MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

Information and Technology Services

MacEwan Control Framework Standard

Authority & Alignment

Authority: **D1200 Code of Conduct, D3300 Internal Controls, D8000 ITM Governance and Management**
Alignment: International standards – CobiT 4.1**, ISO 38500:2008**

Creation Date:	January 16, 2012
Last Update:	March 9, 2015
Document Version:	FINAL

Table of Contents:

1 Introduction

1.1 This document has been developed through the collaboration of several Post-Secondary Institutions (Institutions) for the purpose of providing guidance to individual Institutions who are required to develop, update and implement an effective ITM Control Framework (Control Framework) for managing their information and related technology.

1.2 This Control Framework is supported by:

1.2.1 The Provincial Post-Secondary System (PSS) Control Framework for Information and Technology Alignment Map that:

- Illustrates depth and breadth of the Control Framework scope and complexity
- Provides a holistic perspective of legislation, regulations, Control Objectives for Information and related Technology (COBIT), and various other international standards
- Demonstrates relationships between Provincial PSS strategic directions through to supporting controls

1.3 This Control Framework can be applied to all information, regardless of the media, and the related technology that delivers the information that MacEwan University requires to achieve its strategic direction and mandate.

2 Principles for Information and related Technology

2.1 Principles:

- Are values or general rules intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission and vision
- Are inter-related, and need to be applied as a set
- Will sometimes compete and therefore must be considered in the context of ‘‘all other things being equal’’

2.2 Information must be assembled and presented objectively. Key stakeholders who rely on such information have a right to be assured that it is reliable, secure and available regardless of the media. Principles express MacEwan University’s preferred behavior in the conduct of decisions, investments and activities in the provision of information and related technology.

2.3 MacEwan University recognizes the strategic value of investing in information and related technology to achieve its strategic direction and mandates and accepts the responsibility to accept or mitigate the inherent risks associated with these investments in order to realize its objectives. Principles provide the necessary guidance that is to be actively applied and reflected throughout the University’s controls.

2.4 The Principles have been adapted to support the strategic priorities of the Provincial PSS ITM Strategic Direction.

2.5 The following principles (listed in alphabetical order) have been adapted from ISO 38500, COBIT and various Institutions and Government of Alberta (GoA) Advisory Committees. They are to be applied as an active element in appropriate planning and management activities for information and related technology by providing the values to influence the controls developed by MacEwan University.

Accountability and Responsibility

MacEwan University will identify roles, appropriately segregate duties, and assign accountability and responsibility in respect to management of information and related technology. Individuals and groups will understand and accept assigned accountability and responsibility.

Compliance

Information and related technology controls will conform to applicable legislation, regulations, contractual requirements and institutional policy.

Enterprise Architecture

Enterprise architecture supports governance by systematically and holistically steering multi-stakeholder information and related technology solutions towards superior support of the University's strategic direction and mandate. It will embody 'service above self' because decisions made from an institution-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information and related technology decisions to adhere to institution-wide drivers and priorities.

Governance and Leadership

Information and related technologies are strategic enablers that when effectively managed result in assurance that value is optimized, risk is minimized and stewardship is accepted. The governance and leadership role is the responsibility of boards of governors and executives to provide organizational structure and controls that ensure information and related technology sustains and supports MacEwan University's strategies and mandates.

Information Management

Information is an asset. Information users are the key stakeholders in the application of related technology to address MacEwan University's requirements. These key stakeholders, from across the University, are responsible for developing and sustaining the information environment and defining the goals and objectives for managing information and related technology in alignment with the enterprise architecture. Information must meet these basic COBIT requirements:

- Effectiveness – information is relevant and pertinent to the University as well as delivered in a timely, correct, consistent and usable manner
- Efficiency – information is provided through the optimal use of resources
- Confidentiality – sensitive information is protected from unauthorized disclosure
- Integrity – information is accurate and complete as well as valid in accordance with the University's values and expectations
- Availability – information is available when required by ensuring the necessary resources and associated capabilities are safeguarded now and in the future
- Compliance – laws, regulations, contractual agreements and policy, both internal and external, are complied with
- Reliability – appropriate information is provided to management to ensure they can exercise their fiduciary and governance responsibilities

Information Security

Information Security is a critical function. Protecting valued and sensitive information is essential to MacEwan University's sustainability. The responsibility for this protection lies with all MacEwan stakeholders and can be achieved through the establishment of an intentional culture of security, one that supports the protection of information while also supporting the broader aims of the University.[1]

Investment and Acquisition

Information and related technology investments and acquisitions are made on the basis of appropriate and ongoing analysis, with clear and transparent decision-making. There is appropriate balance between benefits, opportunities, costs, quality and risks in both the short term and the long term.

