Your Logo
Will Be
Placed Here

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) CYBERSECURITY POLICY & STANDARDS

ACME Business Solutions, Inc.

PCI DSS COMPLIANT

PCI DSS
Information Security Policies & Standards
PCI DSS v3

INTERNAL USE
Access Limited to Internal Use Only

Table of Contents

Payment Card Industry Data Security Standard (PCI DSS) Policy Overview 6
Introduction 6
Purpose 6
Scope & Applicability 7
Policy 7
Violations 7
Exceptions 7
Updates 7
Key Terminology 8
Cybersecurity Governance Structure 10
Cybersecurity Considerations For Protecting Systems 10
Policies, Control Objectives, Standards, Procedures & Guidelines Structure 10
Cybersecurity Controls 10
Cybersecurity Program Activities 10
PCI DSS Section 1: Build & Maintain A Secure Network 11
Requirement #1: Install & Maintain A Firewall Configuration To Protect Cardholder Data 11
PCI DSS Control 1.1 11
PCI DSS Control 1.2 12
PCI DSS Control 1.3 12
PCI DSS Control 1.4 13
PCI DSS Control 1.5 13
Requirement #2: Do Not Use Vendor-Supplied Defaults For System Passwords & Other Security Parameters 14
PCI DSS Control 2.1 14
PCI DSS Control 2.2 14
PCI DSS Control 2.3 15
PCI DSS Control 2.4 15
PCI DSS Control 2.5 15
PCI DSS Control 2.6 16
PCI DSS Section 2: Protect Cardholder Data 17
Requirement #3: Protect Stored Cardholder Data 17
PCI DSS Control 3.1 17
PCI DSS Control 3.2 17
PCI DSS Control 3.3 18
PCI DSS Control 3.4 18
PCI DSS Control 3.5 18
PCI DSS Control 3.6 19
PCI DSS Control 3.7 19
Requirement #4: Encrypt Transmission of Cardholder Data Across Open, Public Networks 20
PCI DSS Control 4.1 20
PCI DSS Control 4.2 20
PCI DSS Control 4.3 21
PCI DSS Section 3: Maintain A Vulnerability Management Program 22
Requirement #5: Use & Regularly Update Anti-Virus Software or Programs 22
PCI DSS Control 5.1 22
PCI DSS Control 5.2 22
PCI DSS Control 5.3 23
PCI DSS Control 5.4 23
Requirement #6: Develop & Maintain Secure Systems & Applications 24
PCI DSS Control 6.1 24
PCI DSS Control 6.2 24
PCI DSS Control 6.3 24

PCI DSS Control 6.4 25
PCI DSS Control 6.5 25
PCI DSS Control 6.6 26
PCI DSS Control 6.7 27

PCI DSS Section 4: Implement Strong Access Control Measures 28

Requirement #7: Restrict Access To Cardholder Data By Business Need To Know 28
PCI DSS Control 7.1 28
PCI DSS Control 7.2 28
PCI DSS Control 7.3 29

Requirement #8: Assign A Unique ID To Each Person With Computer Access 29
PCI DSS Control 8.1 29
PCI DSS Control 8.2 30
PCI DSS Control 8.3 31
PCI DSS Control 8.4 31
PCI DSS Control 8.5 31
PCI DSS Control 8.6 32
PCI DSS Control 8.7 32
PCI DSS Control 8.8 34

Requirement #9: Restrict Physical Access To Cardholder Data 34
PCI DSS Control 9.1 34
PCI DSS Control 9.2 35
PCI DSS Control 9.3 35
PCI DSS Control 9.4 35
PCI DSS Control 9.5 36
PCI DSS Control 9.6 36
PCI DSS Control 9.7 36
PCI DSS Control 9.8 37
PCI DSS Control 9.9 37
PCI DSS Control 9.10 38

PCI DSS Section 5: Regularly Monitor & Test Networks 39

Requirement #10: Track & Monitor All Access To Network Resources & Cardholder Data 39
PCI DSS Control 10.1 39
PCI DSS Control 10.2 39
PCI DSS Control 10.3 40
PCI DSS Control 10.4 40
PCI DSS Control 10.5 41
PCI DSS Control 10.6 41
PCI DSS Control 10.7 42
PCI DSS Control 10.8 42
PCI DSS Control 10.9 42

