

I. Purpose:

To outline the requirements mandated by the Payment Card Industry (PCI) Security Standards Council (SSC) to achieve compliance with PCI SSC's Data Security Standards (DSS). Supporting documentation, glossary, and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; and 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

- A. To fulfill the criteria for reporting PCI DSS compliance, agencies shall:
 1. Complete a self-assessment questionnaire (SAQ) annually based on transaction types and validation level;
 2. Complete quarterly external scans of their in-scope publicly facing networks by an authorized scanning vendor (ASV); and
 3. Submit an attestation of compliance (AOC) to their acquiring bank.
- B. Agencies shall acknowledge that compliance with PCI DSS is a continuous process and, as such, are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.
- C. Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.
- D. Agencies shall review their internal policies, procedures, guidelines and other documentation to ensure all necessary verbiage and actions required to comply with the following PCI DSS objectives and requirements are incorporated.
 1. Build and maintain a secure network (see policy 7200-P011)
 - a. Install and maintain a firewall configuration to protect cardholder data (requirement 1).
 - b. Do not use vendor-supplied defaults for system passwords and other security parameters (requirement 2).
 2. Protect Cardholder Data (see policy 7200-P012)
 - a. Protect stored cardholder data (requirement 3).
 - b. Encrypt transmission of cardholder data across open, public networks (requirement 4).
 3. Maintain a Vulnerability Management Program (see policy 7200-P013)
 - a. Use and regularly update anti-virus software or programs (requirement 5).
 - b. Develop and maintain secure systems and applications (requirement 6).

4. Implement Strong Access Control Measures (see policy 7200-P014)
 - a. Restrict access to cardholder data by business need-to-know (requirement 7).
 - b. Assign a unique ID to each person with computer access (requirement 8).
 - c. Restrict physical access to cardholder data (requirement 9).
5. Regularly Monitor and Test Networks (see policy 7200-015)
 - a. Track and monitor all access to network resources and cardholder data (requirement 10).
 - b. Regularly test security systems and processes (requirement 11).
6. Maintain an Information Security Policy (see policy 7200-P016)
 - a. Maintain a policy that addresses information security for all personnel (requirement 12).

I. Purpose:

This document outlines the requirements under objective one of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and, as such, are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 1 – Install and maintain a firewall configuration to protect cardholder data.

1. In addition to the provisions of policy 9400-P174: Network Connections and Management, agencies shall:
 - a. Ensure that their network diagrams include all access points to the cardholder data environment and all connections to cardholder data;
 - b. Document all applications, services, protocols, and ports allowed to communicate in and out of the cardholder data environment by their business justification;
 - c. Review firewall and router rule sets every six months;
 - d. Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and deny all inbound and outbound traffic not specifically needed;
 - e. Implement network segmentation and a DMZ to limit inbound and outbound traffic between the Internet and the cardholder data environment;
 - f. Not attach wireless access points to the cardholder data environment that are not intended to process or transmit cardholder data [*agencies should not utilize wireless networks to process or transmit cardholder data*].
2. In addition to the provisions of policy 9400-P175: Mobile Computing and Telework, agencies shall not authorize the use of personal computing devices (smartphones, PDAs, laptops, etc) to store, process, or transmit cardholder data or access the cardholder data environment.

- B. PCI DSS Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters.
1. In addition to the provisions of policy 9400-P170: User Access Management, agencies shall change all vendor-supplied defaults prior to implementation. This includes, but is not limited to, passwords, SNMP community strings, and unnecessary accounts.
 2. Agencies shall compare their baseline configuration standards against a trusted 3rd-party. Trusted 3rd-parties include, but are not limited to, National Institute of Standards and Technology (NIST), SANS Institute, or the Center for Internet Security (CIS).
 3. In addition to the provisions of policy 9400-P183: Technical Vulnerability Management, agencies shall implement only one primary function per server *[this does not apply to mainframe systems]*.

I. Purpose:

This document outlines the requirements under objective two of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and as such are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 3 – Protect stored cardholder data.

1. Agencies shall not store cardholder data unless required by State or Federal statute/mandate, or overriding business need. Agencies storing cardholder data shall:
 - a. Ensure that storage of cardholder data is reflected in their retention schedules and retention policies are updated to include cardholder data *[agencies should not retain this data longer than 30 days]*;
 - b. Ensure that the primary account number (PAN) is masked when displayed and rendered unreadable anywhere it is stored; and,
 - c. Ensure that cryptographic keys used to encrypt stored cardholder data are protected. Agencies shall document all key-management processes and procedures for use of cryptographic keys to protect cardholder data.
2. Agencies shall not store cardholder data on removable media.
3. Agencies shall not store sensitive authentication data beyond transaction authorization.

