

1.0 Purpose

The purpose of this document is to establish standards for implementing security management procedures in adherence with the UCSF 650-16 Information Security and Confidentiality Policy.

The procedures in this document include:

- Risk Analysis (section 3.1)
- Risk Management (section 3.2)
- Sanction Policy (section 3.3)
- Information System Activity Review (section 3.4)

2.0 Definitions

2.1 Risk: A combination of, 1) the likelihood that a particular vulnerability in a UCSF information system will be intentionally or unintentionally exploited by a threat resulting in loss of confidentiality, integrity, or availability, and 2) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability could have on UCSF operations, assets, or individuals (including privacy) should the exploitation occur.

2.2 Risk Assessment: A key component of risk management that involves identification of: 1) threats and vulnerabilities, and 2) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability could have on organization operations (including functions, image or reputation), organization assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.

2.3 Risk Management: A process of identifying, controlling, and mitigating risks that includes: risk assessment, cost benefit analysis, and selection, implementation, testing, and evaluation of security controls.

2.4 Threat: Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system, resulting in a loss of confidentiality, integrity, or availability.

2.5 Threat Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

2.6 Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the system's security policy.

3.0 Procedures & Responsibilities

2.7 Workforce: All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

3.1 Risk Analysis: Implement procedures for conducting and documenting a risk analysis (Appendix A & B).

3.1.1 Define System Characterization: Define detailed system-related information of the system's processing environment.

- Hardware
- Software
- System interfaces
- Data and information
- Individuals who support and use the IT system.
- System function
- System and data sensitivity (i.e., the sensitivity of the information and therefore the level of protection necessary to guard information). Reference UC Business & Finance Bulletin IS-3, Electronic Information Security. <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf> section on Electronic Information Resource Sensitivity.
- System and data criticality (i.e., the system's value or importance to an organization). Reference UC Business & Finance Bulletin IS-3, Electronic Information Security section on Electronic Information Resource Criticality.
- Network topology
- Flow of information pertaining to the IT system

3.1.2 Identify Risks: The objective is to identify risks. To aid in this identification consider technical and nontechnical vulnerabilities and potential threat-sources that could exploit those vulnerabilities.

3.1.3 Analyze current and planned risk controls: The objective is to analyze the controls that have been implemented or are planned for implementation to minimize or eliminate the likelihood or probability of a threat source's ability to exploit a system's vulnerability.

Security controls encompass the use of technical and nontechnical methods. *Technical* controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and

authentication mechanisms, encryption methods, intrusion detection software). *Nontechnical* controls are management and operational controls such as security policies, operational procedures; and personnel, physical, and environmental security.

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. *Preventive* controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication. *Detective* controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

3.1.4 Determine threat likelihood: Determine the likelihood or probability of potential threats based on the following categories:

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

3.1.5 Analyze impact of threat: The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. *Integrity* is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Loss of *availability* occurs if an IT system is unavailable to its end users and

impedes the organization's ability to fulfill its required function. Loss of system and/or data *confidentiality* is the unauthorized, unanticipated, or unintentional access or disclosure of information.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the very costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's function, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's function, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's function, reputation, or interest.

3.1.6 Determine Risk Level: The objective is to assess the level of risk to the IT system. Risk for a particular threat/vulnerability pair is determined by the combination of the likelihood of a given threat-source's attempt to exploit a given vulnerability; the magnitude of the impact should a threat-source successfully exploit the vulnerability; and the adequacy of planned or existing security controls for mitigating risks.

The final determination of risk is derived by multiplying the ratings assigned for threat likelihood and threat impact.

The matrix below is a 3 x 3 matrix of *threat likelihood* (High, Medium, and Low) and *threat impact* (High, Medium, and Low).

Threat Likelihood	Impact		
	Low (10 - 40)	Medium (50 - 90)	High (100)
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Medium (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

Risk Scale: High (50 to 100), Medium (10 to >50), Low (1 to 9)

This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exploited. The risk scale also presents actions that senior management and/or the system owners must take for each risk level.