Requirement #11: Regularly Test Security Systems & Processes 43
PCI DSS Control 11.1 43
PCI DSS Control 11.2 43
PCI DSS Control 11.3 44
PCI DSS Control 11.4 44
PCI DSS Control 11.5 45
PCI DSS Control 11.6 45

PCI DSS Section 6: Maintain An Cybersecurity Policy 46

Requirement #12: Maintain A Policy That Addresses Cybersecurity For All Personnel 46
PCI DSS Control 12.1 46
PCI DSS Control 12.2 46
PCI DSS Control 12.3 46
PCI DSS Control 12.4 47
PCI DSS Control 12.5 47
PCI DSS Control 12.6 48
PCI DSS Control 12.7 48

PCI DSS Control 12.8 49
PCI DSS Control 12.9 49
PCI DSS Control 12.10 50
PCI DSS Control 12.11 50

Appendices 52

Appendix A: Data Classification & Handling Guidelines 52
A-1: Data Classification 52
A-2: Labeling 53
A-3: General Assumptions 53
A-4: Personally Identifiable Information (PII) 53
Appendix B: Data Classification Examples 56
Appendix C: Data Retention Periods 57
Appendix D: Cybersecurity Roles & Responsibilities 59
D-1: Cybersecurity Roles 59
D-2: Cybersecurity Responsibilities 59
Appendix E: Cybersecurity Exception Request Procedures 62
Appendix F: Types of Security Controls 63
F-1: Preventative Controls 63
F-2: Detective Controls 63
F-3: Corrective Controls 63
F-4: Recovery Controls 63
F-5: Directive Controls 63
F-6: Deterrent Controls 63
F-7: Compensating Controls 63
Appendix G: Rules of Behavior / User Acceptable Use 64
G-1: Acceptable Use 64
G-2: Prohibited Use 64
G-3: Additional Rules For Security & Privileged Users 65
Appendix H: Guidelines For Personal Use Of It Resources 66
Appendix I: Risk Management Framework (RMF) 67
I-1: Risk Management Overview 67
I-2: Risk Management Framework (RMF) 67
I-3: Assessing Risk 69
Appendix J: System Hardening 70
J-1: Server-Class Systems 70
J-2: Workstation-Class Systems 70
J-3: Network Devices 70
J-4: Mobile Devices 71
J-5: Databases 71
Appendix K: PCI DSS Self-Assessment Questionnaire (SAQ) 72
K-1: SAQ Overview 72
K-2: How To Determine Your SAQ 72

Annex 1: Management Directive Template 73

Annex 2: User Acknowledgement Form 74

Annex 3: Certification of Cybersecurity Awareness Training Form 75

Annex 4: User Equipment Receipt of Issue Template 76

Annex 5: Service Provider Indemnification & Non-Disclosure Agreement (NDA) Template 77

Annex 6: Incident Response Form 78

Annex 7: Information Security Officer (ISO) Appointment Orders Template 79

Annex 8: Administrator Account Request Form 80

Annex 9: Change Management Request Form 81

ANNEX 10: CHANGE CONTROL BOARD (CCB) MEETING FORM 83
ANNEX 11: PORTS, PROTOCOLS & SERVICES DOCUMENTATION FORM 84
ANNEX 12: INCIDENT RESPONSE PLAN (IRP) TEMPLATE 85
ANNEX 13: BUSINESS IMPACT ANALYSIS (BIA) TEMPLATE 98
ANNEX 14: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (DRP) TEMPLATE 100
GLOSSARY: ACRONYMS & DEFINITIONS 104
ACRONYMS 104
DEFINITIONS 104
RECORD OF CHANGES 105

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) Cybersecurity Policy & Standards document provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program for PCI DSS v3.2 compliance at ACME Business Solutions, Inc. (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every ACME user who interacts with data and information systems. Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of cardholder data and information systems. This also includes against accidental loss or destruction.

PURPOSE

The purpose of this document is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of ACME's payment card data and related information systems.
- Protecting ACME, its employees, and its clients from illicit use of ACME's information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support ACME's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Cybersecurity risks.

The formation of the policy is driven by many factors, with the key factor being a risk. This policy sets the ground rules under which ACME shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.