B. PCI DSS Requirement 4 – Encrypt transmission of cardholder data across open, public networks.

1. In addition to the provisions of policy 9300-P010: Web SSL Certificate Use Policy, agencies shall ensure strong cryptography and security controls (SSL/TLS, IPsec, etc) are employed to transmit cardholder data over an open, public network.
2. Agencies shall not send/transmit cardholder data by end-user messaging technologies (email, chat, IM, etc). Agencies that receive cardholder data by email, chat, IM, etc, shall immediately delete the

message and through a separate communication, inform the sender that the agency does not accept cardholder data in that fashion.

7200-P013: PCI-DSS – Maintain a Vulnerability Management Program

I. Purpose:

This document outlines the requirements under objective three of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store**, **process**, or **transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and as such are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 5 – Use and regularly update anti-virus software or programs.

In addition to the provisions of Malicious Code Prevention Policy and Guidelines (3200-P161 and 3200-G161 respectively), agencies shall regularly sample the deployed endpoint protection software to ensure the scan engine and detection definitions are current.

B. PCI DSS Requirement 6 – Develop and maintain secure systems and applications.

1. In addition to the provisions of policy 9400-P183: Technical Vulnerability Management, agencies shall establish a process to update their workstation and server configuration standards to address new vulnerabilities and the remediation of new vulnerabilities.
2. In addition to the provisions of policy 9400-P180: Information Security in the System Lifecycle, agencies that develop or contract to develop software applications for use with cardholder data or for use within the cardholder data environment shall:
 - a. Adhere to PCI DSS requirements 6.3, 6.4, 6.5, and 6.6
 - b. Adhere to all appropriate sections of the PCI Payment Application (PA) Data Security Standard (DSS) [https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf]

I. Purpose:

This document outlines the requirements under objective four of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and as such are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 7 – Restrict access to cardholder data by business need-to-know.

In addition to the provisions of policy 9400-P170: User Access Management, agencies shall develop an authorization form, signed by a designated approver, that specifies the required privileges for personnel with access to cardholder data or the cardholder data environment.

B. PCI DSS Requirement 8 – Assign a unique ID to each person with computer access.

1. In addition to the provisions of policy 9400-P170: User Access Management, agencies shall ensure at a minimum that policies 9400-P174: Network Connections and Management (A)(5), 9400-P175: Mobile Computing and Telework (B), and 9200-P121: Third Party Security (C)(3) are applied to all remote users.
2. Agencies that have administrative control over a vendor supplied payment application, virtual terminal, physical terminal, or other portions of the cardholder data environment shall develop and document procedures to implement or ensure implementation of PCI DSS Requirement 8.5.

C. PCI DSS Requirement 9 – Restrict physical access to cardholder data.

1. Requirement 9 applies to cardholder data in all forms (electronic, printed, etc).
2. While Requirement 9 is typically interpreted to apply to data centers, agencies that have physical control over systems in or connected to the cardholder data environment shall ensure all appropriate controls of this requirement are employed.
3. Agencies that process cardholder data on printed or hand-written documents shall ensure protection of those documents in accordance with all appropriate controls of this requirement.

I. Purpose:

This document outlines the requirements under objective five of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and as such are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 10 – Track and monitor all access to network resources and cardholder data.

1. In addition to the provisions of policy 9400-P167: Information Technology Resource Monitoring, agencies shall:
 - a. Implement automated audit trails for all system components to reconstruct the following:
 - i. All individual accesses to cardholder data;
 - ii. All actions taken by any individual with root or administrative privileges ;
 - iii. Access to all audit trails;
 - iv. Invalid logical access attempt;
 - v. Use of identification and authentication mechanisms;
 - vi. Initialization of the audit logs; and
 - vii. Creation and deletion of system-level objects.
 - b. Record the following, at a minimum, for all system components for each event:
 - i. User identification;
 - ii. Type of event;
 - iii. Date and time;
 - iv. Success or failure indication;
 - v. Origination of event; and
 - vi. Identity or name of affected data, system component, or resource.
 - c. Review logs for all system components at least daily.
 - d. Retain audit trail history for at least one (1) year.

2. Agencies shall utilize file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. *[adding new data should not cause an alert]*

B. PCI DSS Requirement 11 – Regularly test security systems and processes.

1. In addition to the provisions of policy 9400-P167: Information Technology Resource Monitoring; agencies shall deploy file-integrity monitoring tools on system components to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
2. In addition to the provision of policy 9400-183: Technical Vulnerability Management, agencies shall:
 - a. Test for rogue wireless access points at least quarterly, if wireless is deployed in the agency.
 - b. Run internal and external vulnerability scans at least quarterly and after significant network changes. Scans need only be performed on system components that are in-scope for PCI DSS. External scans shall be performed by a authorized scanning vendor (ASV) per PCI DSS requirements (see policy 7200-P010: PCI DSS Compliance)
 - c. Perform internal and external penetration tests at least annually and after significant network changes. Tests need only be performed on system components that are in-scope for PCI DSS. Penetration test must include:
 - i. Network-layer penetration tests; and
 - ii. Application-layer penetration tests.
 - d. Use intrusion detection and/or prevention systems to monitor all traffic in the cardholder data environment.

