[redacted]

RISK ANALYSIS & RISK MANAGEMENT

Table of Contents

PREFACE **2**

PART 1: RISK ANALYSIS **3**

Introduction
Objective of Risk Analysis
Risk Assessment
Risk Evaluation
Risk Matrix
Risk Analysis Integration

PART 2: RISK MANAGEMENT **7**

Introduction
Objective of Risk Management
Evaluation of Controls
Prioritization and Selection of Controls
Implementation of Controls
Continual Risk Management Methodologies

APPENDIX **10**

A. Sample Assessment Questions
B. Risk Assessment Report Outline
C. Sample Control Implementation Plan

[redacted]

RISK ANALYSIS & RISK MANAGEMENT

Preface

This document represents guidelines excerpted from NIST SP 800-30 *Risk Management Guide for Information Technology Systems.* The ideas and methodologies described in this document have been adopted by CompanyX as part of its standard operating procedures.

__________ ______________________________ ______________________
Date Signature Title

__________ ______________________________ ______________________
Date Signature Title

__________ ______________________________ ______________________
Date Signature Title

__________ ______________________________ ______________________
Date Signature Title

Revision History

Revision #	Effective Date
1.0	

PART 1:

RISK ANALYSIS

Introduction

Risk is defined by NIST as anything that would impact the organization's ability to perform their mission. In this context, we consider CompanyX's mission statement:

"To guide individuals through the complex healthcare environment toward healthier living, measurably reducing health-related costs."

When evaluating risk, we must consider both the probability of occurrence and the impact the occurrence would have. According to NIST:

> ***Risk*** is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization.

Risk analysis and risk management require involvement and effective support by all aspects of the organization. At CompanyX, this includes senior management, the CIO, system information owners, business and functional managers, the CompanyX Systems Security Officer, and all of the IT operations staff. Structured methodologies must be in place to support risk analysis and risk management activities. This document attempts to create such a framework within CompanyX. As with all management decisions, trade-offs must be made between risk considerations and operational considerations, and these decisions must be made in concert with others throughout the organization. Central to the concept of risk analysis is that (a) all system changes are appropriately evaluated, approved, and implemented only after a risk analysis has been done, and (b) training is provided at all levels to minimize risks.

Objective of Risk Analysis

The objectives of risk analysis activities at CompanyX shall be to:
(1) Identify risks – via performance of a risk assessment;
(2) Evaluate each risk according to probability and impact – via performance of a risk evaluation;
(3) Determine which risks to address– via creation of a risk matrix;
(4) Devise methodology for continual risk analysis – via integration of risk analysis into daily operations.

Each of these is discussed in detail below.

Risk Assessment

In order to identify risks, a risk assessment shall be performed of each system at CompanyX. This assessment shall include system characteristics such as:

- Hardware, software, connectivity
- Operational environment, including physical & network security
- Boundaries, interfaces (internal, external)
- System functions, purpose (mission)
- Data criticality (importance to the organization)
- Data sensitivity

- People using and supporting it
- Applicable security policies (organizational, federal laws, etc.)
- History of prior threats
- List of vulnerabilities, including results of security tests
- Current controls in place, how they are configured/used, effectiveness (authentication, encryption, backup, etc.)

Information gathering for risk assessment is done through:

- questionnaires and/or on-site interviews - see sample provided in Appendix A;
- observations and experiences of staff associated with the systems;
- reviews of documents, such as policies, security audit test results, and prior risk analyses;
- quarterly security self-audits, as well as annual external security audits – these include penetration and vulnerability testing, as well as assessment of compliance to CompanyX' security policies and procedures; and
- reports of security concerns made through the CompanyX Security Compliance Hotline – note that security concerns made be made anonymously through this vehicle.

Risk Evaluation

For each vulnerability or threat identified in the assessment, a risk evaluation shall be done. The intent of risk evaluation is to determine:

- Where the threat comes from (sources)
- Situation(s) that triggers the threat
- Controls in place or planned (intrusion detection tools, etc.)
- Likelihood of threat occurring (rate as High, Medium, or Low)
- Impact, i.e., effect of loss of integrity, availability, and confidentiality (rate as High, Medium, or Low)
- Adequacy of current and planned controls
- Recommendation for new controls

A sample outline for a Risk Assessment Report is provided in Appendix B.

