The objective and rationale for managing risk in the Company is to facilitate the identification of the material business risks, manage those material business risks and internally report to the responsible person and to the board on those material business risks identified.

Your company recognizes the need for an Information Technology (IT) risk management process to ensure performance and continuity of business. This process is based on the fact that the business relies on the availability and reliability of IT and this reliability will continue to grow as the business increasingly utilizes IT as a means for supporting all business centric processes and for general administration and communication.

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

**Borrowed and adapted from a model created by University of Virginia**

## A. Process Overview

Step 1: IT Mission Impact Analysis

* Determine your department’s ***critical assets*** (hardware, software, information, people) based on Table 1 below and your department’s mission

Step 2: IT **Risk Assessment**

* Assess departmental security practices against University, national and international standards
* Map your department’s assets from Step 1 to the threat scenarios provided (and others that your department identifies)
* Assign weight to each threat to your assets based on the likelihood of it occurring in your environment and the impact of any vulnerability
* Prioritize the threats you face
* Map these threats back to response strategies provided (and others your department develops)
* Create (or update if you already have one) your department’s security plan for mitigating or accepting the identified risks
* Take into account previously implemented strategies and existing plans – use (and document) effort and analysis that you have already produced
* Document your key decisions and justifications

Step 3: IT Mission Continuity Planning

* Create (or update) a response plan for your department to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed
* Test your plan

Step 4: Evaluation and Reassessment

* Repeat Steps 1-3 every three years or when there are significant changes to departmental IT assets or risk environment
* Review the success of your prior analysis, testing and any responses made, whether they were corrective, preventative or post-incident
* Incorporate responses to any intervening changes (new operating system, critical applications or data, or University, state or federal standards)

See [section F.](#_F._Reporting_Requirements) below for the reporting requirements of this process, and see [Appendix A](#_Appendix_A:_Sample) for sample responses to these steps. These examples do not necessarily cover all the issues facing your department, but they are intended as examples of the type and level of response expected. The time necessary to complete the ITS-RM process will vary with the size of the department, the breadth of its mission and the complexity of its IT infrastructure. Departments should establish internal deadlines for the completion of each step of the process in order to ensure steady progress.

### IT Security Risk Management Process Flow

w_bnidno[1]w_bnidno[1]w_bnidno[1]

1. **Disaster recovery plan example**
2. **Interim manual procedures example**
3. **Criteria**
4. **Template**
5. **Assessment questions**
6. **Threat scenarios**
7. **Response strategies**
8. **Security plan template & example**

*Security*

*Plan*

*Interim*

*Manual*

*Procedures*

*Disaster*

*Recovery*

*Plan*

Step 4 – Evaluation and Reassessment

Required at least once every two or three years

Step 3 – Mission

Continuity Planning

Create a response plan to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed

Step 2 – Assess Risks

For each critical asset:

1. Assign weight to likelihood & impact of threats to each asset
2. Prioritize threats
3. Select response strategies
4. Develop security plan

*Critical*

*Assets*

*List*

Step 1 - Identify

Critical IT Assets

## Terminology

### Source of Terminology

Most of the definitions and most of the examples below are appropriated from the US National Security Agency (NSA).

### Definitions

**Risk**:

* (Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; [[Oxford English Dictionary](http://en.wikipedia.org/wiki/Oxford_English_Dictionary)]
* Effect of uncertainty on objectives; [[ISO 31000](http://en.wikipedia.org/wiki/ISO_31000) (2009)]

**Management:** (New World Dictionary of the American Language)

* The art or manner of *controlling* the movement or behavior of something
* To have charge of; direct; conduct; administer

**Risk Management:**

1. identification, assessment, and prioritization of [risks](http://en.wikipedia.org/wiki/Risk)
2. followed by application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events

**Risk Management (Simply Put):** Determine what your risks are and then decide on a course of action to deal with those risks.

**Aim of Risk Management:** To aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks

**Critical Asset:** Something that when disclosed, modified, destroyed, or misused will cause harmful consequences to the business (department or its – or the University’s – goals and mission) or will provide an undesired and unintended benefit to someone

*Examples*: Information, people, software, hardware, facilities, etc.

**Risk Assessment:** A study of threats and vulnerabilities, the design effectiveness of present security mechanisms, and the potential impact of these factors on a department’s ability to perform its mission

**Threat:** The capabilities and intentions of adversaries to exploit an information system; or any natural or unintentional event with the potential to cause harm to an information system, resulting in a degradation of a department’s ability to fully perform its mission

*Examples*: adversarial (terrorists, foreign states, disgruntled employees, criminals, recreational hackers, commercial competitors) and non-adversarial (nature, unintentional human acts)

**Attack:** A well-defined set of actions by the threat (an active agent) that, if successful, would damage a critical asset – cause an undesirable state of affairs – resulting in harm to a department’s ability to perform its mission

[An attack is an *action*; a vulnerability is an *opportunity*.]

**Vulnerability:** A characteristic of an information system or its components that could be exploited by an adversary, or harmed by a natural act or an act unintentionally caused by human activity

*Examples*: Inadequate password management, easy access to a facility, weak cryptography, a software flaw, an open port

[Or a facility housing the asset that is subject to fire or flood.]

**Consequence:** The harmful result of a successful attack, degrading a department’s ability to perform its mission

*Examples of consequences to a department’s mission*

* Loss of information confidentiality
* Loss of information integrity
* Loss of availability of information or system functions [natural disaster]
* Inability to correctly authenticate sender of information [forged log-ins, redirected transactions]
* Inability to verify receipt of information by the *intended* recipient [credit card connections]

**Risk Mitigation:** Actions or countermeasures we can take to lessen risk

* Affect threat agent or their capabilities
* Eliminate or limit our vulnerabilities

*Countermeasure Examples*

* Fix known exploitable software flaws
* Enforce operational procedures
* Provide encryption capability
* Improve physical security
* Disconnect unreliable networks
* Train system administrators [*Train everybody!*]
* Install virus scanning software

**Risk Management Decision:** Determination by administration to

* Take specific actions that will mitigate risk to mission, or
* Reject countermeasure recommendations and accept risk to mission

**Residual Risk:** That portion of risk that remains

* Management decides to accept risk
* Unconsidered threat factors
* Unconsidered vulnerabilities
* Incorrect conclusions