Risk Level	Risk Description and Necessary Actions
High	For a rating of a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	For a rating of a medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	For a rating of a low risk, the system's owner must determine whether corrective actions are still required or decide to accept the risk.

3.1.7 Recommend controls: Define controls for mitigating or eliminating the identified risks that are appropriate to the organization's operations. The objective of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.

3.1.8 Document Risk Assessment results: Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls defined), the results should be documented in a Risk Assessment report. See Appendix A. Sample Risk Assessment Report Outline.

3.1.9 Process Flow Reference: See Appendix B. Risk Analysis

Process Flow.

3.2 Risk Management: System managers and owners must implement procedures for conducting a risk management process.

3.2.1 Prioritize Actions: Based on the risk levels identified in the risk assessment report, prioritize the actions required to implement specific controls.

3.2.2 Evaluate recommended control options: The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization and IT system. During this step, evaluate and analyze the *feasibility* (e.g., compatibility, user acceptance) and *effectiveness* (e.g., degree of protection and level of risk mitigation) of the recommended control options. The objective is to select the most appropriate control option for minimizing risk.

3.2.3 Conduct Cost-Benefit Analysis: To allocate resources and implement cost-effective controls, after identifying all possible controls and evaluating their feasibility and effectiveness, organizations should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances. The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend \$1,000 on a control to reduce a \$200 risk.

3.2.4 Select Controls: On the basis of the results of the cost-benefit analysis, system owners should determine the most cost-effective control(s) for reducing risk to the organization's function. The selected controls should combine technical, operational, and management control elements to ensure adequate security for the IT system and the organization.

3.2.5 Assign Responsibility: Identify the appropriate individuals (in-house personnel or external contracting staff) who have the required expertise and skill-sets to implement the selected control and assign responsibility specific to the required implementation tasks.

3.2.6 Develop Safeguard Implementation Plan: During this step, develop a safeguard implementation plan (or action plan). The safeguard implementation plan prioritizes the actions and

projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. The plan should, at a minimum, contain the following information:

- Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- Recommended controls (output from risk assessment report)
- Prioritized actions (with priority given to items with Very High and High risk levels)
- Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- Required resources for implementing the selected planned controls
- Lists of responsible individuals, teams and staff
- Start date for implementation
- Target completion date for implementation
- Maintenance requirements

See Appendix D: Sample Risk Management Plan template

3.2.7 Implement selected controls: Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk. *Residual risk* should be identified and documented within the Safeguard Implementation Plan.

3.2.8 Perform ongoing Risk Management: Perform the risk management process on an ongoing basis, periodically assessing risks and implementing new controls in response to changes in information systems as well as federal, state, and university policy.

3.2.9 Process Flow Reference: see Appendix C. Risk Management Process Flow

3.3 Workforce Sanction Process:

Violation of any of the University's policies and procedures related to the privacy or security of any individually identifiable personal health or financial information or of any state or federal laws or regulations governing a patient's right to privacy or security may result in legal and/or disciplinary action up to and

including immediate termination of the employment/professional relationship with UCSF. Sanctions, including remedial, corrective or disciplinary actions, will be consistent with appropriate University of California policies, and workforce members may be personally liable for civil and criminal penalties.

The HIPAA Security rule that governs this procedure is: *164.308(a)(ii)(C) Sanction Policy (Required)*. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

3.3.1 Remedial Actions: Remedial actions are not disciplinary but are done to correct mistakes and enhance compliance and will be in accordance with existing University policies and procedures. In most cases, remedial actions are designed to improve the performance of University personnel. The exact nature of and need for remedial action will be identified by supervisors within departments and may involve department chairs, deans and the Academic Senate as appropriate.

3.3.2 Corrective or Disciplinary Actions: In cases of intentional misconduct, repeated violations, or after documented remedial actions have failed to correct the problem, the University will initiate corrective or disciplinary actions where necessary. The initiation of corrective or disciplinary action by the University does not preclude or replace any criminal proceedings that may be taken by the district attorney.