Service Orientation

Understanding Student, Faculty and Administration needs and expectations drives service delivery strategies. Information Technology Management should endeavor to build and strengthen engaging and trusted relationships through consultation and collaboration. Services should be readily available and technology maximized to offer optimized choice wherever possible. Information Technology Management strategies will mutually enhance institutional value and service delivery capability, explore opportunities to improve the experience of interacting with the Institution and create value by understanding service delivery

[1] ISACA, *Creating a Culture of Security*, USA, 2011

costs and improving internal processes that sustain benefits to all key stakeholders. Service delivery models are designed to be easily adapted to meet the changing needs of MacEwan University and its key stakeholders as well as the emergence of new technologies. This flexibility will enable proactive tailoring of service delivery to meet the needs of its dynamic stakeholder base.

Technology Management

Technology is an asset fundamental to the delivery of information. MacEwan University will manage information related technology proactively. Existing and emerging technologies will be constantly assessed to inform the technological direction required to realize the University's strategic direction and mandate, the enterprise architecture design and potential institutional opportunities. Technology management will provide consistent, effective and secure technological solutions institution-wide that are aligned with the University's need for assurance that it is receiving value for its investment.

3 Control Framework

3.1 The Control Framework has been designed to ensure:

- Alignment with the MacEwan University's strategic direction and mandate
- Benefits from investments in technology are maximized
- Resources are used responsibly
- Risks are managed appropriately

3.2 The Control Framework provides a set of consistent principles that guide the development of controls and ensure alignment with the strategic direction and mandates of the University. It also assigns accountability and responsibility, influences how the controls should be structured and maintains a common glossary of terms.

3.3 The Control Framework provides a road map for developing internal controls for information and related technology assets required to implement strategic directions and mandates. The Control Framework uses COBIT and other international standards to meet quality, regulatory, fiduciary and security requirements.

3.4 The Control Framework sets the context for information and related technology control development and sound management practices that serve to direct information users of the University in the performance of their duties to achieve the desired institutional outcomes.

3.5 A standardized Control Framework and normalized set of controls is fundamental to:

- Supporting future partnerships that might include sharing of applications, services and skilled resources
- Accelerating the ability to integrate, interface and trust intra/inter-institutionally thereby decreasing overall costs and timelines of collaborative initiatives
- Facilitating and sustain learner access to a variety of learning opportunities through the effective use of technology
- Enhancing the quality, integrity and continuity of the teaching, learning, administrative and research environments

3.6 COBIT explains that a Control Framework and controls are needed by:

- Boards and Executives - to ensure fiduciary responsibilities are met and management expectations for the use of information and related technology across the system and within the University are aligned with institutional and provincial strategic directions and mandates.
- Management - to make sound information and related technology investment decisions, to balance risk and control, and to benchmark the existing and future environment.
- Information users - to obtain assurance that information and related technology products and services they use are secure, reliable, accessible and available.
- Auditors - to provide assurance that management's information is reliable and complete, to identify opportunities for improving control over and the use of resources, and to make recommendations to improve related technology systems and practices.

3.7 The Control Framework is part of an integrated and consistent approach to managing information and related technology within the University as well as across the Alberta Post-Secondary Sector.

3.8 MacEwan University recognizes that information and related technology are valuable assets that must be managed throughout their lifecycle in a disciplined manner to support the Institution. The Control Framework provides the foundation for ensuring integrity, confidentiality and availability of information.

4 Control Alignment and Relationships

4.1 The Control Framework has been designed to ensure that the controls are influenced by the strategic directions and mandates of MacEwan University.

4.2 Specific alignment and relationships between controls and related content are specified within the control documents themselves.

5 Controls

5.1 As defined by COBIT, controls include policies, procedures, practices and organizational structures designed to provide reasonable assurance that objectives will be achieved and unwanted events will be prevented or detected and corrected. This Control Framework expands on this definition to include standards and guidelines as defined in Sections 5.6 and 5.7 respectively.

5.2 By nature, controls are dynamic and need to be revised regularly to reflect constant change, both internally and externally. Examples of change drivers include, but are not limited to:

- MacEwan University's direction or needs
- Organizational structure
- Planned improvements
- Compliance incidents
- Risk and privacy impact assessments
- Legislation and regulations
- Industry standards
- Testing or audit results that conclude the control is ineffective

5.3 Policy:

5.3.1 A policy regulates organizational action. It can be defined as:

- High-level direction for what to do in a particular situation or set of circumstances
- A type of position statement
- A philosophy, a mission, or general objective

5.3.2 The purpose of a policy is to:

- Ensure compliance with applicable legislation, regulations, and contractual requirements
- Promote accountability

5.3.3 Policies should be:

- Integrated with strategic decision making and institutional planning
- Supported by accountable leadership and governance
- Used to provide ongoing communication of direction and expected benefits
- Aimed at 'root cause' issues
- Adaptive but not reactive
- Inclusive and responsive
- Actively applied in day-to-day activities
- Tested and validated to the extent possible
- Reviewed regularly to maintain currency and relevance
- Monitored for compliance and measured for effectiveness on a regular basis

5.3.4 Policies should be developed when:

- Non-legislative alternatives (management practices) will not stand alone
- Compliance with desired behavior must be compelled
- There is a need to control, direct or inform
- An issue is important or benefits from clarification
- Cultural or organizational change is desired

5.4 Organizational Structure:

5.4.1 As adapted from the Project Management Institute's Project Management Book of Knowledge (PMBoK), an organization structure is an institution-wide environmental factor that can affect the availability of resources and influence how business is conducted.