Threats which are common to most systems, and should be evaluated for each system include, but are not limited to:

1. Human Threats, such as:
    - Errors & Omissions: data entry errors, programming errors (bugs).
    - Fraud & Theft: break-ins, computer theft, fraudulent act (e.g., replay, impersonation, interception), information theft, industrial espionage, information bribery.
    - Employee Sabotage: destruction of hardware and facilities, deleting data, bomb/terrorism, system tampering, disabling/bypassing security measures.
    - Malicious Hacking: hacking, social engineering, system intrusion, unauthorized system access, computer crime (e.g., cyberstalking), spoofing, information warfare, system attack (e.g., distributed denial of service), system penetration, economic exploitation, intrusion on personal privacy, access to business secrets (proprietary, and/or technology-related information), assault on an employee, blackmail, computer abuse, input of falsified or corrupted data, malicious code (e.g., virus, logic bomb, Trojan horse, worm), sale of personal information, password guessing.

2. Natural/Environmental Threats, such as:
    - Loss of physical infrastructure support, due to flood, earthquake, tornado, landslide, fire, avalanche, electrical storm, power outage, liquid/chemical spill.

Of the two major threat sources, human threats by far make up the majority and are often the hardest to guard against. Sources of human threats include terminated/disgruntled employees, cyber criminals, industrial espionage, terrorists, insiders (dishonest employees), unintentional (poorly trained users, data entry/programming error), unauthorized users, and vendors.

Risk Matrix

To determine which risks to mitigate, a qualitative analysis of each risk is performed, based on the likelihood and impact (see definition of levels below). Then, a risk matrix can be created.

Likelihood Level – categorize the likelihood of each risk as:

- High - The threat-source is highly motivated and sufficiently capable, and the 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.

Impact Level – categorize the impact of each risk as:

- High - Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, 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 mission, 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 mission, reputation, or interest.

Note that "impact level" is also called BIA = business impact analysis. It is the impact on the business if that risk is allowed to occur.

To construct a quantitative Risk Matrix, follow these steps:

1. Assign probabilities for the likelihood: 1.0 for High, 0.5 for Medium, and 0.1 for Low.
2. Assign values for the impact: 100 for High, 50 for Medium, 10 for Low.
3. Multiply the likelihood probability by the impact value.

Quantitatively, such a risk matrix may be represented thusly:

Risk Likelihood	1.0	10	50	100
	0.5	5	25	50
	0.1	1	5	10
		10	50	100
		Risk Impact		

Next, assign an overall risk level, where High = >50-100, Medium = >10-50, and Low = 1-10. Then, based on the overall risk level, take the appropriate actions. See below.

Overall Risk Level:

- High - If an observation or finding is evaluated as 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 - If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
- Low - If an observation is described as low risk, the system's designated approving authority (at CompanyX, this is often the VP of Enterprise Systems or Systems Security Architect) must determine whether corrective actions are still required or decide to accept the risk.

The output of the Risk Analysis is a recommendation on which risks should be addressed (controlled) based on their risk level. The selection of the control method and its implementation is part of Risk Management.

Risk Analysis Integration

To have an effective risk analysis program, it is essential that CompanyX integrate risk analysis into daily operations and throughout each system's lifecycle. Below is a sampling of lifecycle activities:

a. Planning of new systems – Security strategies are taken into consideration and incorporated into the scope.
b. Development of systems – As systems are purchased or developed (programmed), security analysis is done and influences the architecture and design during development (how the system is constructed). A security requirements checklist is developed for the system and documented.
c. Implementation of systems – Decisions are made with regard to how system security features are configured, enabled, tested and verified. Test plans for systems include system security testing to ensure that applied controls are meeting the security standard/policy. See also NIST SP 800-53A.
d. Operation & maintenance of systems – Daily on-going functions are being performed according to processes, policies and procedures. Periodically, systems are re-assessed for risk management activities. This occurs yearly or when system changes occur (such as adding a new interface).
e. Disposal of systems – Disposal, archiving, replacement, or sanitizing hardware and software is done in a secure and systematic manner, to ensure residual data is appropriately handled.
f. Testing of systems – Use of an automated vulnerability scanning tool, periodic penetration testing, and/or external security evaluations are employed.