Should the University initiate corrective or disciplinary action it must do so in accordance with the rules set forth in the *Faculty Code of Conduct, the Medical Staff Bylaws, Rules and Regulations*, as well as any other existing and applicable personnel policies, collective bargaining agreements, or University policies and procedures.

3.4 Information System Activity Review: Implement procedures for conducting information system activity reviews:

3.4.1 List Identified risk: Perform a risk analysis to identify the particular vulnerabilities of individual systems.

3.4.2 Develop audit trails: Develop audit trails specific to each system that contain system and user events.

- 3.4.3 Define system activity reviewers:** Identify the individuals who are authorized and responsible for reviewing system activity.
- 3.4.4 Define objectives of the system activity review:** List the specific objectives of the system activity review for the review team. The list should include the following objectives, at least:
- Identify breaches of security policies
 - Identify if there are faults within the application or computing environment
 - Identify attempts to penetrate a system to gain unauthorized access
- 3.4.5 Define system activity review methods:** Establish the tools and methods that the review team will utilize to examine system activity.
- 3.4.6 Define frequency of system activity reviews:** Define the schedule and frequency of the reviews (daily, weekly, monthly, annual).
- 3.4.7 Conduct system activity reviews**
- 3.4.8 Document results of system activity reviews**

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rule: Security Management Process	164.308(a)(1) http://www.ucsf.edu/hipaa/dept_compliance/
Information Security and Confidentiality Policy	5.01.04 Med Center 650-XX Campus http://www.ucsf.edu/hipaa/dept_compliance/
System Audit Controls Procedures	60-014 http://www.ucsf.edu/hipaa/dept_compliance/
UCSF Campus and UCSF Medical Center Departmental HIPAA Security Compliance web site	http://www.ucsf.edu/hipaa/dept_compliance/
<p>Example documents:</p> <ul style="list-style-type: none"> • UCSF HIPAA Security Assessment Plan • UCSF HIPAA Security Assessment Checklist • Toolkit for System Administrators/System Owners • Risk Analysis Template • Risk Assessment Summary Report Template • Threats, Vulnerabilities and Safeguards 	

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	1/28/2005	Dan Yee, IT, Guy Zuzovsky, SOM HR, David Odato, HR, and Mike Tyburski, HR. Modified to match SOM template.	Initial Release

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Appendix A: Sample Risk Assessment Report Outline

Executive Summary

1.1 Scope

The security risk assessment addresses the following questions:

- What needs to be protected?
- What security measures are currently in place?
- Who and what are the threats and vulnerabilities?
- What are the implications if they were damaged or lost?
- What is the value to the business unit?
- What can be done to minimize exposure to the loss or damage?

A Risk Analysis includes the following activities:

- Identify system risks
- Determine risk probabilities
- Assess potential risk impact
- Rank risks in order of probability and impact
- Determine acceptable levels of risk

Example scope statement: The Risk Assessment analyzed specific areas of vulnerability including Organizational, Administrative, Technical, and Physical vulnerabilities and the extent to which the threats posed a risk to UCSF Medical Center. The assessment did not include external threats such as Nuclear Mishap, Biological Contamination, and Catastrophic Weather/Geological phenomenon.

1.2 Risk Analysis Steps

- Summarize steps taken during analysis

Examples:

1.2.1 *Assessed each of the servers maintained by the department and evaluated the locations of those devices to determine security risks and vulnerabilities.*

1.2.2 *Evaluated backup activities to determine whether they are incremental or full backups and whether the backup media is stored in a secured storage locker and/or closet or room.*

1.2.3 *Evaluated existing methods for approving, establishing, modifying and deactivating end-user accounts.*

- Summarize method used to account for assets, including hardware and software inventory, all devices and electronic storage/media that could contain ePHI.

Examples:

1.2.4 *Conducted a physical inventory of all departmental assets; paying special attention to those devices that may contain ePHI.*

- Summarize assumptions used in determining movement of ePHI that could be transmitted.