7200-P016: PCI-DSS – Maintain an Information Security Policy

I. Purpose:

This document outlines the requirements under objective six of the Payment Card Industry (PCI) Security Standards Council (SSC) Data Security Standard (DSS). These requirements are mandated in order to achieve compliance with the security standard. Glossary of terms, supporting documentation and current security standard can be found at PCI SSC's website (<https://www.pcisecuritystandards.org/>).

II. Scope:

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to "agency" or "agencies") that, 1) accept payment cards (credit and/or debit) for goods or services; 2) **store, process, or transmit** cardholder data, as defined by the PCI DSS, for those goods and/or services.

III. Policy:

Agencies shall acknowledge that compliance with PCI DSS is a continuous process and as such are mandated to comply with all requirements of PCI DSS regardless of the scope of their attestation.

Agencies utilizing services from other agencies shall coordinate compliance efforts as necessary.

A. PCI-DSS Requirement 12 – Maintain a policy that addresses information security for all personnel.

1. Agencies shall develop and document the internal processes and procedures necessary to implement the required security controls of PCI DSS.
2. On the anniversary date of their compliance, agencies shall conduct a risk assessment based on threats and vulnerabilities identified during that year. Until a document can be drafted that specifically addresses the concerns of the State of Wyoming, agencies shall adhere to National Institute of Standards and Technology (NIST) Special Publications (SP) [800-30 section 3](#) and [800-39 section 3.2](#) for risk assessment guidelines (Appendix A).
3. In addition to the provisions of policies 3200-P163: Network Security Management and 9400-P170: User Access Management, agencies shall designate an individual or team to manage and/or monitor PCI compliance. The designated team or individual shall ensure that roles and responsibilities for the flow of cardholder data within the agency are thoroughly documented.
4. In addition to the provisions of policy 1100-P141: Information Security Awareness and Training, agencies shall incorporate PCI DSS into existing training and emphasize the importance of cardholder data security into current awareness materials.
5. Agencies shall ensure potential employees are screened prior to hiring to minimize the risk to cardholder data. Screening may include but is not limited to:
 - a. Background checks (if authorized by WS § 7-19-101 (et al) & WS § 7-19-201); and/or
 - b. Application review (employment history, credit history, reference checks).

7200-P016: PCI-DSS – Maintain an Information Security Policy

6. In addition to the provisions outlined in “Reporting Security Events and Vulnerabilities” and “Information Security Incident Management” (9400-P190 and 9400-P191 respectively), agencies shall utilize the contacts in Appendix A in the event cardholder data is breached. Agencies shall utilize WS § 40-12-502 as the minimum guidelines for breach notification.

3. RISK ASSESSMENT

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4.

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.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described in Sections 3.1 through 3.9—

- Step 1—System Characterization (Section 3.1)
- Step 2—Threat Identification (Section 3.2)
- Step 3—Vulnerability Identification (Section 3.3)
- Step 4—Control Analysis (Section 3.4)
- Step 5—Likelihood Determination (Section 3.5)
- Step 6—Impact Analysis (Section 3.6)
- Step 7—Risk Determination (Section 3.7)
- Step 8—Control Recommendations (Section 3.8)
- Step 9—Results Documentation (Section 3.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 3-1 depicts these steps and the inputs to and outputs from each step.