To be effective, these risk analysis activities must be made part of CompanyX's standard operating processes. It is essential that the Systems Security Architect (or designated internal or external IT security personnel) is incorporated into all systems-related projects at CompanyX throughout the system's lifecycle. Project management tasks corresponding to these activities shall be included in all project plans in which these system lifecycle events occur.

PART 2:

RISK MANAGEMENT

Introduction

Risk Management is defined by NIST as the implementation of mitigation strategies to reduce risks to an acceptable level. In practice, it means protecting systems and data that support the mission by balancing operational and economic costs of protective measures.

A successful risk management program relies upon:

- senior management's commitment;
- full support and participation of the IT team;
- competence of the risk assessment, e.g., having the expertise to apply the risk assessment methodology, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization;
- awareness and cooperation of users who must follow procedures and comply with the implemented controls; and
- ongoing evaluation and assessment of risks.

Objective of Risk Management

The objectives of risk management activities at CompanyX shall be to:
(1) Evaluate risk control methods;
(2) Prioritize and select controls;
(3) Implement controls; and
(4) Devise a methodology for continued risk management.

These are discussed in detail below.

Evaluation of Controls

Control of risks can be via technical or non-technical methods.

- Technical controls: 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: management and operational controls, such as security policies, operational procedures, and personnel, physical, and environmental security.

Additionally, a control may be:

- preventive – inhibits attempts to violate security, or
- detective – warns of violations or attempted violations.

In evaluating controls, all methodologies must be considered. At CompanyX, multiple methodologies are often applied. Ways of improving current control methodologies are also considered. This is a continually evolving science and art. It is important to note that risk mitigation strategies are effective at reducing but not totally eliminating risk. Therefore, any residual risk(s) must still be assessed and addressed.

Prioritization and Selection of Controls

The controls applied must be prioritized based on cost-benefit analysis, operational impact, feasibility, and effectiveness.   It is CompanyX's approach to look for the least-cost approach and implement the most appropriate controls to decrease risk to an acceptable level, with minimal adverse impact on the organization's resources and mission. This sometimes must be done collaboratively with other stakeholders.

After identifying all possible controls and evaluating their feasibility and effectiveness, a cost-benefit analysis must be conducted in order to demonstrate that the costs of implementing the control(s) can be justified by the reduction in level of risk. For example, it may not be worthwhile to spend $1,000 on a control to reduce a $200 risk. When performing a cost-benefit analysis, CompanyX shall consider the following:

1. Determine the impact of implementing the new control(s), as well as the impact of not implementing the new control(s). Relate the cost of not implementing it to the impact on the mission.
2. Estimate the costs for implementation, including hardware/software purchases, implementation policies and procedures, personnel resources, training, maintenance, and whether the implementation of the control reduces effectiveness or productivity (for example, if the increased security reduces system performance or functionality).
3. If the control would cost more than the risk reduction provided, or if it does not reduce risk sufficiently, then look for something else.

CompanyX's policy shall be to select the control(s) which best address the risk from an effectiveness, feasibility, operational impact and cost-benefit standpoint.

Implementation of Controls

Implementation of the selected control(s) requires:

- determining resources,
- assigning responsibility, and
- developing an implementation plan.

A sample Risk Implementation Plan is shown in Appendix C. It is important to note that implementation of many technical controls require standard procedures – such as CompanyX's Change Management Process – be utilized, so as to limit the turbulence and potential risk to the existing computing environment.   Implementation of some controls may require a full-scale project plan, complete with milestones and approvals at various steps, or are themselves part of a larger project, such as a new system implementation. Non-technical controls, such as policies and procedures, are revisited annually, and are part of CompanyX's continuing process improvement program.