This policy, including related standards and procedures, are necessary to support the management of information risks in daily operations. The development of policy provides due care to ensure ACME users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of ACME data.

Scope & Applicability

This policy and its related standards, procedures, and guidelines apply to all ACME data, information systems, activities, and assets owned, leased, controlled, or used by ACME, its agents, contractors, or other business partners on behalf of ACME that are within scope of the PCI DSS. This policy applies to all ACME employees, contractors, sub-contractors, and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store, or dispose of ACME data.

Some standards are explicitly stated for persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions shall comply with the standards. ACME departments shall use this policy and its standards or may create a more restrictive set of policies and standards, but not one that is less restrictive, less comprehensive, or less compliant than this policy and its standards.

This policy and its standards do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Appendix D: Cybersecurity Roles & Responsibilities provides a detailed description of ACME user roles and responsibilities, in regards to Cybersecurity.

ACME reserves the right to revoke, change, or supplement this policy and its standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

Policy

ACME shall design, implement and maintain a coherent set of standards and procedures to manage risks to cardholder data, in an effort to ensure an acceptable level of Cybersecurity risk. Within the scope of the Cardholder Data Environment (CDE), ACME will protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its information systems and cardholder data, regardless of how it is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations

Any ACME user found to have violated any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

While every exception to a policy or standard potentially weakens protection mechanisms for ACME information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in Appendix E: Cybersecurity Exception Request Procedures.

Updates

Updates to the PCI DSS Cybersecurity Policy will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, standards, procedures, and guidelines.

KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Cybersecurity Terms*, is the primary reference document that ACME uses to define common cybersecurity terms. [1] Key terminology to be aware of includes:

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Contract Owner: A term describing a person or entity that has been given formal responsibility for entering into and managing legal contracts with service providers. Contract owners are formally responsible for making sure due care and due diligence are performed by service providers, in regards to PCI DSS compliance.

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align ACME with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. Appendix A: Data Classification & Handling Guidelines provides guidance on data classification and handling restrictions.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Cybersecurity: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System: A term describing an asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

[1] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include Personally Identifiable Information, Payment Card Data (PCD), and all other forms of data classified as Restricted or Confidential in Appendix A: Data Classification & Handling Guidelines.

Service Provider: A term that includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If a company provides a service that involves only the provision of public network access (such as a telecommunications company providing just the communication link) that entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Sensitive Personally Identifiable Information (sPII): sPII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: [2]

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Standard: A term describing formally established requirements in regard to processes, actions, and configurations.

[2] The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - http://www.leg.state.or.us/ors/646a.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

CYBERSECURITY CONSIDERATIONS FOR PROTECTING SYSTEMS

Appendix F: Type of Security Controls provides a detailed description of information security considerations in protecting information systems, based on the importance of the system and the sensitivity of the data processed or stored by the system.

POLICIES, CONTROL OBJECTIVES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Information security documentation is comprised of five main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies the condition that should be met;
(3) Standards that provides quantifiable requirements to be met;
(4) Procedures that establish how tasks must be performed to meet the requirements established in standards; and
(5) Guidelines are recommended, but not mandatory.

Figure 1: Policy Framework

CYBERSECURITY CONTROLS

Security controls are sometimes synonymous with standards, since controls are generally designed to directly map to standards. The PCI DSS Cybersecurity Policy security controls have a well-defined organization and structure, which supports ongoing compliance with the PCI DSS.

CYBERSECURITY PROGRAM ACTIVITIES

An Cybersecurity Management System (ISMS) focuses on cybersecurity management and IT-related risks. The governing principle behind ACME's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with ISO/IEC 27001, ACME's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between ACME's networks and untrusted networks, as well as traffic into and out of more sensitive areas within ACME's internal trusted networks. The Cardholder Data Environment (CDE) is an example of a more sensitive area within ACME's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in PCI DSS Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of PCI DSS Requirement 1.

PCI DSS CONTROL 1.1

Control Objective: The organization establishes firewall and router configuration standards that follow industry-recognized leading practices.