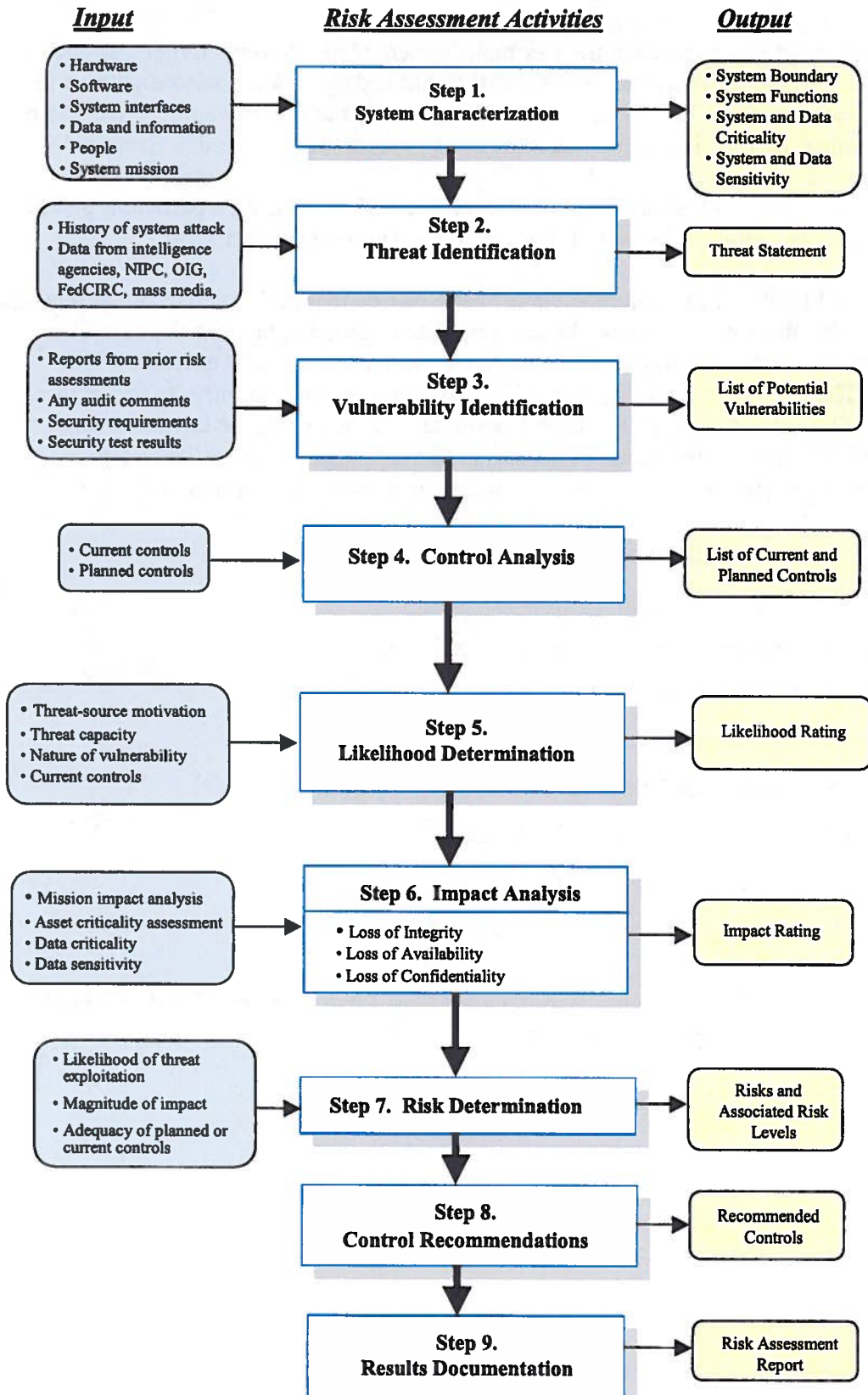


Figure 3-1. Risk Assessment Methodology Flowchart

3.1 STEP 1: SYSTEM CHARACTERIZATION

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

Section 3.1.1 describes the system-related information used to characterize an IT system and its operational environment. Section 3.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the IT system processing environment.

The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

3.1.1 System-Related Information

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.⁴

Additional information related to the operational environment 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 who provide technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture

⁴ The level of protection required to maintain system and data integrity, confidentiality, and availability.

- 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., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- 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, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development.

For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

3.1.2 Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

- **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. The questionnaire could also be used during on-site visits and interviews.
- **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). On-site visits also allow risk

assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

- **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 plan⁵, security policies) can provide good information about the security controls used by and planned for the IT system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.
- **Use of Automated Scanning Tool.** 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).

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1—Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

3.2 STEP 2: 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 (Section 3.5), one must consider threat-sources, potential vulnerabilities (Section 3.3), and existing controls (Section 3.4).

Threat: The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

3.2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.

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.

⁵ During the initial phase, a risk assessment could be used to develop the initial system security plan.

A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources can be natural, human, or environmental.

In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include “natural flood” because

of the low likelihood of such an event’s occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization’s IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer’s writing a Trojan horse program to bypass system security in order to “get the job done.”

Common Threat-Sources

- Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.

3.2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 3-1 presents an overview of many of today’s common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. 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; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering 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.

Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	<ul style="list-style-type: none"> • Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	<ul style="list-style-type: none"> • Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	<ul style="list-style-type: none"> • Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	<ul style="list-style-type: none"> • Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	<ul style="list-style-type: none"> • Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising a system vulnerability, as described in Section 3.5.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation’s National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Output from Step 2—A threat statement containing a list of threat-sources that could exploit system vulnerabilities

3.3 STEP 3: VULNERABILITY IDENTIFICATION

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

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

Table 3-2 presents examples of vulnerability/threat pairs.

Table 3-2. Vulnerability/Threat Pairs

Vulnerability	Threat-Source	Threat Action
Terminated employees’ system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company’s network and accessing company proprietary data
Company firewall allows inbound telnet, and <i>guest</i> ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the <i>guest</i> ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Vulnerability	Threat-Source	Threat Action
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:

- If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers).
- If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.

3.3.1 Vulnerability Sources

The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in Section 3.1.2. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the IT system assessed
- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (<http://icat.nist.gov>)

- Security advisories, such as FedCIRC and the Department of Energy’s Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

3.3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include—

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing.⁶

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). However, it should be noted that some of the *potential* vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site’s environment and requirements. Some of the “vulnerabilities” flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization’s security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an IT system’s ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.