Continual Risk Management Methodologies

Risk management must be continual, throughout the lifespan of a system. Any time there are major changes to the system, software, or network, a re-evaluation and assessment must be completed. New risks may surface, or the residual risks may have changed, and if increased substantially, must be addressed. Additionally, new laws/regulations, or changes in policies and procedures, or changes in the business objectives or mission, necessitate re-evaluation.

It is CompanyX's policy that a complete systems risk assessment shall be completed no less frequently than every 3 years, and that the results shall be signed off by the CIO, Systems Security Officer, VP of Enterprise Systems, and IT Directors. On-going training and awareness shall be completed for key systems staff regularly.

APPENDIX A:

SAMPLE ASSESSMENT QUESTIONS

Sample questions to be asked during interviews with systems and business operations personnel to gain an understanding of the operational characteristics of each system include:

- Who are the valid users? How are invalid users prevented?
- What is the mission of the system or application? What role does it serve within the organization as a whole?
- How important is the system (and/or the information gathered/stored by it) to CompanyX's mission? What is its criticality?
- What is the system availability requirement? Are there usage peaks and valleys?
- What information (both incoming and outgoing) is required? From/to what sources?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system or application?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g., financial, personnel, research and development, medical, command and control)?
- What is the sensitivity (or classification) level of the information? Does it include confidential information and/or PHI?
- What information handled by or about the system should not be disclosed and to whom?
- Where specifically is the information processed and stored?
- What are the types of information storage? Are there temporary or archival storage requirements?
- What is the potential impact on the organization if the information is disclosed to unauthorized personnel?
- What are the requirements for information availability and integrity? From a contractual, legal and operational perspective?
- What is the effect on CompanyX's mission if the system or information is not reliable or unavailable?
- How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time?
- What other processing or communications options can the user access?
- Could a system or security malfunction or unavailability result in injury or death?

APPENDIX B:

SAMPLE RISK ASSESSMENT REPORT OUTLINE

EXECUTIVE SUMMARY

I. Introduction

- Purpose
- Scope of this risk assessment
- Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.

II. Risk Assessment Approach

Briefly describe the approach used to conduct the risk assessment, such as:

- The participants (e.g., risk assessment team members)
- The technique used to gather information (e.g., the use of tools, questionnaires)
- The development and description of risk scale (e.g., risk-level matrix).

III. System Characterization

- Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users.
- Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

V. Risk Assessment Results

List the observations (vulnerability/threat pairs). Each observation must include:

- Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
- A discussion of the threat-source and vulnerability pair
- Identification of existing mitigating security controls
- Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk.

VI. Summary

Total the number of observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

APPENDIX C:

SAMPLE CONTROL IMPLEMENTATION PLAN SUMMARY

1. **Risk (Vulnerability/Threat Pair)**
   Example: Unauthorized users can telnet to XYZ server and browse sensitive company files with the guest ID.
2. **Risk Level**
   Example: High
3. **Recommended Controls**
   Example:
   - Disallow inbound telnet
   - Disallow "world" access to sensitive company files
   - Disable the guest ID or assign difficult-to-guess password to the guest ID
4. **Action Priority**
   Example: High
5. **Selected Planned Controls**
   Example:
   - Disallow inbound telnet
   - Disallow "world" access to sensitive company files
   - Disabled the guest ID
6. **Required Resources**
   Example: 10 hours to reconfigure and test the system
7. **Responsible Team/Persons**
   Example: John Doe, XYZ server system administrator; Jim Smith, company firewall administrator
8. **Start Date/End Date**
   Example: 9-1-2008 to 9-2-2008
9. **Maintenance Requirement/Comments**
   Example: Perform periodic system security review and testing to ensure adequate security is provided for the XYZ server

Notes:
(1) The risks (vulnerability/threat pairs) are output from the risk assessment process
(2) The associated risk level of each identified risk (vulnerability/threat pair) is the output from the risk assessment process
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources (e.g., funds, people, technology)
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) List of team(s) and persons who will be responsible for implementing the new or enhanced controls
(8) Start date and projected end date for implementing the new or enhanced controls
(9) Maintenance requirement for the new or enhanced controls after implementation.