MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

ITM Risk Management Framework

Standard

Effective Date: February 26, 2015

Authority & Alignment

Authority: D1200 Code of Conduct, D3300 Internal Controls, D8000 ITM Governance and Management
Alignment: Cobit, ISO 31000:2009, ISACA RiskIT Framework 2009

Overview

"Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk". All activities of an organization involve risk. Organizations manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required."[1]

ITM risk is the risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

Adoption and use of an ITM risk management framework enables:

- The integration of ITM risk into the overall enterprise risk management (ERM) process of the University
- The identification of the ITM risk profile in the context of the risk tolerance of the University
- The effective management of ITM risk

Scope and Definitions

This standard applies to the assessment of the risk involved with the use of IT at MacEwan University. It will apply to IT Infrastructure, Application and Service risk.

Compliance & Exceptions

Responsibility for compliance with MacEwan policies and standards extends to all members of the MacEwan community. Non-compliance may create risk for MacEwan and will be addressed accordingly (see clause 4.5.1 "Respect for the law and University governance" of the University's policy D1200 Code of Conduct – Employees for additional guidance).

Standard Requirements

1. ITM Risk Management practices will be founded on the following principles[2]:
    a. ITM risk management activities always align to the University's strategic objectives.

[1] CAN/SCA-ISO 31000:2009-10 page v
[2] RiskIT Framework, 2009 ISACA

i. The approach to risk management is comprehensive and cross-functional.
ii. ITM risks are expressed in terms of the consequences they can have on the achievement of the University's objectives.
iii. ITM risk is evaluated in terms of protection against value destruction and of enabling value generation.

b. ITM risk governance aligns the management of ITM-related risk with Enterprise Risk Management:
i. The University's tolerance for risk is clearly defined.
ii. Risk reporting and assessment is consolidated across the University.
iii. Risk issues, principles and risk management methods are integrated across the University.

c. ITM governance should balance the costs and benefits of managing ITM risk.
i. Risk is prioritized and addressed in line with the University's tolerance for risk.
ii. Controls are implemented to address risk based on the University's tolerance for risk.

d. There should be open communication regarding ITM risk.
i. Open, accurate, and timely information on ITM risk is used as the basis for all ITM-related decisions.

e. A risk-aware culture is actively promoted throughout the University.

f. ITM risk management is continuously improved and is embedded in operating practices.
i. Management of ITM risk is an iterative process.
ii. ITM risks associated with changes in the University are identified in advance of the change, where possible.
iii. Risk assessment methods, roles and responsibilities, tools, techniques and criteria are reviewed periodically.
iv. Risk management practices are straightforward and easy to use.

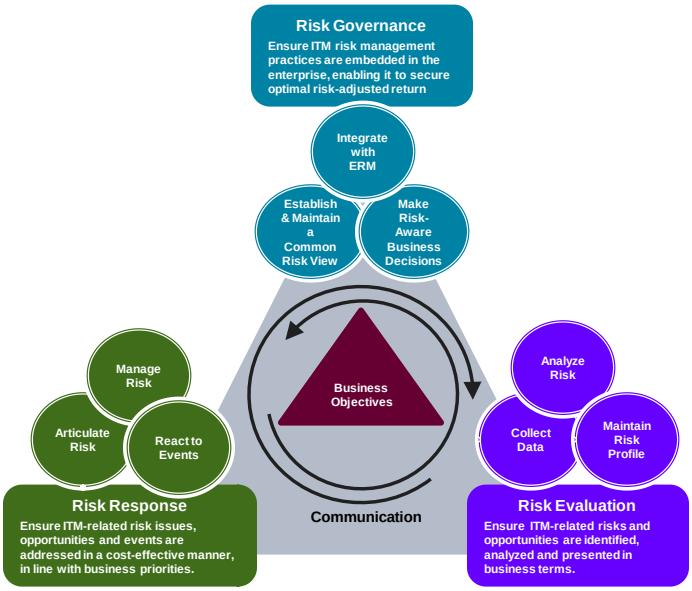
2. The ITM risk management framework includes the domains of risk governance, risk evaluation and risk response as shown in Figure 1.

a. Governance - ITM risk management practices are embedded in the day-to-day activities of the University.

b. Evaluation - ITM-related threats and opportunities are identified, analyzed and presented to management.