⁶ The NIST SP draft 800-42, *Network Security Testing Overview*, describes the methodology for network system testing and the use of automated tools.

The results of these types of optional security testing will help identify a system's vulnerabilities.

3.3.3 Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether 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, information), nonautomated procedures, processes, and information transfers associated with a given IT system in the following security areas:

- Management
- Operational
- Technical.

Table 3-3 lists security criteria suggested for use in identifying an IT system's vulnerabilities in each security area.

Table 3-3. Security Criteria

Security Area	Security Criteria
Management Security	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers

Security Area	Security Criteria
Technical Security	<ul style="list-style-type: none"> • Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment:

- CSA of 1987
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

The NIST SP 800-26, *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.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3—A list of the system vulnerabilities (observations)⁷ that could be exercised by the potential threat-sources

3.4 STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

⁷ Because the risk assessment report is not an audit report, some sites may prefer to address the identified vulnerabilities as observations instead of findings in the risk assessment report.

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 (Step 5 below), the implementation of current or planned controls must be considered. 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.

Sections 3.4.1 through 3.4.3, respectively, discuss control methods, control categories, and the control analysis technique.

3.4.1 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.

3.4.2 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.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

3.4.3 Control Analysis Technique

As discussed in Section 3.3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as 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.

Output from Step 4—List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event

3.5 STEP 5: 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. Table 3-4 below describes these three likelihood levels.

Table 3-4. Likelihood Definitions

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.

Output from Step 5—Likelihood rating (High, Medium, Low)

3.6 STEP 6: IMPACT ANALYSIS

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, 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. 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. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **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. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. 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. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table 3.5).

Table 3-5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
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.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

- An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6—Magnitude of impact (High, Medium, or Low)

3.7 STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk 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.

To measure risk, a risk scale and a risk-level matrix must be developed. Section 3.7.1 presents a standard risk-level matrix; Section 3.7.2 describes the resulting risk levels.

3.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 3.6 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. 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
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)⁸

3.7.2 Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. 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 exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table 3-7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
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 DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7—Risk level (High, Medium, Low)

⁸ If the level indicated on certain items is so low as to be deemed to be "negligible" or non significant (value is <1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.

3.8 STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

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.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8—Recommendation of control(s) and alternative solutions to mitigate risk

3.9 STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should 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. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but 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. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report. Appendix B provides a suggested outline for the risk assessment report.

Output from Step 9—Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation

to the particular mission/business line. Organization-wide assessments of risk can be based solely on the assumptions, constraints, risk tolerances, priorities, and trade-offs established in the risk framing step (derived primarily from Tier 1 activities) or can be based on risk assessments conducted across multiple mission/business lines (derived primarily from Tier 2 activities). Risk assessments conducted at one tier can be used to refine/enhance threat, vulnerability, likelihood, and impact information used in assessments conducted in other tiers. The degree that information from risk assessments can be reused is shaped by the similarity of missions/business functions and the degree of autonomy that organizational entities or subcomponents have with respect to parent organizations. Organizations that are decentralized can expect to conduct more risk assessment activities at Tier 2 and, as a result, may have a greater need to communicate within Tier 2 to identify cross-cutting threats and vulnerabilities. Decentralized organizations can still benefit from Tier 1 risk assessments and, in particular, the identification of an initial set of threat and vulnerability sources. Organization-wide risk assessments provide some initial prioritization of risks for decision makers to consider when entering the risk response step.

Organizations benefit significantly from conducting risk assessments as part of an organization-wide risk management process. However, once risk assessments are complete, it is prudent for organizations to invest some time in keeping the assessments current. Maintaining currency of risk assessments may require support from the risk monitoring step (e.g., observing changes in organizational information systems and environments of operation). Keeping risk assessments up to date provides many potential benefits such as timely, relevant information that enables senior leaders/executives to perform near real-time risk management. Maintaining risk assessments also reduces future assessment costs and supports ongoing risk monitoring efforts. Organizations may determine that conducting comprehensive risk assessments as a way of maintaining current risk assessments do not provide sufficient value. In such situations, organizations consider conducting incremental and/or differential risk assessments. Incremental risk assessments consider only new information (e.g., the effects of using a new information system on mission/business risk), whereas differential risk assessments consider how changes affect the overall risk determination. Incremental or differential risk assessments are useful if organizations require a more targeted review of risk, seek an expanded understanding of risk, or desire an expanded understanding of the risk in relation to missions/business functions.

