University of Colorado Colorado Springs

Information Technology Department

Process Definition

UCCS IT Risk Management Process

Revision History

Revision Number	Date	Change Request Number	Figure or Section Number	A - Add M - Modify D - Delete	Title or Brief Description
0.1	8/14				Initial Draft and revisions
1.0	10/14				Approval by Jerry Wilson

1 Scope & Rationale for IT Risk Management Process

1.1 Purpose

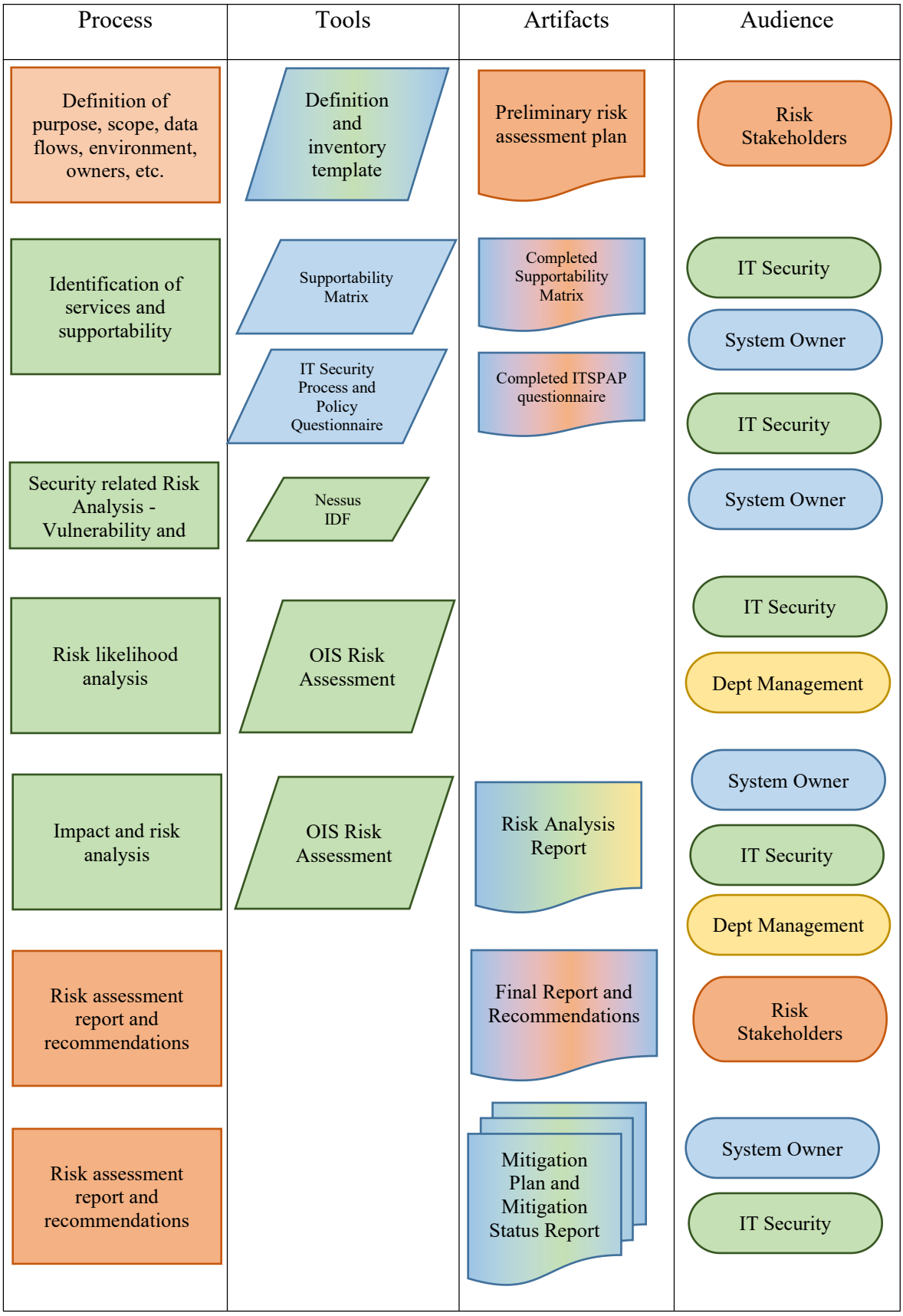
The University of Colorado Colorado Springs (UCCS) recognizes the need for an *Information Technology* (IT) *risk management* process to ensure performance and continuity at the University. This process is based on the fact that the campus relies on the availability and reliability of IT and this reliability will continue to grow as the campus increasingly utilizes IT as a means for supporting educational and administrative processes, dissemination of information, and for general communication. Because the perception of *risk* varies among the different constituencies across campus, a need exists for consistent criteria and shared understanding.

A total failure, partial failure, or security compromise seriously and adversely affects the campus. The risk management process will identify UCCS *information assets*, including both hardware and software that are considered *essential* to the campus mission. This process will also identify *information assets* that are considered to be of secondary and peripheral significance.

This document defines the UCCS *risk management* process in conjunction with OIS Risk Assessment process and associated tools and artifacts. Because IT technology, staff, and systems change, risk management is a continual process that the campus will continually engage in to ensure high performance of the campus IT infrastructure.

1.2 Overview of IT Risk Management Process

The following flow chart provides an overview of the risk management process.