Standard: Asset custodians are required to establish firewall and router configuration processes that include the following: [3]

(a) Asset custodians are required to establish and maintaining a formal process for approving and testing all network connections and changes to both firewall and router configurations; [4]

(b) Asset custodians are required to establish and maintaining detailed network diagrams. Network diagrams must: [5]
   1. Document all connections to cardholder data, including any wireless networks;
   2. Be reviewed annually; and
   3. Be updated as the network changes to reflect the current architecture in place;

(c) Asset custodians are required to establish and maintaining detailed data flow diagrams that show all cardholder data flows across systems and networks; A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and ACME's internal networks; [6]

(d) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes; [7]

(e) A documented business justification is required for all services, protocols, and ports allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure; [8] and

(f) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover: [9]
   1. Validation of Access Control Lists (ACLs); and
   2. Vulnerability management (e.g., validating software and firmware is current).

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP)

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[3] PCI DSS v3.2 Requirement 1.1
[4] PCI DSS v3.2 Requirement 1.1.1
[5] PCI DSS v3.2 Requirement 1.1.2
[6] PCI DSS v3.2 Requirement 1.1.4
[7] PCI DSS v3.2 Requirement 1.1.5
[8] PCI DSS v3.2 Requirement 1.1.6
[9] PCI DSS v3.2 Requirement 1.1.7

PCI DSS CONTROL 1.2

Control Objective: The organization builds firewall and router configurations that restrict connections between untrusted networks and any system components in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to deploy and configure of firewalls and routers in order to restrict connections between untrusted networks and any system components within the Cardholder Data Environment (CDE) by the following means: [10]

(a) Implementing Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to the CDE to only that which is necessary, as defined by a business justification; [11]
(b) Securing and synchronizing router and firewall configuration files; [12] and
(c) Positioning perimeter firewalls between wireless networks and the CDE.[13]

Supplemental Guidance: Not all firewalls and routers have the functionality for the running configuration to be different that the configuration loaded at startup. However, if the functionality exists, the startup configuration must be synchronized with the correct running configuration so that a reboot of the device will not degrade network security.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 1.3

Control Objective: The organization prohibits direct public access to the Internet and any system component in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to establish and manage firewall and router configuration standards to prohibit direct public access to the Internet and any system component in the Cardholder Data Environment (CDE) that includes, but is not limited to: [14]

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [15]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [16]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [17]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [18]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [19]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [20] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [21]

Supplemental Guidance: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated so that filtering decisions would not only be based on administrator-defined rules, but also on the context that has been built by previous connections as well as previous packets belonging to the same connection.

[10] PCI DSS v3.2 Requirement 1.2
[11] PCI DSS v3.2 Requirement 1.2.1
[12] PCI DSS v3.2 Requirement 1.2.2
[13] PCI DSS v3.2 Requirement 1.2.3
[14] PCI DSS v3.2 Requirement 1.3
[15] PCI DSS v3.2 Requirement 1.3.1
[16] PCI DSS v3.2 Requirement 1.3.2
[17] PCI DSS v3.2 Requirement 1.3.3
[18] PCI DSS v3.2 Requirement 1.3.4
[19] PCI DSS v3.2 Requirement 1.3.5
[20] PCI DSS v3.2 Requirement 1.3.6
[21] PCI DSS v3.2 Requirement 1.3.7

REQUIREMENT #3: PROTECT STORED CARDHOLDER DATA

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

PCI DSS CONTROL 3.1

Control Objective: The organization implements a process for to minimize the storage of cardholder data.

Standard: Data owners are required to determine the business requirements for data retention and securely dispose of cardholder data once the data is no longer necessary. This includes, but is not limited to: [37]

(a) Implement a data retention and disposal policy that covers cardholder data;
(b) Limiting cardholder data retention time to that which is required for legal, regulatory, and business requirements;
(c) Conducting a quarterly process (automatic or manual) to identify and securely delete stored cardholder data that exceeds defined retention requirements.
(d) Performing secure deletion of electronic-based cardholder data; and
(e) Shredding physical-based cardholder data.

Supplemental Guidance: Specific requirements for the retention of cardholder data are driven by business needs (e.g., cardholder data needs to be held for X period for Y business reasons) and documentation should exist to justify the business need.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 3.2

Control Objective: The organization does not store sensitive authentication data after authorization.