5.4.2 COBIT further explains that organization structures reveal vertical operational responsibilities, and horizontal linkages, and may be represented by an organization chart to demonstrate governance.

5.5 Procedure or Process:

5.5.1 Procedures or processes are action oriented and can be defined as:
- The steps people are expected to take and the sequence in which to perform those steps
- A set of actions which are the official or accepted way of doing something
- The customary or normal method of completing a task or objective
- A protocol for implementation
- Directions or instructions, that is, the 'how to'

5.5.2 The purpose of a procedure is to:
- Assign accountability and responsibility for activities
- Identify those that need to be consulted or informed
- Ensure compliance with a policy
- Inform users how to implement the requirements, achieve the necessary results, and of consequences for non-compliance

5.6 Standard:

5.6.1 A mandatory requirement, code of practice or specification established and approved by authority that is used as a baseline to measure the quality or performance of a process or procedure

5.6.2 The purpose of a standard is to:
- Outline specific requirements or rules that must be met
- Regulate, direct, and control actions or conduct

5.6.3 Standards should be developed to:
- Detail universal information or technical standards that are replicable, transferable and adaptable across the Institution (i.e. address data standards)
- Formally adopt national or international industry standards (i.e. ISO, ITIL)
- Define acceptable minimum requirements (i.e. passwords)
- Facilitate enhancements and acquisitions of products or specific technology oriented standards that establish conformity, interoperability and interchangeability (i.e. MS Office)
- Establish mandatory institutional practices that improve outcomes, mitigate risks and increase reliability (i.e. contracts, templates)

5.7 Guideline:

5.7.1 A guideline is a recommended, non-mandatory control that is advisory in nature. It provides optional or new best practices that are endorsed by subject matter experts within the industry. Although a guideline is voluntary, the implication is that the concepts will be adopted to improve current practices.

5.7.2 Guidelines are developed to provide:

- Alternative approaches for consideration where a standard does not exist
- Advice on best practices and industry standards
- Guidance for continuous improvement

6 Control Implementation

6.1 Implementation of controls should be consistent with MacEwan University's governance and control framework, appropriate for the organization, and integrated with existing methods and practices.

6.2 It is recognized that control implementation must be managed and may take time. Thorough assessments, action plans and timelines to remediate issues should be reasonable and demonstrate adequate progress towards implementation.

6.3 Management and auditors can be assured the implementers are proactively recognizing issues, acknowledging MacEwan University may not be ready to remediate the issue due to internal/external constraints and limitations, and developing reasonable action plans and timelines that can be monitored for progress.

6.4 The following assessments and plans may be used by management to support the successful implementation of the controls:

6.4.1 Statement of Applicability – designed to assess whether a control is relevant or applicable to the Institution, currently exists and is documented, and whether it is adequate to meet the control objective and address the risk it was intended to mitigate.

6.4.2 Controls Assessment - designed to validate the statement of applicability as well as enable management to make informed decisions by outlining controls required by legislation, international standards, policy and contracts; identifying gaps in the current state; identifying options and consideration of other compensating controls, and recognizing limitations or constraints to immediate implementation.

6.4.3 Remediation Action Plan – provides detailed description of the actions required to overcome the limitation or constraint, a rationale to support the action, the objective of the intended outcome, prioritization, dependent activities, an owner, and a target completion date.

6.4.4 Implementation Plan - specifies the detailed activities of the implementation process, provides an auditable record of the completed tasks, assigns the appropriate resources and time schedule to each task, identifies training and communication requirements and ensures a post implementation review is conducted.

7 Balanced Risk Approach

7.1 "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."[2]

7.2 The following risk principles provide the necessary guidance required to maintain an appropriate balance between relevant risk considerations, the strategic direction and mandate of MacEwan University, and cost effectiveness. Application of these principles in this Control Framework is intended to be coordinated with MacEwan University's Enterprise Risk Management Framework. These principles should be applied when designing and implementing the controls:

[2] CAN/SCA-ISO 31000:2009-10 page v

7.2.1 Risk will be managed with an enterprise perspective, recognizing both the potential value of opportunity and the potential impact of adverse effects.

7.2.2 Risk will be managed proactively by identifying uncertainties and anticipating potential outcomes and benefits.

7.2.3 Risk management will be used to trigger innovation and progress.

7.2.4 Risk awareness will be promoted using processes that value the individual voice in recognition that it brings unique knowledge and insight to identifying and managing risk.

7.2.5 Risk management will be an integral and vital part of project management with methods and tools that are adaptable to a project's infrastructure and culture of the project stakeholders.

7.2.6 Risk management is a continuous process that focuses on results.

7.2.7 Reasonable and practical controls will be selected and implemented on the basis of and in proportion to the risks they are designed to mitigate.