STEP 2: RISK ASSESSMENT

Inputs and Preconditions

Inputs to the risk assessment step from the risk framing step include, for example: (i) acceptable risk assessment methodologies; (ii) the breadth and depth of analysis employed during risk assessments; (iii) the level of granularity required for describing threats; (iv) whether/how to assess external service providers; and (v) whether/how to aggregate risk assessment results from different organizational entities or mission/business functions to the organization as a whole. Organizational expectations regarding risk assessment methodologies, techniques, and/or procedures are shaped heavily by governance structures, risk tolerance, culture, trust, and life cycle processes. Prior to conducting risk assessments, organizations understand the fundamental reasons for conducting the assessments and what constitutes adequate depth and breadth for the assessments. Risk assumptions, risk constraints, risk tolerance, and priorities/trade-offs defined during the risk framing step shape how organizations use risk assessments—for example, localized applications of the risk assessments within each of the risk management tiers (i.e., governance, mission/business process, information systems) or global applications of the risk assessments across the entire organization. Risk assessments can be conducted by organizations even when some of the inputs from the risk framing step have not been received or preconditions established. However, in those situations, the quality of the risk assessment results may be affected. In addition to the risk framing step, the risk assessment step can receive inputs from the risk monitoring step, especially during mission operations and the operations/maintenance phase of the SDLC (e.g., when organizations discover new threats or vulnerabilities that require an immediate reassessment of risk). The risk assessment step can also receive inputs from the risk response step (e.g., when organizations are considering the risk of employing new technology-based solutions as alternatives for risk reduction measures). As courses of action are developed in the risk

response step, a differential risk assessment may be needed to evaluate differences that each course of action makes in the overall risk determination.

Activities

THREAT AND VULNERABILITY IDENTIFICATION

TASK 2-1: Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.

Supplemental Guidance: Threat identification requires an examination of threat sources and events. For examining threat sources and events, organizations identify threat capabilities, intentions, and targeting information from all available sources. Organizations can leverage a number of sources for threat information at strategic or tactical levels. Threat information generated any tier can be used to inform or refine the risk-related activities in any other tier. For example, specific threats (i.e., tactics, techniques, and procedures) identified during Tier 1 threat assessments may directly affect mission/business process and architectural design decisions at Tier 2. Specific threat information generated at Tiers 2 and 3 can be used by organizations to refine threat information generated during initial threat assessments carried out at Tier 1.

Vulnerability identification occurs at all tiers. Vulnerabilities related to organizational governance (e.g., inconsistent decisions about the relative priorities of mission/business processes, selection of incompatible implementations of security controls) as well as vulnerabilities related to external dependencies (e.g., electrical power, supply chain, telecommunications), are most effectively identified at Tier 1. However, most vulnerability identification occurs at Tiers 2 and 3. At Tier 2, process and architecture-related vulnerabilities (e.g., exploitable weaknesses or deficiencies in mission/business processes, enterprise/information security architectures) are more likely to be identified. At Tier 3, information system vulnerabilities are the primary focus. These vulnerabilities are commonly found in the hardware, software, and firmware components of information systems or in the environments in which the systems operate. Vulnerabilities associated with architectural design and mission/business processes can have a greater impact on the ability of organizations to successfully carry out missions and business functions due to the potential impact across multiple information systems and mission environments. The refined vulnerability assessments conducted at Tiers 2 and 3 are shared with organizational personnel responsible for assessing risks more strategically. Vulnerability assessments conducted at Tier 2 and Tier 3 have the opportunity to evaluate additional related variables such as location, proximity to other high risk assets (physical or logical), and resource considerations related to operational environments. Information specific to operational environments allows for more useful and actionable assessment results. Vulnerability identification can be accomplished at a per-individual weakness/deficiency level or at a root-cause level. When selecting between approaches, organizations consider whether the overall objective is identifying each specific instance or symptom of a problem or understanding the underlying root causes of problems. Understanding specific exploitable weaknesses or deficiencies is helpful when problems are first identified or when quick fixes are required. This specific understanding also provides organizations with necessary sources of information for eventually diagnosing potential root causes of problems, especially those problems that are systemic in nature.

Organizations with more established enterprise and information security architectures and mature life cycle processes have outputs that can be used to inform risk assessment processes. Risk assumptions, constraints, tolerances, priorities, and trade-offs used for developing enterprise or information security architectures can be useful sources of information for initial risk assessment activities. Risk assessments conducted to support the development of segment or solution architectures may also serve as information sources for the identification of threats and vulnerabilities. Another factor influencing threat and vulnerability identification is organizational culture. Organizations that promote free and open communications and non-retribution for sharing adverse information tend to foster greater openness from individuals working within those organizations. Frequently, organizational personnel operating at Tiers 2 and 3 have valuable information and can make meaningful contributions in the area of threat and vulnerability identification. The culture of organizations influences the willingness of personnel to communicate potential threat and vulnerability information, which ultimately affects the quality and quantity of the threats/vulnerabilities identified.

RISK DETERMINATION

TASK 2-2: Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.

