risk, providing an input to risk evaluation and to making decisions on whether risks need to be treated, and if so, on instituting the most appropriate risk treatment methods. This analysis can also provide input into options to address risks, as well as to inform the decision making required across different types and levels of risk. Risk analysis should also seek to identify potential causes and sources of risk in order to analyze their consequence and the likelihood that the consequence will occur.

All identified in scope risks within IT Services will be assessed using a common scale that will consider:

- The potential consequences if the risk were to occur, and
- the likelihood of the University being impacted

The consequence and likelihood will then be used to rank the risk in accordance with the following four categories (depicted in Figure 2): ***Extreme, High, Medium, Low***

Risk Rating Tables

Risk Matrix

		Consequences				
		1. Insignificant	2. Minor	3. Moderate	4. Major	5. Catastrophic
Likelihood	a. Almost Certain	Medium	High	High	Extreme	Extreme
	b. Likely	Low	Medium	High	High	Extreme
	c. Possible	Low	Medium	Medium	High	High
	d. Unlikely	Low	Low	Medium	Medium	High
	e. Rare	Low	Low	Low	Medium	Medium

This analysis, which is undertaken based on the existing status of the risk, with consideration of the controls that may already be in place, identifies the inherent risk. This common approach to risk rating is necessary to ensure that the most significant risks to the University can be readily identified and prioritized in a way that has the greatest overall benefit to the University.

2.3 Risk Evalulation

The purpose of risk evaluation is to assist in making decisions, based on the outcome of risk analysis, about which risks require treatment and to establish priority for treatment implementation. The rating of a risk, together with the risk appetite of IT Services, will be used to determine:

- The urgency with which action should be undertaken
- The nature of the action that is required
- The reporting requirements for the risk
- How the risk will be monitored

3. Risk Treatment

Selection of the most appropriate treatment options will involve:

- Balancing the costs and efforts of implementation against the benefits derived
- Considering the values and perceptions of impacted stakeholders
- Considering the secondary risks that may occur as a result of the treatment options

Treatment options shall consider:

1. Avoidance
   Opting to not proceed with the activity or choosing an alternative approach to achieve a similar outcome
2. Mitigation
   Improving management controls and procedures. Neutralize the consequence by improving management controls and / or procedures that minimize adverse consequences
3. Transfer
   Moving the risk to another more appropriate party
4. Acceptance
   Accepting that identified controls are appropriate, recognizing that these must be monitored

4. Monitoring and Review
   IT Services will plan to regular monitor and review identified IT risks and respond with necessary actions effectively manage risks