Standard: Asset custodians are required to ensure sensitive authentication data is not stored after authorization, even if it is encrypted. ACME is prohibited from storing: [38]

(a) The full contents of any track: [39]
    1. Tracks are from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere.
    2. This data is alternatively called the full track, track, track 1, track 2, and magnetic-stripe data.
(b) Storing the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions; [40] and
(c) Storing the Personal Identification Number (PIN) or the encrypted PIN block. [41]

Supplemental Guidance: The following data sources should be examined to verify that the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip are not stored under any circumstance:

- Incoming transaction data;
- All logs (e.g., transaction, history, debugging, error);
- History files;
- Trace files;
- Several database schemas; and
- Database contents.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[37] PCI DSS v3.2 Requirement 3.1
[38] PCI DSS v3.2 Requirement 3.2
[39] PCI DSS v3.2 Requirement 3.2.1
[40] PCI DSS v3.2 Requirement 3.2.2
[41] PCI DSS v3.2 Requirement 3.2.3

REQUIREMENT #12: MAINTAIN A POLICY THAT ADDRESSES CYBERSECURITY FOR ALL PERSONNEL

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, the term "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are resident on the entity's site or otherwise have access to the Cardholder Data Environment (CDE).

PCI DSS CONTROL 12.1

Control Objective: The organization establishes, publishes, maintains and disseminates a security policy.

Standard: ACME's PCI DSS Cybersecurity Policy fulfills the requirement within PCI DSS for a security policy. ACME's management is responsible for the annual review of the PCI DSS Cybersecurity Policy, as well as updates, as necessary. [218]

Supplemental Guidance: A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

Procedures: While, ACME's PCI DSS Cybersecurity Policy establishes the documentation requirement for PCI DSS, asset custodians, and data owners are required to:

- Review and update the PCI DSS Cybersecurity Policy, as needed; and
- Disseminate the PCI DSS Cybersecurity Policy to staff and subordinates to ensure all ACME personnel who interact with the CDE understand their requirements.

PCI DSS CONTROL 12.2

Control Objective: The organization implements a risk-assessment process.

Standard: Asset custodians and data owners are required to implement a risk-assessment process that: [219]

(a) Is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Identifies critical assets, threats, and vulnerabilities; and
(c) Results in a formal risk assessment.

Supplemental Guidance: Examples of risk assessment methodologies include but are not limited to

- OCTAVE;
- ISO 27005; and
- NIST SP 800-30.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 12.3

Control Objective: The organization develops and implements usage policies for critical technologies.

Standard: Asset custodians and data owners are required to develop and implement usage policies for critical technologies and defining the proper use of these technologies. Usage policies require the following: [220]

(a) Explicit approval by authorized parties; [221]
(b) Authentication for the use of the technology; [222]
(c) A list of all such devices and personnel with access; [223]

[218] PCI DSS v3.2 Requirements 12.1, 12.1.1
[219] PCI DSS v3.2 Requirement 12.2
[220] PCI DSS v3.2 Requirement 12.3
[221] PCI DSS v3.2 Requirement 12.3.1
[222] PCI DSS v3.2 Requirement 12.3.2
[223] PCI DSS v3.2 Requirement 12.3.3

(d) A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices); [224]
(e) Acceptable uses of the technology; [225]
(f) Acceptable network locations for the technologies; [226]
(g) List of company-approved products; [227]
(h) Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity; [228]
(i) Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use; [229] and
(j) For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. [230]

Supplemental Guidance: Appendix G: Rules of Behavior / User Acceptable Use covers ACME's rules of behavior. Examples of critical technologies include, but are not limited to:

- Remote-access technologies;
- Wireless technologies;
- Removable electronic media
- Laptops;
- Tablets;
- Smart phones;
- Personal data/digital assistants (PDAs),
- E-mail usage; and
- Internet usage.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS Control 12.4

Control Objective: The organization defines information security responsibilities for all personnel. [231]

Standard: ACME's Human Resources (HR) department is required to ensure that information security policies, standards and procedures clearly define information security responsibilities for all personnel.

Supplemental Guidance: Cybersecurity roles and responsibilities are defined in Appendix D: Cybersecurity Roles & Responsibilities.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS Control 12.5

Control Objective: The organization assigns an individual or a team information security management responsibilities.

