# Risk Assessment Process

|  |
| --- |
| Contents  * 1 Purpose, Timeline, and Overview * 2 Roles and Responsibilities * 3 System Characterization   + 3.1 System-Related Information   + 3.2 Information-Gathering Techniques * 4 Threat identification   + 4.1 Threat-Source Identification   + 4.2 Motivation and Resources of Threat Actors     - 4.2.1 Threat Sources * 5 Vulnerability Identification   + 5.1 Vulnerability Sources   + 5.2 System Security Testing   + 5.3 Development of Security Requirements Checklist * 6 Control Analysis   + 6.1 Control Methods   + 6.2 Control Categories   + 6.3 Control Analysis Technique * 7 Likelihood determination * 8 Impact Analysis * 9 Risk Determination   + 9.1 Risk-Level Matrix   + 9.2 Description of Risk Level * 10 Control Recommendations * 11 Results Documentation * 12 Risk Management Techniques * 13 Create a risk-management plan * 14 Implementation   + 14.1 Prioritize Actions   + 14.2 Evaluate Recommended Control Options   + 14.3 Conduct Cost-Benefit Analysis   + 14.4 Select Controls   + 14.5 Assign Responsibility   + 14.6 Implement Selected Control(s) * 15 Reassess After Environment Changes * 16 Testing and Review Procedures * 17 External Resources |

## Purpose, Timeline, and Overview

This document establishes a risk assessment process for the Cardholder Data Environment (CDE) at the ACME-NA division of ACME Corporation. This risk assessment process will be exercised annually to test security controls, limitations, network connections, and restrictions so that we can adequately identify and to stop any unauthorized access attempts.

Risk assessment is a key part of an effective risk management process. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. It process gives corporate leaders the information necessary to balance the operational and economic costs of protective measures. It encompasses four processes: risk assessment, risk mitigation, and evaluation and assessment. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

## Roles and Responsibilities

Risk management is a management responsibility. This section describes the key roles of the personnel who support and participate in the risk management process.

* **Senior Management**. Senior management must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.
* **IT Management Team**. The IT Management Team is responsible for the company's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
* **System and Information Owners**. The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.
* **Business and Functional Managers**. The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment.
* **Security Team**. The Security Team is responsible for proper implementation of security requirements in all corporate IT systems. As changes occur in the existing IT system environment, the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems. They must also ensure the use of the IT systems and data according to company policies, guidelines, and rules of behavior.

## System Characterization

The first step is to define the scope of the effort. In this step, we will define the boundaries of the CDE, identify the resources and the information that constitute the system, identify the regulatory and compliance requirements, and compile system information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to completing a thorough assessment.

### System-Related Information

Identifying risk for an IT system requires a keen understanding of the system’s processing environment. Security Team will collect information about the CDE including:

* Hardware & Software
* System interfaces (e.g., internal and external connectivity)
* Data and information (e.g. internal and external data flow, processing, and storage).
* Persons who support and use the IT system
* System purpose/mission
* System and data criticality and sensitivity.

Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:

* The functional requirements of the IT system
* Users of the system (e.g., system users, application users, customers, third parties)
* System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
* System security architecture
* Current network topology (e.g., network diagram)
* Information storage protection that safeguards system and data availability, integrity, and confidentiality
* Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
* Technical controls used for the IT system (e.g., identification and authentication, access control, audit, encryption)
* Management controls used for the IT system (e.g., rules of behavior, security planning)
* Operational controls used for the IT system (e.g., personnel security, backups, contingency, account and management; segregation of user functions)
* Physical security environment of the IT system (e.g., facility security, data center policies)
* Environmental security implemented for the IT system processing environment.

### Information-Gathering Techniques

A combination of the following techniques will be used in gathering information relevant to the CDE:

* Questionnaire. To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system.
* On-site Interviews. Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed).
* Document Review. Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system.
* Use of Automated Scanning Tools. Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

## Threat identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls.

### Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile list of potential threat-sources that are applicable.

* Natural Threats—Floods, tornadoes, electrical storms, and other such events.
* Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts or deliberate actions.

### Motivation and Resources of Threat Actors

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

#### Threat Sources

Below is a list of resources to help us develop a list of potential threats actors:

* Previous incident reports
* Security news, forums, conferences
* Billing/Development managers and staff
* ACME community managers who are in touch with the players
* Partnerships and informal discussions with other online game security teams.
* Discussions with ACME HQ Security Team

## Vulnerability Identification

### Vulnerability Sources

We will identify potential technical and nontechnical vulnerabilities associated with systems in the CDE through information-gathering techniques. We will review the following information sources as we build a list of potential vulnerabilities to test and confirm.

