
IT RISK MANAGEMENT PLAN

Version 1.0
05/23/2017

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Nathan Zierfuss-Hubbard, CISO	05/23/2017			Initial Risk Management Plan draft
1.0	Karl Kowalski, CITO	n/a	IT Council	8/22/2017	Approval of Initial Risk Management Plan

TABLE OF CONTENTS

VERSION HISTORY	2
INTRODUCTION	1
1.1 Purpose Of The Risk Management Plan	1
RISK MANAGEMENT PROCEDURE	1
1.2 Process	1
1.3 Risk Identification	1
1.4 Risk Analysis	1
1.4.1 Qualitative Risk Analysis	1
1.4.2 Quantitative Risk Analysis	2
1.5 Risk Response Planning	2
1.6 Risk Monitoring, Controlling, And Reporting	2
TOOLS AND PRACTICES	3
APPENDIX A: REFERENCES	5
APPENDIX B: KEY TERMS	6

INTRODUCTION

1.1 PURPOSE OF THE RISK MANAGEMENT PLAN

This risk management plan provides the process that identifies information technology associated risk on an ongoing basis, documents identified risks and the response to them the organization expects.

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with information technology will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.

The Risk Management Plan is created by the CISO, is informed and updated by the CIOs, is monitored by responsible IT Managers. The intended audience of this document is the IT personnel and University management.

RISK MANAGEMENT PROCEDURE

1.2 PROCESS

The CITO working with the campus CIOs and ISOs will ensure that risks are actively identified, analyzed, and managed throughout the life of the IT resources. Risks will be identified as early as possible to minimize their impact. The steps for accomplishing this are outlined in the following sections. The IT manager responsible for a service will serve as the responsible party for addressing risk in their services.

1.3 RISK IDENTIFICATION

Risk identification will involve the IT leadership, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and management plans. The identification effort will take place annually.

A Risk Register will be generated and updated as needed and will be stored electronically by the CITO.

1.4 RISK ANALYSIS

All risks identified will be assessed to identify the range of possible outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

1.4.1 Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed IT leadership, with input from ISOs using the following approach:

Probability

- High – Greater than <70%> probability of occurrence
- Medium – Between <30%> and <70%> probability of occurrence
- Low – Below <30%> probability of occurrence

Impact

I m p a c t	H	Yellow	Red	Red
	M	Green	Yellow	Red
	L	Green	Green	Yellow
		L	M	H
Probability				

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance

Risks that fall within the RED and YELLOW zones will have risk response planning which may include both risk mitigation and a risk contingency plan.

1.4.2 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on business and IT activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in the Risk Register.

1.5 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a responsible IT Manager for monitoring purposes to ensure that the risk will not “fall through the cracks”.

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the responsible IT Manager and ISO will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include redesign, redevelopment, additional access controls, non-technical administrative controls, new or changed processes, etc.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

1.6 RISK MONITORING, CONTROLLING, AND REPORTING

The level of risk associated with IT will be tracked, monitored and reported.

A “Top 5 Risk List” will be maintained by the CITO and will be reported as a component of IT status reporting processes as appropriate.

All IT change requests will be analyzed for their possible impact to identified risks.

Management will be notified of important changes to risk status as a component of regular status reporting.

TOOLS AND PRACTICES

A Risk Register will be maintained by the CITO and will be reviewed as a standing agenda item for appropriate committee or group meetings.

RISK MANAGEMENT PLAN APPROVAL

The undersigned acknowledge they have reviewed the **IT Risk Management Plan**. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
Board of Regents Policy: Information Resources	Board policy covering use, protection and administration of information resources	https://www.alaska.edu/bor/policy/02-07.pdf
University Regulation: Information Resources	University regulations covering application of Board policy on Information Resources	https://www.alaska.edu/bor/policy/02-07.pdf
University Standards and Best Practices	University Office of Information Technology Standards and Best Practices related to Information Technology	https://www.alaska.edu/oit/standards/

APPENDIX B: KEY TERMS

The following table provides definitions for terms relevant to the Risk Management Plan.

Term	Definition
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
ISO	Information Security Officer