Your Organization

Risk Management Plan

This document contains information and data which are privileged, confidential, and/or proprietary.

Table of Contents

Executive Summary

Enter details about the organization and it IT Infrastructure.

There are three primary elements that should be identified for any given risk:

- *Threats*: Each risk is associated with a particular threat – which is defined as something that can cause some loss of asset confidentiality, integrity or availability. A virus is a threat, for instance.
- *Vulnerabilities*: These are weaknesses in resources and/or processes that allow for a threat to be realized. For a virus threat to be realized (to have impact), the virus will need to find a vulnerability – perhaps a device without anti-virus software.
- *Impacts*: Impact represents the cost of a security incident that occurs when threat exploits vulnerability. Risk management plans attempt to monitor and control threats and vulnerabilities in an attempt to minimize impact.

The organization must establish risk management policies and supporting documents in order to successfully identify, analyze and monitor risks. It is also essential to establish a risk management committee with broad campus representation in order to promote risk management awareness and ensure that the proper protocols are carried out and clearly communicated across the university.

With protocol defined and a risk management committee established, the university will be ready for full deployment. The plan will involve regular assessment of risk within each division and department, the introduction of non-IT related risk assessment (natural disasters, terrorism, fire, etc.) into the process and direct connections with organization's business processes. Indeed, risk assessment should become a core business process unto itself to ensure that organizational assets are protected and legal obligations are met.

Introduction

Mission

The mission of information technology security is to protect critical information resources that support the organization’s mission.

Goal

The goal of this risk management process is to protect the organization and its ability to perform its mission.

Objective

The objective of risk management is not to eliminate all risk, but rather to keep risk at a level where protection failures are within anticipated and acceptable ranges.

Definitions

Risk: a combination of threats, vulnerabilities, and consequences or impact.

Risk Management: the act, manner, or practice of supervising or controlling risks, including avoidance, acceptance, mitigation, or transfer of risks.

IT Risk Assessment/analysis: The process of weighing and prioritizing risks to the organization’s IT assets. The risk assessment process identifies what needs to be protected. An IT risk assessment is effectively a cost-benefit analysis of the organization's IT assets.

Information Resources/Assets: an IT application or supporting infrastructure which can be drawn on when needed to be used for support or help in performing day to day operations.

Availability: the property that data or information is accessible and useable upon demand by an authorized person

Confidentiality: the property that data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: the property that data or information have not been altered or destroyed in an unauthorized manner.

How we get there

Scope of the problem

Certain Information System Resources and processes must be maintained for the organization to continue functioning effectively. Unauthorized changes to the systems, applications and organizational data can undermine the organization's credibility and viability. Also, violations of federal or state mandates and laws can lead to major penalties. All of these events have the potential to impact the organization’s ability to perform its mission and meet its goals and objectives.

Information Resources and related processes have three key elements which as a whole create ongoing risk(s) to the mission, goals and objectives. They are: Threats, Vulnerabilities, and Impacts.

Three Elements of Risk

Information Resources and the processes to use them are a vital part of the ongoing mission of the organization and its business goals and objectives. The following describes these three elements in more detail:

Threats – Threats can be both internal to the organization and external and come in many different forms. The common element is they work against the confidentiality, integrity, and availability of information resources. Some of the possible threats would be the alteration of data or systems or release of protected information whether intentional or un-intentional. Others would be competitors, hackers and other cyber criminals, acts of terrorism, viruses, and spyware to name a few.

Vulnerabilities – Vulnerabilities are weaknesses or holes in information resources and processes which allow the potential for unauthorized or unintentional change or manipulation of resources which impact the confidentiality, integrity, and availability of these resources.

Impacts – Impacts are the costs associated with failure in protecting the confidentiality, integrity, and availability of information resources. These costs can be increased expenses or outflows (fines, man hours, equipment replacement, legal fees, etc.) or decreased revenues or inflows (reduction in enrollment, donations, or endowments) due to negative publicity.