Supplemental Guidance: Organizations determine risk by considering the likelihood that known threats exploit known vulnerabilities and the resulting consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur. Organizations use threat and vulnerability information together with likelihood and consequences/impact information to determine risk either qualitatively or quantitatively. Organizations can employ a variety of approaches to determine the likelihood of threats exploiting vulnerabilities. Likelihood determinations can be based on either threat assumptions or actual threat information (e.g., historical data on cyber attacks, historical data on earthquakes, or specific information

on adversary capabilities, intentions, and targeting). When specific and credible threat information is available (e.g., types of cyber attacks, cyber attack trends, frequencies of attacks), organizations can use empirical data and statistical analyses to determine more specific probabilities of threats occurring. Assessment of likelihood can also be influenced by whether vulnerability identification occurred at the individual weakness or deficiency level or at the root-cause level. The relative ease/difficulty of vulnerability exploitation, the sophistication of adversaries, and the nature of operational environments all influence the likelihood that threats exploit vulnerabilities. Organizations can characterize adverse impacts by security objective (e.g., loss of confidentiality, integrity, or availability). However, to maximize usefulness, adverse impact is expressed in or translated into terms of organizational missions, business functions, and stakeholders.

Risk Determination and Uncertainty

Risk determinations require analysis of threat, vulnerability, likelihood, and impact-related information. Organizations also need to examine mission/business vulnerability to threats for which no safeguards/countermeasures (i.e., security controls or viable implementations of controls) exist when evaluating risk. The nature of the inputs provided to this step (e.g., general, specific, strategic, tactical) directly affects the type of outputs or risk determinations made. Organizations also consider additional insights related to the anticipated time frames associated with particular risks. Time horizons associated with potential threats can shape future risk responses (e.g., risk may not be a concern if the time horizon for the risk is in the distant future).

Organizational guidance for determining risk under uncertainty indicates how combinations of likelihood and impact are combined into a determination of the risk level or risk score/rating. Organizations need to understand the type and amount of uncertainty surrounding risk decisions so that risk determinations can be understood. During the risk framing step, organizations may have provided guidance on how to analyze risk and how to determine risk when a high degree of uncertainty exists. Uncertainty is particularly a concern when the risk assessment considers advanced persistent threats, for which analysis of interacting vulnerabilities may be needed, the common body of knowledge is sparse, and past behavior may not be predictive.

While threat and vulnerability determinations apply frequently to missions and business functions, the specific requirements associated with the missions/business functions, including the environments of operation, may lead to different assessment results. Different missions, business functions, and environments of operation can lead to differences in the applicability of specific threat information considered and the likelihood of threats causing potential harm. Understanding the threat component of the risk assessment requires insight into the particular threats facing specific missions or business functions. Such awareness of threats includes understanding the capability, intent, and targeting of particular adversaries. The risk tolerance of organizations and underlying beliefs associated with how the risk tolerance is formed (including the culture within organizations) may shape the perception of impact and likelihood in the context of identified threats and vulnerabilities.

Even with the establishment of explicit criteria, risk assessments are influenced by organizational culture and the personal experiences and accumulated knowledge of the individuals conducting the assessments. As a result, assessors of risk can reach different conclusions from the same information. This diversity of perspective can enrich the risk assessment process and provide decision makers with a greater array of information and potentially fewer biases. However, such diversity may also lead to risk assessments that are inconsistent. Organizationally-defined and applied processes provide the means to identify inconsistent practices and include processes to identify and resolve such inconsistencies.

Outputs and Post Conditions

The output of the risk assessment step is a determination of risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Depending on the approach that organizations take, either the overall risk to the organization or the inputs used to determine risk may be communicated to the decision makers responsible for risk response. In certain situations, there are recurring cycles between the risk assessment step and the risk response step until particular objectives are achieved. Based on the course of action selected during the risk response step, some residual risk may remain. Under certain circumstances, the level of residual risk could trigger a reassessment of risk. This reassessment is typically incremental (assessing only the new information) and differential (assessing how the new information changes the overall risk determination).

The aggregation of risk assessment results from all three tiers drives the management of portfolios of risks undertaken by organizations. Identified risks common to more than one mission/business function within organizations may also be the source for future assessment activities at Tier 1, such as root-cause analysis. Gaining a better understanding of the reasons why certain risks are more common or frequent assists decision makers in selecting risk responses that address underlying (or root-cause) problems instead of solely focusing on the surface issues surrounding the existence of the risks. The results of risk assessments can also shape future design and development decisions related to enterprise architecture, information security architecture, and organizational information systems. The extent to which missions

and business functions are vulnerable to a set of identified threats and the relative ease with which those threats can be exploited, contribute to the risk-related information provided to senior leaders/executives.

Outputs from the risk assessment step can be useful inputs to the risk framing and risk monitoring steps. For example, risk determinations can result in revisiting the organizational risk tolerance established during the risk framing step. Organizations can also choose to use information from the risk assessment step to inform the risk monitoring step. For example, risk assessments can include recommendations to monitor specific elements of risk (e.g., threat sources) so that if certain thresholds are crossed, previous risk assessment results can be reviewed and updated, as appropriate. Particular thresholds established as part of risk monitoring programs can also serve as the basis for reassessments of risk. If organizations establish criteria as a part of the risk framing step for when risk assessment results do not warrant risk responses, then assessment results could be fed directly to the risk monitoring step as a source of input.