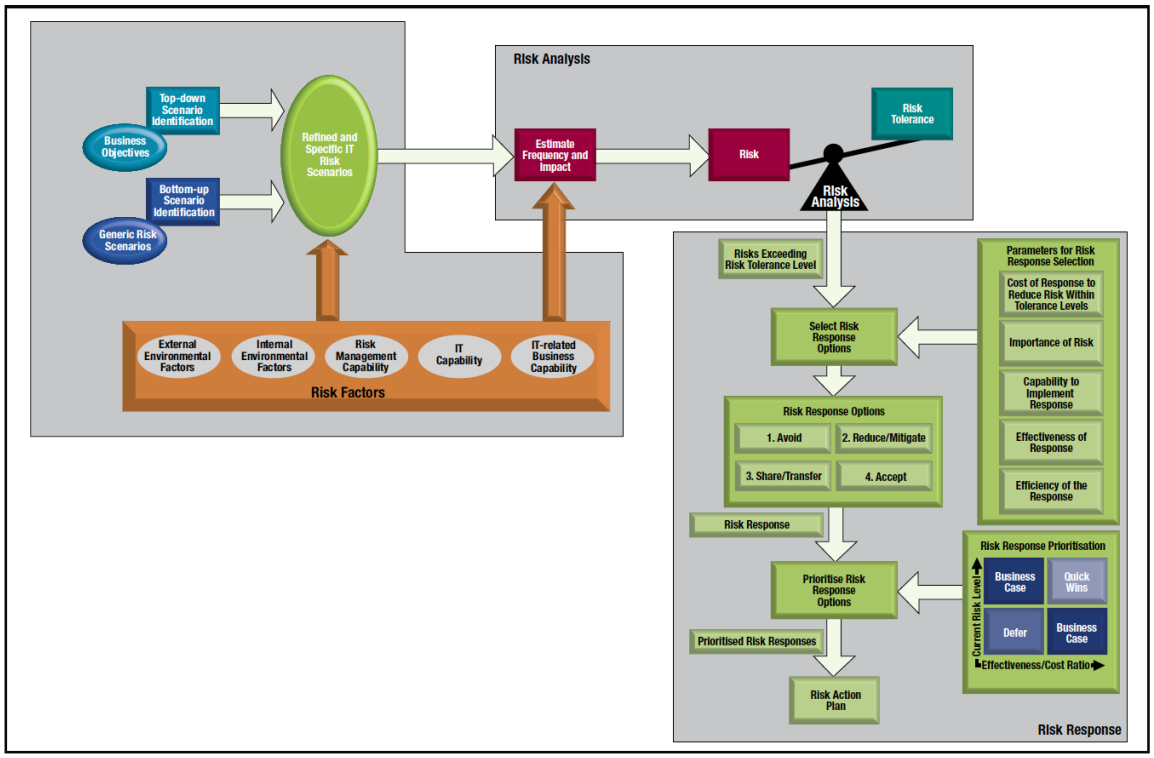
c. Response - ITM-related risk issues and events are addressed in a timely and effective manner.

Figure 1 – ITM Risk Framework[3]



3. ITM risk management will follow the process as shown in Figure 2

Figure 2 - Risk Analysis and Response[4]



4. IT risk assessment will be a continuous process with an outcome that IT has a current, correct and comprehensive understanding of its risks.[5]

[3] Risk IT Framework, 2009 ISACA
[4] Risk IT Practitioner Guide, 2009 ISACA

5. Responsibility for IT Risk Assessment will lie with the ITS Office of Information Security.
6. IT risk will be documented in an ITS Risk Register.
7. Detailed risk assessment will use the *MacEwan IT Risk Register Entry Template.*

Related Content

Type	***Title***
Guideline	MacEwan Generic IT Risk Scenarios Guideline.docx
Template	MacEwan Risk Register Entry Template
Form	ITS Risk Register.xls
Procedure	Risk Management Procedure

Key Words

Risk, risk management framework, risk principles, risk governance, risk evaluation, risk response

Measurement

- ✓ Records of meetings and decisions to show that explicit discussions on risks have taken place.
- ✓ The number of risk assessments with approved risk response plans.
- ✓ The number of controls developed in response to risk assessment.
- ✓ Completeness of the ITS Risk Register.

Contact

CIO
Coordinator, Information Security and Compliance

[5] ISO 31000:2009