* Previous risk assessments, security review reports, and system test and evaluation reports
* Automated system audit reports, system anomaly reports and security event logs
* System documentation and diagrams including architecture and controls
* Vulnerability lists, such as the CVE
* Security and update advisories from vendors, US-CERT, Secunia, SecurityFocus and SANS

### System Security Testing

System security testing will be used to identify system vulnerabilities efficiently. Testing will positively confirm or deny all "potential" vulnerabilities

Test methods include:

* Network-layer penetration tests using automated scanning tools
  + Internal Network Pentest
  + External Network Pentest
* Application-layer penetration testing using automated scanning tools and manual code review
  + Web Application Vulnerability Tester
  + Custom Code Review

### Development of Security Requirements Checklist

Determine if the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system’s design or implementation does or does not satisfy that security control requirement. A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, and information), non-automated procedures, processes, and information transfers associated with a given IT system in the following security areas:

**Management Security**

* Assignment of responsibilities
* Continuity of support
* Incident response capability
* Periodic review of security controls
* Personnel clearance and background investigations
* Risk assessment
* Security and technical training
* Separation of duties
* System authorization and reauthorization
* System or application security plan

**Operational Security**

* Data media access and disposal
* External data distribution and labeling
* Facility protection (e.g., computer room, data center, office)
* Workstations, laptops, and stand-alone personal computers

**Technical Security**

* Communications (e.g., dial-in, system interconnection, routers)
* Cryptography
* Discretionary access control
* Identification and authentication
* Intrusion detection
* Object reuse
* System audit

The [NIST SP 800-26](http://csrc.nist.gov/groups/SMA/fisma/documents/Status-of-NIST-SP-800-26_v2.pdf), Security Self-Assessment Guide for Information Technology Systems, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

## Control Analysis

Analyze the controls that have been implemented. Derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

### Control Methods

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.

Adequate internal controls should be structured to assure senior management that:

* Personnel create, transmit, and store records and transactions in a safe and secure manner;
* Adequate segregation of duties exists;
* Data are accurate and reliable;
* Operating procedures are efficient and effective;
* Procedures are in effect to assure continuity of business;
* The company identifies and monitors high-risk conditions, functions, and activities; and
* There is proper adherence to company standards and policies, applicable laws and regulations, and other guidelines.

### Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

* 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.

### Control Analysis Technique

The security requirements checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist will be used to validate security compliance. Therefore, it is essential to update such checklists to reflect changes in an organization’s control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist’s validity.

## Likelihood determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment; the following governing factors must be considered:

* Threat-source motivation and capability
* Nature of the vulnerability
* Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low.

## Impact Analysis

The next major step is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. 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. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

* Loss of **Integrity**. System and data integrity refers to the requirement that information be protected from improper modification. Corrupted or inaccurate information is of little value.
* Loss of **Availability**. If a mission-critical IT system is unavailable to its end users, the organization’s mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users’ performance of their functions in supporting the organization’s mission.
* Loss of **Confidentiality**. System and data confidentiality refers to the protection of information from unauthorized disclosure. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization’s interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Typically we will be using a qualitative impact analysis for this risk assessment.

## Risk Determination

For a particular threat/vulnerability pair can be expressed as a function of:

* The likelihood of a given threat-source’s attempting to exercise a given vulnerability
* The magnitude of the impact should a threat-source successfully exercise the vulnerability
* The adequacy of planned or existing security controls for reducing or eliminating risk.

### Risk-Level Matrix

We will use a risk scale and a risk-level matrix to measure risk. The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example, the probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low

### Description of Risk Level

Our 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 exercised. The risk scale also presents actions that senior management, the mission owners, should take for each risk level.

## Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks will be provided. We will recommend controls to reduce the level of risk to the IT system and its data to an acceptable level. The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

## Results Documentation

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results will be documented in an official report or briefing. A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. The risk assessment report will be presented as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

## Risk Management Techniques

Once risks have been identified and assessed, we will begin to formulate a risk management strategy using a combination of these four standard approaches:

* **Avoidance** (eliminate)
* **Reduction** (mitigate)
* **Transfer** (outsource or insure)
* **Accept** (accept and budget)

## Create a risk-management plan

Security Team will meet with the Director of Operations to make a plan and to select appropriate controls and/or countermeasures to measure each risk. The risk management plan will propose applicable and effective security controls for managing the risks. For high risk or high cost items, the strategy will be approved by higher ranking officers in the company such as the CFO.

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization’s mission and its IT systems, because of each organization’s unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The “best of breed” approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

## Implementation

Implementation of the risk remediation plan will begin promptly following approval. The remediation plan can involve one-time events such as purchasing insurance and ongoing activities such as weekly monitoring. When control actions must be taken, the following rule applies: Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities. The following risk mitigation methodology describes the approach to control implementation:

### Prioritize Actions

Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization’s interest and mission.

### 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, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

### Conduct Cost-Benefit Analysis

To aid management in decision making and to identify cost-effective controls, a cost benefit analysis may be required.

### Select Controls

On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization’s mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the IT system and the organization.

### Assign Responsibility

IT management will assign appropriate persons (in-house personnel or external contracting staff) to tasks carrying out new controls.

### Implement Selected Control(s)

Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk.

## Reassess After Environment Changes

Risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Our risk management process will be updated periodically to evaluate whether the previously selected security controls are still applicable and effective, and to evaluate the possible risk level changes in the business environment.

Penetration tests are performed at least once a year and after any significant infrastructure or application upgrade or modification in the CDE.

* X:\security\Internal Audits

## Testing and Review Procedures

* Internal Network Pentest
* External Network Pentest
* Custom Code Review
* Application Vulnerability Test
* List of Security Audit Procedures

## External Resources

* This Risk Assessment Process is based largely on [NIST SP800-30 Risk Management Guide for IT Systems](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
* [NIST SP800-53A Guide for Assessing the Security Controls in Federal Information Systems](http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf)