IT: RISK MANAGEMENT PROCEDURE

Procedure Type:	Institution	**Initially Approved:**	April 01, 2011
Procedure Sponsor:	VP Administration	**Last Revised:**	August 11, 2020
Administrative Responsibility:	Computing & Technical Services (CTS)	**Review Scheduled:**	August 2025
Approver:	President and CEO		

A. INTENT

This procedure defines a consistent approach to the risk assessment, mitigation and management of information assets at AUArts. It provides a framework for executive leadership with an appraisal of all Information Technology (IT) risks and a means of assessing the effort of their mitigation and a means for accepting some risks without mitigation.

B. SCOPE

This document applies to AUArts information assets and the foreseeable risks to which they may be exposed. It defines analysis methods, monitoring and management processes, and mitigation strategies.

C. PROCEDURES

1. Risk Assessment

1.1 At each ITSC Meeting, incidents captured in the Helpdesk ticket system are reviewed by the ITSC to expose unexpected risks.
1.2 Risk assessments are incorporated into all Requests for Change according to the IT Change Management Procedure.
1.3 An enterprise Risk Management Matrix is used for assessing IT risks.
1.4 The ITSC reviews all identified risks and considers whether to accept, avoid, transfer or mitigate the risk.
1.5 The ITSC performs an annual overall Information Technology Risk Assessment process and updates the list of known risks and mitigation strategies in accordance with the AUArts Risk Management framework.
1.6 IT Risks are submitted for inclusion in the annual Enterprise Risk Management Report.

2. Risk Management

2.1 The ITSC is responsible for managing all identified IT risks. Risk management involves coordinating the activities involved to direct and control IT risks.

2.2 For mitigated risks:

a. Mitigation strategies shall be documented and implemented by the ITSC to maintain AUArts operations at acceptable levels.

b. Mitigation strategies shall reduce the risks to an acceptable level and include where necessary:

i. requirements and constraints of legislation and regulations

ii. organizational objectives

iii. operational requirements and constraints

iv. cost of managing risks versus the cost of damages in the absence of risk management activities

2.3 For unmitigated risks:

a. The ITSC will indicate where the IT risk was accepted, avoided or transferred. Documentation shall include the following information as needed:

i. Risk level (score) of the Information Asset at risk

ii. All risk management strategy options considered

iii. Residual risk remaining as a result of not mitigating

iv. The estimated cost or operational impact of the unmitigated risk

Roles and Responsibilities

3. All Users

3.1 All AUArts authorized users who use, have access to, or are responsible for AUArts information assets have a role in the effective management of IT risks.

3.2 All staff should actively participate in identifying potential risks in their area and contribute to the implementation of appropriate mitigation strategies.

4. Information Asset Owners

4.1 Understanding their assets sufficiently in order to identify potential risks and work with the ITSC to classify and manage risks to the information asset.

5. The Information Technology Steering Committee (ITSC)

5.1 Ensuring IT risk management is implemented and maintained in accordance with this procedure and the Risk management Policy.

5.2 Overseeing the processes for the identification, assessment and mitigation of Information Technology risks.

5.3 Assessing and managing all identified IT risks.

5.4 Reporting IT risks for inclusion in the annual Enterprise Risk Management Report.

D. DEFINITIONS

Authorized Users:	Includes students, staff, faculty, employees and third-party users such as contractors, consultants, temporary users, suppliers and service providers.
Information:	AUArts data in any form or media, including databases and computer files, which is collected, transmitted, stored or maintained on AUArts' information systems or elsewhere.
Information Systems:	AUArts' Information Technology (IT) networks, systems and applications.
Information Assets:	Information and information systems.
IT Steering Committee:	Membership for the ITSC is defined in the ITSC Terms of Reference. The ITSC meets regularly to evaluate change requests and coordinate IT management responsibilities.
Risk:	The effect of uncertainty on objectives, which can be positive or negative, and is measured as a combination of probability of occurrence and impact of an event/change in circumstance.
Risk Appetite/Tolerance:	The amount and type of risk that the Board of Governors is prepared to pursue or retain. The Board currently requires reported risks with a score of a medium (either equal to or greater than 6) to be reported with a risk treatment plan.
Risk Management:	The name given to the coordinated activities of the institution to direct and control risk.
Risk Acceptance:	Retain the risk by informed decision.
Risk Avoidance:	Deciding not to start or continue to pursue an activity or program as a result of the identified risk.
Risk Mitigation:	Reduce the probability and/or negative consequences (impact) of a risk to a desirable level.
Risk Transfer:	Give Responsibility of a risk to a third party (e.g. insurance, bonds, warranties, third party contracts).
Risk Impact:	A level of the severity of an event affecting the achievement of objectives.
Risk Probability:	A level of the likelihood of something happening.
Risk Level:	Risk Impact x Risk Probability.

E. RELATED POLICIES

- Risk Management Policy

F. RELATED LEGISLATION

G. RELATED DOCUMENTS

- Information Asset Inventory
- System Recovery Management Plan
- ITSC Meeting Minutes
- Risk Management Matrix

H. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
07/31/2020	Template Update and Content Revisions		Director, CTS	