Examples:

1.2.5 *Consideration given to the likelihood that ePHI could be transmitted between physicians and clinicians within and outside the department.*

- Summarize identified situations that ePHI could be lost, stolen, sent to the wrong party, destroyed, made inaccessible, or altered.

Examples:

1.2.6 *Local servers are not backed up and they are not kept in a locked room.*

1.2.7 *Access to the room is not strictly controlled by use of proximity cards or other means.*

1.2.8 *Access to ePHI applications does not require unique user ID access.*

1.2.9 *Auditing features are not available on most of the ePHI applications.*

1.2.10 *Department does not enforce and adhere to security incident reporting procedures.*

1.2.11 *If access to data required to conduct business functions is lost, the department has not implemented downtime procedures.*

1.3 Key Risk Analysis Report Findings

1.3.1 Assets

- Summarize the assets in your business unit

1.3.2 Risks and Vulnerabilities

- Summarize the current risks and vulnerabilities

Examples:

- *Departmental server is not physically secure due to the fact that it is kept under an employee's desk.*

- *Procedures that ensure that access to department information assets is curtailed when an individual transfers to another department are not in place*

- *Backup tapes are not sent offsite.*

1.3.3 Threats

- Summarize the current threats

Examples:

- *Server can be physically damaged. Unauthorized access cannot be prevented.*
- *User may continue to access department information when there is no longer a need for such access.*
- *Backup tapes may not be available in the event of an emergency.*

1.3.4 Safeguards

- Summarize current and planned safeguards

Examples:

- *Relocate server into a locked room and strictly control access only to those individuals who are responsible for maintaining the server.*
- *Implement access control procedures that ensure an individual's access to the department, systems and data is deactivated when they are no longer employed in the department.*
- *Establish a method to ensure that backup tapes are readily available for use in the event of an emergency.*

2 Recommendations

If not corrected, the vulnerabilities you have identified could result in considerable loss to your department. List the immediate and long-term steps that you will take to remediate the risk exposures.

2.1 Immediate Remediation Steps

Examples:

2.1.1 *Create a departmental procedure that will ensure that when someone leaves the department, access to departmental information is curtailed.*

2.1.2 *Put personal firewalls on servers; relocate servers into a locked room with strictly controlled access.*