The threats, vulnerabilities, and impacts to information resources are not constant and will change over time. Because of this, the threats to, vulnerabilities of, and overall impact for every information resource, not only must be evaluated, but re-evaluated on a regular basis to ensure these ongoing risk(s) are continuously managed.

Managing Risk

To manage risk we must know what the risks are. To do this we must identify all information system resources and data, determine their importance and level of impact if compromised, determine the acceptable risk tolerance, and define the appropriate controls. In addition, we must also ensure processes are in place to allow and adjust for changes in the three key elements which will occur over time.

Policies, procedures, guidelines, and standards must be developed to define roles and responsibilities and provide guidance and directions. All of these pieces will need to be cyclical and re-occurring to ensure each information resource is not only evaluated, but re-evaluated regularly over time. They will also need to be omni directional to ensure relevant information collected as part of one process is identified, captured, and communicated to other processes to enable people to carry out their roles and responsibilities as effectively as possible and allow the entire risk management process to continually mature and grow.

We have divided this program into six functional areas which each have a unique primary standalone focus/purpose, while at the same time also rely on and support all the other functional areas allowing for both change and growth.

The following describes these six functional areas in more detail:

Control Activities – Policies and procedures are established, implemented, and enforced to help ensure the risk responses are effectively carried out. These policies and procedures can be mandated (Government, regulatory, Executive directives, etc.) and/or determined necessary through the ongoing efforts of the other functional areas.

Policies and Procedures will be established by Information Technology, implemented by all those defined by scope or where applicable, and will be enforced by internal and external IT audits. These policies, procedures, and any related documents will be posted to a central location as they are approved.

Resource Identification – Information system resources and data are identified and classified based on business impact as it relates to: Confidentiality, Integrity, and Availability to ensure all existing information resources are identified and appropriately classified, and any new information resources are identified and classified prior to deployment.

This functional area not only supports the other functional areas of the Risk Management Program, but also supports the Disaster Recovery Plan and

Business Resumption Plan by ensuring all information resources are known and have been appropriately prioritized for each of these plans.

In addition to identification and classification, this functional area will define an owner and a subject matter expert for the resource to be used as points of contact for the resource. Other information about the resource such as business function and information flow will be collected as well.

The information collected as part of this functional area will be centrally stored and managed to allow for various reporting requirements and tracking of review and assessment completion/compliance.

Control Review – Risks to information system resources and data are analyzed and likelihood and impact are considered as a basis for determining how they should be controlled and managed. This analysis will not only assess the impact of basic or inherent risks like weak passwords and permissions but will also look for any prolonged or residual risks like the lack of or the use of configuration and change controls or processes.

This is a complete assessment of each information resource where business impact, data and resource classification, and risk(s) are analyzed, existing controls are examined, and a determination made as to whether existing controls are appropriate or if new controls should be implemented. This area will also determined what mitigating controls can be implemented if a control does not exist to meet the appropriate level of control.

The control review process will completed by the resource owner or a delegate in conjunction with a subject matter expert on the resource, a subject matter expert (SME) for any and all supporting infrastructures, and a member of IT Information Security Services (ISS) for review. For a control review of an infrastructure it will be the responsibility of the SME's of the infrastructure to complete the review with ISS.

To ensure the results of the control review are agreed upon at an appropriate level, the control review will require an approval from a Director or higher from each of the following areas: IT ISS, Internal Audit, Compliance, and Legal.

Information collected as part of this functional area will be used to determine if the need exists to develop new policy, procedures, guidelines, or standards.

Risk Assessment – A regular self assessment is performed to ensure current resource and data classification are accurate and the appropriate controls are in place based on the latest control reviews and assessments. This is a self assessment conducted by the resource owner to validate compliance to all related policies and procedures.