Process
Tools
Artifacts
Audience
Definition of purpose, scope, data flows, environment, owners, etc.
Definition and inventory template
Preliminary risk assessment plan
Risk Stakeholders
Identification of services and supportability
Supportability Matrix
Completed Supportability Matrix
IT Security
System Owner
IT Security Process and Policy Questionnaire
Completed ITSPAP questionnaire
IT Security
Security related Risk Analysis - Vulnerability and
Nessus IDF
System Owner
Risk likelihood analysis
OIS Risk Assessment
IT Security
Dept Management
Impact and risk analysis
OIS Risk Assessment
Risk Analysis Report
System Owner
IT Security
Dept Management
Risk assessment report and recommendations
Final Report and Recommendations
Risk Stakeholders
Risk assessment report and recommendations
Mitigation Plan and Mitigation Status Report
System Owner
IT Security

1.3 Scope

Participation Scope

APS 6005 – IT Security Program requires that all departments identify risk and report them. Periodic risk assessments should be performed on any resource that utilizes information technology resources.

Certain departments using, processing, or storing certain types of data may require third-party risk assessments. Additionally, resources that are under any mandated compliance must perform risk assessments at least every two (2) or when significant changes are performed to the information resource.

Information technology risk assessments shall be performed according to an internal risk assessment scheduled as determined by the Information Security Officer and the Chief Information Officer.

Additionally periodic risk assessments and supportability based risk assessments may be performed as requested by the campus CIO or business and process owner that has a vested interest in the services that the Information Technology Department provides.

Content Scope

Information technology *risk analysis* and management requires a broad range of information on IT assets, services and possible threats. The data collection phases of the *risk management* process include an IT asset *inventory*, a procedures and policies questionnaire, supportable services assessment and possibly a *vulnerability* assessment of essential assets where the risk is considered security related. The details of each of these data sets are covered in supporting documents (inventory template, procedure and policy questionnaire, supportability matrix, and outline of vulnerability assessments). The level of information required in each area is generally basic and can often be provided by a questionnaire and matrices. Departments with *essential* or *life/safety* functions, systems or data will require more in-depth information and analysis.

2 Risk Framework

UCCS Risk Framework is aligned with CU OIS Risk Assessment Process, however there are areas in which more detail is needed for the campus level.

2.1 Definition and Scope Phase

The Information Technology Department is responsible for the formation and maintenance of the campus IT risk management process. IT will submit the process to campus IT constituencies (IT Governance) for review when the process is updated or

modified. The document will define the process steps, scope of the process, artifacts of the process, roles and responsibilities.

The IT risk management process will be reviewed annually by both IT Security and IT leadership and updated to reflect changes to policies and risk management approaches.

Artifact: Definition and Inventory Template

It is the responsibility of the system owner or data custodian, and in the case of security related risk assessments, IT Security, to produce the Definition and Inventory Template which will be used to define the purpose, scope, boundaries, data flows, system/process environment, owners, assumptions, constraints, and expectations from the assessment. This template will also include asset criticality and data classification.

2.2 Identification of Services and Supportability

In addition to the OIS Risk Assessment process on threats and event identification, system owners shall complete the supportability matrix and in the case of a security related assessment, the IT Security Process and Policy questionnaire. These artifacts are designed to help identify potential risk areas not realized by external events.

Artifact: Supportability Matrix

It is the responsibility of the system or service owner to fill out the supportability matrix. The matrix focuses on key business functions and their reliance on IT services. It helps identify what areas are key for the function of the service and if the service is supportable in all functions. Those functions that are partially or not supportable can be identified as a risk area.

Artifact: IT Security Process and Policy Questionnaire

It is the responsibility of the system owner to fill out the ITSPAP questionnaire. The questionnaire focuses on internal security and policy to help determine gaps in security or help identify external factors that could become risks. Example provided in the appendix.

2.3 Security Related Vulnerability and Threat Control Analysis

Vulnerability assessment shall be performed by IT Security using both automated and manual tools if the risk assessment being performed is a security related risk. Based on the criticality of the data and known threats of the system interviews with key stakeholders of the system may also be performed.

Artifact: Vulnerability Analysis report and possible data discovery report

2.4 Vulnerability and Threat Likelihood Analysis

This phase shall be completed by IT Security, and will feed outputs into next phases.

2.5 Impact and Risk Analysis

This phase shall be performed by IT leadership or IT security for security related risk assessments, modeling off the OIS Risk Assessment process.

Artifact: Risk Analysis Report

The Risk Analysis Report will be generated by IT leadership or IT security for security related risk assessments and given to the system owner and departmental management. The Risk Analysis will take into consideration the supportability of the service and the vulnerability and threat analysis combined with the likelihood analysis to come up with an over assessment of risk for the given system or service.

2.6 Risk Assessment Report and Recommendations

A final report will be issued to all risk stakeholders on completion of the assessment. The report shall contain the findings and recommended mitigation recommendations.

3 Mitigation

Following the creation of the Risk Assessment Report and Recommendations, each department will need to address the risks covered in the report. There are numerous ways of addressing risk including reduction, avoidance, acceptance and transfer. The decisions on how to best deal with a particular risk require consideration of the business needs of the organization in addition to an understanding of the risk. For security related risk assessments, IT Security will provide the department with recommendations for addressing risk in general and specific risks as appropriate. The department is responsible for creating a risk mitigation plan that includes a timeline for the implementation of mitigation steps and submitting it to IT Security and IT leadership. IT Security and IT leadership will review the plan and provide feedback to the department. If necessary, the department will revise the plan and resubmit it to the IT Security and IT leadership.

Depending on the risks and mitigation plan, IT leadership or IT Security may follow up with the department and request a mitigation status report. This report will give the status of each of the mitigation steps listed in the department's mitigation plan.

Artifact: Risk Mitigation Plan

A report detailing the department's planned risk mitigation steps including a timeline for implementation will be created by the department and given to IT Security and IT leadership.

Artifact: Risk Mitigation Status Report

A report providing an update on the status of implementation of the risk mitigation steps covered in the department's risk mitigation plan will be created by the department at the request of the IT Security or IT leadership and given to IT Security and IT leadership.