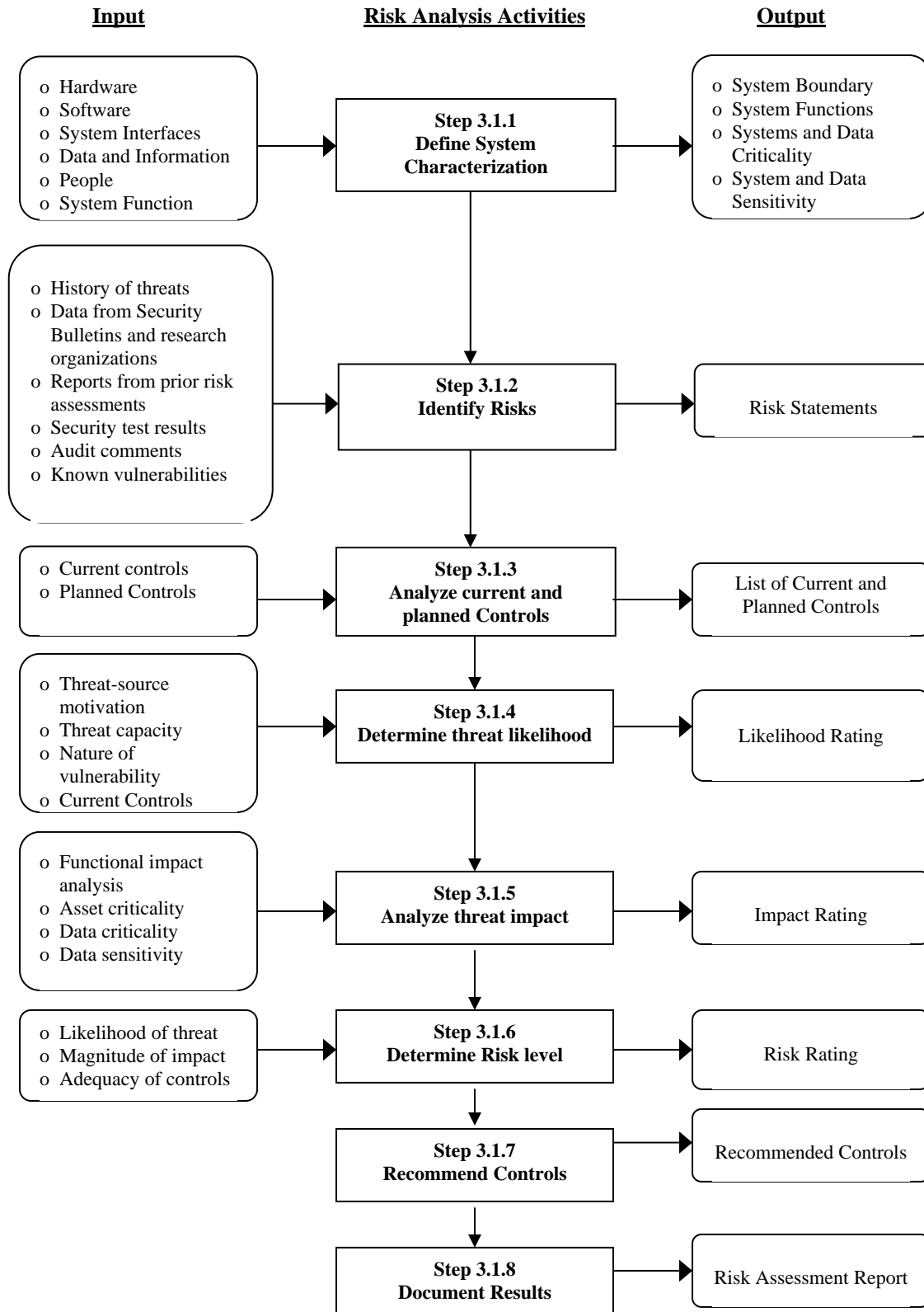
2.1.3 *Begin sending backup tapes offsite.*

2.2 Long-term Remediation Steps

Examples:

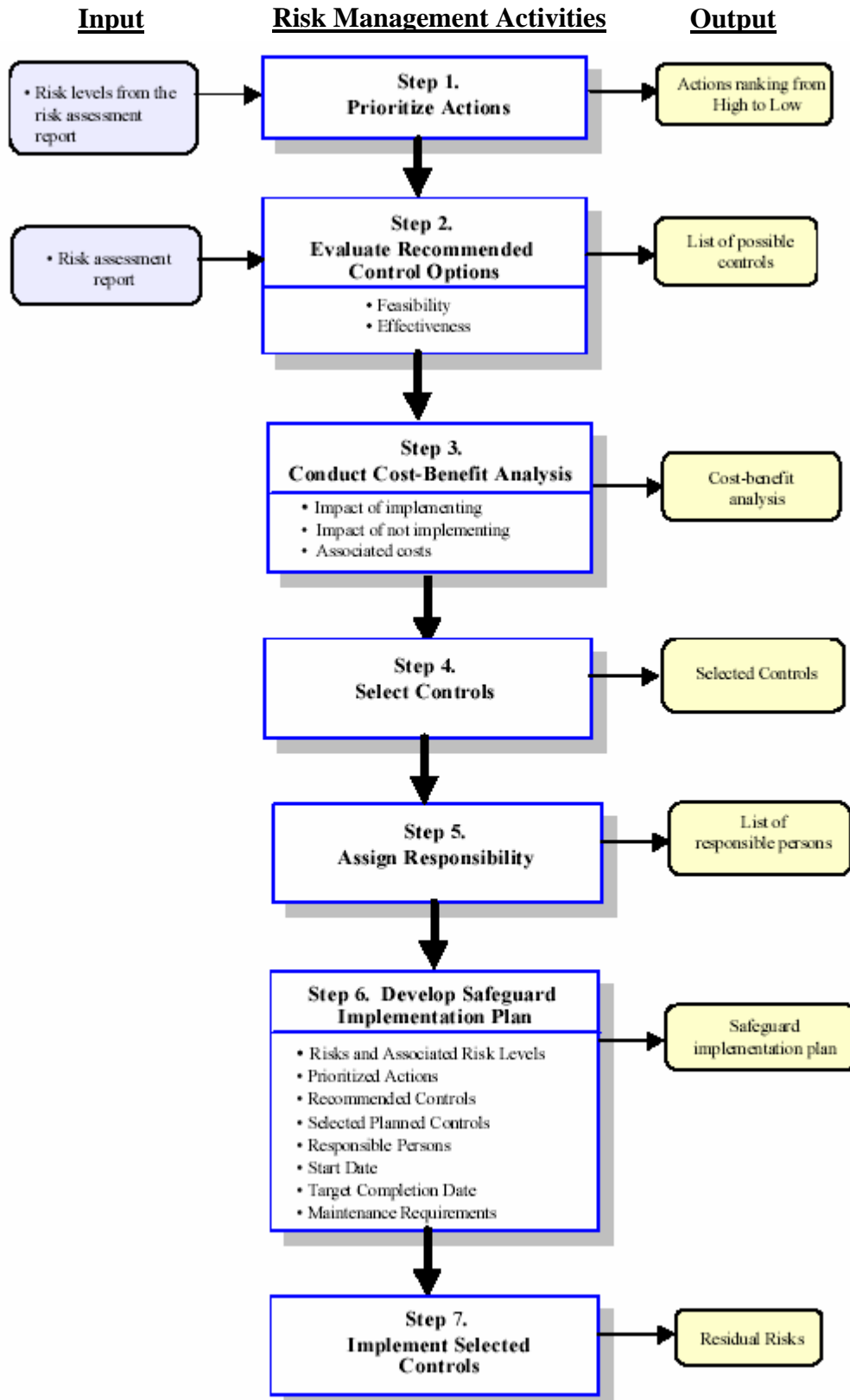
Develop physically secured area for departmental servers.

Appendix B: Risk Assessment Process Flow



If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.

Appendix C: Risk Management Process Flow



Appendix D: Sample Risk Management Plan Template

(1) Risk (Vulnerability/ Threat- Source Pair)	(2) Risk Level	(3) Recommend ed Controls	(4) Priority	(5) Recommended Control Status	(6) Required Resource s	(7) Responsible Team/ Persons	(8) Start / End Date	(9) Mainten ance Require ment	Comments
Unauthoriz ed users can telnet to XYZ server and browse sensitive company files with the <i>guest</i> ID.	High	Disallow inbound telnet	High	Disabled the <i>guest</i> ID	10 hours to reconfigur e and test the system	John Doe, XYZ server system administrator; Jim Smith, company firewall administrator	9-1-03 to 9-2-03		
Unauthoriz ed users can telnet to XYZ server and browse sensitive company files with the <i>guest</i> ID.		Disallow .world access to sensitive company files	High	Disabled the <i>guest</i> ID	10 hours to reconfigur e and test the system	John Doe, XYZ server system administrator; Jim Smith, company firewall administrator	9-1-03 to 9-2-03		
Unauthoriz ed users can telnet to XYZ server and browse sensitive company files with the <i>guest</i> ID.		Disable the <i>guest</i> ID or assign difficult- to-guess password to the <i>guest</i> ID	High	Disabled the <i>guest</i> ID	10 hours to reconfigur e and test the system	John Doe, XYZ server system administrator; Jim Smith, company firewall administrator	9-1-03 to 9-2-03		

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.