This functional area serves two key roles. The first role is to address change. Threats, vulnerabilities, and impact can and will likely change over time. This assessment provides the method to quickly determine if the initial identification and classification are still valid and if they are still valid, to ensure the appropriate level of control determined during the Control Review are still in place and being utilized/managed properly. Any control found to be missing or not managed as previously defined by the control review, will be reported as a control issue to management and tracked until resolved.

The second role is to determine the need to redefine the control(s) or level of control being implemented. As technology, threats, vulnerabilities, and impact change so must the definition and level of controls. We do this by constantly evaluating the assessment questions to ensure the controls in question are still valid for the environment, adequately describe the requirement, and can be responded to accurately.

Information and Communication – Communication occurs in a broad sense, flowing down, across, and up the entity to ensure all information which aids in the protection of data and control of risk(s) is made available.

Because there is such a high level of risk associated with the formal identification of risk(s), any and all information collected through the performance of any functional area which identifies existing risk(s) will be considered confidential and protected accordingly.

Monitoring – The entirety of risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing risk management activities, separate evaluations, or both and enforced by Internal Audit.

Be Proactive instead of Reactive

The organization has internal and external auditors who perform regular risk assessments of information system resources and processes. These assessments do identify risks, but it forces all those involved to be placed in a reactive mode to fix all the findings of the assessment.

It is preferable to have colleges and departments to perform self–assessments and become self aware of the risks associated with their resources and processes and be able to identify and correct them before the auditors arrive.

However many departments do not have the IT, self-assessment expertise, or know how to know where to start.

It is a team effort

Identifying these critical resources or processes requires that IT work closely with managers and auditors to learn about the critical processes in their areas and with legal counsel to learn about related legislative requirements. It is necessary to identify associated IT security weaknesses, to evaluate and prioritize the associated risks, and to create teams who can help develop and implement an effective response strategy. This teamwork forms the foundation for an effective information security program.

To make all of these processes more manageable, the risk management process has been divided into three phases.

The Three Phases

To get our Risk Management Program implemented we will take a phased approach. The primary phases will consist of the following and will be described along with any sub-phases in greater detail below: Initial Development, Testing, and Awareness, Risk Analysis of Critical Areas and Processes, and Institution–Wide Risk Assessment.

Phase 1: Development and Testing

Initial Development Phase –This phase will consist of the creation of the initial policies, and supporting processes, procedures, standards, and guidelines. All of these documents will be drafted and presented to both internal and external groups for review and comment. We will also use Legal, Compliance, and Internal Audit to ensure the intent is thoroughly understood, binding, and enforceable/auditable. Revisions will be made as necessary to ensure the desired result for initial deployment.

Once the documents have been reviewed by all groups and any needed revisions made, they will presented to the appropriate executive level for approval. Once approved, they will be posted to an IT central respoitory accessible via the corporate website.

Initial Documentation Phase – It will be essential to keep a permanent record of all the documents and data collected as part of risk management. This phase will be used to determine methods of documentation, document management, and the storage of all data collected.

Initial Deployment Phase – In this phase, a new or existing information resource will be used to test the policies and related documents created during the Initial Development Phase and the records and document management processes/procedures developed during the Initial Documentation Phase. For this test a small group of IT departmental resources or a single IT managed enterprise level resource will be selected as a test environment. IT information resources will be used for this phase to ensure we have the resources and capabilities to support and complete these activities prior to complete deployment. Once selected, the Resource Identification and Control Review functional areas will be completed from start to finish for the resource(s).

Adjustment Phase – This phase will be implemented in conjunction with the Initial Deployment Phase. As the policies and related documents are implemented and performed during the Initial Deployment Phase, any issues identified as critical to the continuation of the Initial Deployment Phase will be addresses and adjustments made. These adjustments will go through the review process as indicated in the Initial Development Phase and then upon consensus and approval the new documents will be introduced as part of the test.

Adjustments will include modifications of policies and related documents, creation of new polices and/or related documents, and changes to document and record management processes/procedures.

