Athabasca University

PROCEDURE

Information Technology Risk Management Procedure			
Parent Policy	Digital Governance Control Framework – Governing Policy		
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	VPIT & CIO	**Effective Date**	December 12, 2019
Procedure Contact	Chief Information Security Officer (CISO)	**Review Date**	December 12, 2024

1. Purpose

The University is committed to managing risks associated with IT digital governance including the commitment to: the integration of risk management at an enterprise level; make well-informed decisions about the extent of the University's risk, risk appetite and the risk tolerance; understand and manage all significant IT risk types; and, understand how to respond to risk.

2. Scope

This procedure includes all process areas within the scope of digital governance projects and IT operations, but may be further refined (through approval by Executive Team) to define the expected breadth and depth of risk management activities. The Chief Information Security Officer (CISO) is accountable for ensuring via the Digital Governance Committee (DGC) activities that the application of risk management principles to projects and operations have been addressed in the required reviews by the Digital Governance Technical Subcommittee as well as any future security-specific subcommittee of Digital Governance. Risk aware behaviour and mitigation is expected of every member of the University Community involved in these activities.

3. Definitions

Digital Governance Committee	An advisory committee reporting to Executive Team for the purpose of assisting Executive Team in fulfilling its due diligence, fiduciary, financial reporting and audit response responsibilities by monitoring, evaluating and providing advice to the Executive Team on matters affecting all university digital initiatives.
Digital Governance	A non-voting working group who reports to the Digital Governance Committee (DGC). The purpose of the sub-

Technical Sub-Committee	committee is to facilitate the successful delivery of the technical and security-related aspects of approved digital initiatives.
Risk Management	The responsible administration of any digital initiative requires awareness of risks that can occur with uncertain frequency and impact and create challenges in meeting strategic goals and objectives. Handling such risks, through a risk management approach, is essential to achieving objectives. Appropriate risk management ensures all new or known risk attributes have been defined (e.g., owner, likelihood, impact) and analyzed and alerting the PSC to risk changes and their potential impact to the project, other projects, or the organization.
Risk Register	A document that identifies the potential risks to a digital initiative along with attributes for each risk.
Risk Tolerance	Depending on risk type, defined by either Deputy CIO, CISO or Privacy Officer as the acceptable level of variation relative to the achievement of objectives.
Standard Operating Procedure (SOP)	A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often inform the Policy Framework. A SOP is highly detailed, regularly revised and is deemed internal to the University, although a SOP may be shared on a need-to-know basis.

4. Guiding Principles

4.1. Digital Governance standards associated with risk management are:

a. Open communication is critical to successful risk management. Expectations for reporting on risks up through Integrated Resource Planning, Digital Governance Committee, or related sub-committee structures, will be defined internally.

b. The University's tolerance for risk must be understood with regard to every digital project, operation or activity.

4.2. Specific procedural content may address components of risk management including: development of an overall/enterprise Risk Management Framework; undertaking risk assessments; defining the University's risk appetite and tolerance; identification of typical risks and expected mitigation strategies; methods for evaluating risk; development of processes for communication and

other risk responses such as action plans; and development of specific risk management processes.

4.3. Risk Register and Risk Mitigation Process related procedural content may include expectations for a description of risk, its owner, mitigation tactics, and use of a rating system for likelihood and impact.

5. Applicable Legislation and Regulations

None applicable

6. Related Procedures/Documents

Digital Governance Framework for AU
Alberta Association in Higher Education for Information Technology's ITM Control Framework

NOTE: The subject matter and scope of this procedure are also supported by internal-use only Standard Operating Procedures.

History

Date	*Action*
December 12, 2019	Executive Team (Policy Approved)