3.3 RESPONDING TO RISK

Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Identifying and analyzing alternative courses of action⁵⁶ typically occurs at Tier 1 or Tier 2. This is due to the fact that alternative courses of action (i.e., potential risk responses) are evaluated in terms of anticipated organization-wide impacts and the ability of organizations to continue to successfully carry out organizational missions and business functions. Decisions to employ risk response measures organization-wide are typically made at Tier 1, although the decisions are informed by risk-related information from the lower tiers. At Tier 2, alternative courses of action are evaluated in terms of anticipated impacts on organizational missions/business functions, the associated mission/business processes supporting the missions/business functions, and resource requirements. At Tier 3, alternative courses of action tend to be evaluated in terms of the system development life cycle or the maximum amount of time available for implementing the selected course(s) of action. The breadth of potential risk responses is a major factor for whether the activity is carried out at Tier 1, Tier 2, or Tier 3. Risk decisions are influenced by organizational risk tolerance developed as part of risk framing activities at Tier 1. Organizations can implement risk decisions at any of the risk management tiers with different objectives and utility of information produced.

STEP 3: RISK RESPONSE

Inputs and Preconditions

Inputs from the risk assessment and risk framing steps include: (i) identification of threat sources and threat events; (ii) identification of vulnerabilities that are subject to exploitation; (iii) estimates of potential consequences and/or impact if threats exploit vulnerabilities; (iv) likelihood estimates that threats exploit vulnerabilities; (v) a determination of risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; (vi) risk response guidance from the organizational risk management strategy (see Appendix H); and (vii) the general organizational directions and guidance on appropriate responses to risk. In addition to the risk assessment and risk framing steps, the risk response step can receive inputs from the risk monitoring step (e.g., when organizations experience a breach or compromise to their information systems or environments of operation that require an immediate response to address the incident and reduce additional risk that results from the event). The risk response step can also receive inputs from the risk framing step (e.g., when organizations are required to deploy new safeguards and countermeasures in their information systems based on security requirements in new legislation or OMB policies). The risk framing step also directly shapes the resource constraints associated with selecting an appropriate course of action. Additional preconditions established at the risk framing step may include: (i) constraints based on architecture and previous investments; (ii) organizational preferences and tolerances; (iii) the expected effectiveness at mitigating risk (including how effectiveness is measured and monitored); and (iv) the time horizon for

⁵⁶ A *course of action* is a time-phased or situation-dependent combination of risk response measures. A *risk response measure* is a specific action taken to respond to an identified risk. Risk response measures can be separately managed and can include, for example, the implementation of security controls to mitigate risk, promulgation of security policies to avoid risk or to accept risk in specific circumstances, and organizational agreements to share or transfer risk.

7200-P016: PCI-DSS – Maintain an Information Security Policy

Appendix A – Breach Notification

Below are the Elavon contacts agencies will need should a breach occur at their location(s). These contacts will work with the State and be the liaison with the card brands (Visa, MC, Discover, etc).

Contacts for breach occurrence:

Christopher Rochelle
Merchant Data Compromise Coordinator
Global Association Management & Compliance
Elavon
7300 Chapman Highway
Knoxville, TN 37920 USA
Phone: 865.403.8736
E-mail: Christopher.Rochelle@elavon.com

Chris Geron
Vice President
Global Association Management & Compliance
Elavon
7300 Chapman Highway
Knoxville, TN 37920 USA
Phone: 865.403.8852
E-mail: Chris.Geron@elavon.com

Bridget Stover
Client Executive
Client Relations
Elavon
621 Capitol Mall
Sacramento CA 95814
Direct: (916) 498-3443
Email: bridget.stover@Elavon.com

7200-P016: PCI-DSS – Maintain an Information Security Policy

Appendix B – Breach Notification

Below are the Elavon contacts agencies will need should a breach occur at their location(s). These contacts will work with the State and be the liaison with the card brands (Visa, MC, Discover, etc).

Contacts for breach occurrence:

Christopher Rochelle
Merchant Data Compromise Coordinator
Global Association Management & Compliance
Elavon
7300 Chapman Highway
Knoxville, TN 37920 USA
Phone: 865.403.8736
E-mail: Christopher.Rochelle@elavon.com

Chris Geron
Vice President
Global Association Management & Compliance
Elavon
7300 Chapman Highway
Knoxville, TN 37920 USA
Phone: 865.403.8852
E-mail: Chris.Geron@elavon.com

Bridget Stover
Client Executive
Client Relations
Elavon
621 Capitol Mall
Sacramento CA 95814
Direct: (916) 498-3443
Email: bridget.stover@Elavon.com