Phase 2: Awareness and Area Assessment

Awareness Phase – This phase will consist of the creation of a risk management committee. This committee will consist of members from each college, IT, compliance, Internal Audit, and others as found necessary to ensure as much involvement as possible.

Initially, the risk management program will be introduced and explained to the members of the committee who will then be able to take what they have learned back to their departments. From there, the primary goal of this committee will be awareness. The committee will meet regularly as an open forum for information sharing and training when needed.

Collection Phase – Once the committee has been established, a collection process will be initiated through this committee to perform resource identification and classification. In this phase an in–depth look at what resources and data are being utilized and how they should be classified.

Second Deployment Phase –The collection phase will be used to identify the critical or sensitive information resources. These critical information resources will be the target of the second deployment phase in which a complete control review will be conducted.

As in the Initial Deployment Phase of Phase 1, this phase will continue to test all existing policies, procedures, and record management but this time will work in conjunction with the members of the committee to ensure clarity, understanding and alignment with business processes.

The committee will meet regularly throughout this phase and throughout all remaining phases as the primary communication channel through which information regarding security, risk management, and compliance with policy will flow to the rest of the organization.

Second Adjustment Phase – This phase, like the Adjustment Phase from Phase 1 will be implemented in conjunction with the Deployment phase and will be used to make any adjustments or changes needed to policies, procedures, or any other part of the process to ensure the process is working and the goals and objectives are being met.

Phase 3: Full Deployment

Goals and Objectives – Upon successful completion of the first two primary phases the program will be ready for full deployment. This phase is ongoing and has several goals and objectives to ensure the mission, goal, and objective of ISS is being met. The goals and objectives of the third phase are: to perform complete assessments on all remaining resources by area or department, to broaden or expand the scope of the assessments and tie them to business processes, schedule secondary review assessments, a new product review process, and continuous monitoring and measurements.

Remaining Assessments – All remaining information system resources will be identified, classified, and assessment performed. This will be done by area or department as determined and prioritized by management and the risk management committee.

As each of remaining areas/departments is addressed for each resource, the information collected will be used to make adjustments to the risk management program as needed and on a continuous basis.

Expanding Scope – Notably, these processes focus primarily on IT and process issues relating to risk. With the understanding that this is only part of the process, ultimately, risk assessment must take into account natural disasters, fire, and other non IT specific events that can make a system unavailable. Because of this the scope of the assessments will gradually be expanded during this phase to include these elements and others.

Tie to Business Processes – As the scope of the assessments expands the direct ties between the information system resources and business processes will become clearer and better defined. This will allow management to better determine the level which each information system resource supports the mission of the area, department, or organization as a whole.

These risk management processes will also aid business processes like the business continuity plans, business resumption plans, and disaster recovery plans by better identifying what information system resources exist and their overall priority to the University as a whole.

It has been emphasized that risk management is a process as opposed to a once–off event. As stated before, this is because technology, threats, vulnerabilities, and impacts all change over time and because of this, risk assessments must be repeated periodically.

Secondary Review Assessments – As part of the risk assessment of each resource, a determination will be made based on the classification and importance of the resource on the frequency at which the resource should be re-evaluated. Secondary Review Assessments will then be scheduled for the resource at the frequency determined to ensure the resource and its controls are reviewed periodically for compliance and adequacy.

New Product Review – Now that processes are in place for the assessment and secondary reviews of all resources, a process must be put in place to address new resources being developed or purchased. This is the Product Review.

The Product Review will provide a high level view of a resource under development or in research for purchase. This high level view will allow all groups/departments to preview the resource and its functionality. This will allow a determination to be made as to whether the product is needed, if a similar product is already available or been developed through/by another group or department, and/or if the resource brings any new security risks to the environment.

This process will also set the stage for the rest of the risk management processes. Once the product review process has been completed and approval granted the resource will be scheduled for its assessment.

Monitoring and Measuring – Throughout the execution of all risk management processes, monitoring and measurements will occur. This will be performed through the risk management committee, Information Security Services, and Internal Audit.