Standard: ACME's assigned Information Security Officer (ISO) is required to perform or delegate the following information security management responsibilities: [232]

(a) Establish, document, and distribute security policies and procedures; [233]
(b) Monitor and analyze security alerts and information; [234]
(c) Distribute and escalate security alerts to appropriate personnel; [235]

[224] PCI DSS v3.2 Requirement 12.3.4
[225] PCI DSS v3.2 Requirement 12.3.5
[226] PCI DSS v3.2 Requirement 12.3.6
[227] PCI DSS v3.2 Requirement 12.3.7
[228] PCI DSS v3.2 Requirement 12.3.8
[229] PCI DSS v3.2 Requirement 12.3.9
[230] PCI DSS v3.2 Requirement 12.3.10
[231] PCI DSS v3.2 Requirement 12.4 & 12.4.1
[232] PCI DSS v3.2 Requirement 12.5
[233] PCI DSS v3.2 Requirement 12.5.1
[234] PCI DSS v3.2 Requirement 12.5.2
[235] PCI DSS v3.2 Requirement 12.5.2

(d) Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; [236]
(e) Administer user accounts, including additions, deletions, and modifications; [237] and
(f) Monitor and control all access to data. [238]

Supplemental Guidance: Cybersecurity roles and responsibilities are defined in Appendix D: Cybersecurity Roles & Responsibilities.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS Control 12.6

Control Objective: The organization implements a formal security awareness program.

Standard: ACME's assigned Information Security Officer (ISO), in conjunction with ACME's Human Resources (HR) department, is required to develop and implement a formal security awareness program to make all personnel aware of the importance of cardholder data security, which includes: [239]

(a) Educating personnel upon hire and at least annually; [240] and
(b) Requiring applicable personnel to acknowledge at least annually that they have read and understood the PCI DSS Cybersecurity Policy and procedures. [241]

Supplemental Guidance: Awareness methods can vary depending on the role of the personnel and their level of access to the cardholder data. If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.

Requiring an acknowledgment by personnel in writing or electronically helps ensure that they have read and understood the security policies and that they have made and will continue to make a commitment to comply with these policies.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS Control 12.7

Control Objective: The organization screens potential personnel prior to hiring to minimize the risk of attacks from internal sources.

Standard: ACME's Human Resources (HR) department is responsible for screening potential personnel prior to hiring to minimize the risk of attacks from internal sources. [242]

Supplemental Guidance: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. Examples of background checks include, but are not limited to:

- Previous employment history;
- Criminal record;
- Credit history; and Reference checks.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[236] PCI DSS v3.2 Requirement 12.5.3
[237] PCI DSS v3.2 Requirement 12.5.4
[238] PCI DSS v3.2 Requirement 12.5.5
[239] PCI DSS v3.2 Requirement 12.6
[240] PCI DSS v3.2 Requirement 12.6.1
[241] PCI DSS v3.2 Requirement 12.6.2
[242] PCI DSS v3.2 Requirement 12.7

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by ACME
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by ACME, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME. · Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to ACME. · Impact would not be damaging or a risk to business operations.

A-5: DATA HANDLING GUIDELINES

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-ACME employees.	▪ NDA is recommended prior to access by non-ACME employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*
Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*

APPENDIX B: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

DATA CLASS	SENSITIVE DATA ELEMENTS	PUBLIC	INTERNAL USE	CONFIDENTIAL	RESTRICTED
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	
	Investment-Related Activity			X	
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X	
	Debt Amount Information			X	
	SEC Disclosure Information			X	

APPENDIX D: CYBERSECURITY ROLES & RESPONSIBILITIES

D-1: CYBERSECURITY ROLES

Every user at ACME, regardless of position or job classification, has an important role, when it comes to safeguarding the Confidentiality, Integrity, and Availability (CIA) of the information systems and data maintained by ACME. It is important that every individual fully understands their role, their associated responsibilities, and abide by the security standards, policies, and procedures set forth by the PCI DSS Cybersecurity Policy.

Role	Description of Security Role
Information Security Officer (ISO)	The ISO is accountable to the organization's senior management for the development and implementation of the information security program. The ISO will be the central point of contact for setting the day-to-day direction of the information security program and its overall goals, objectives, responsibilities, and priorities
Asset Owners	Business or department manager with budgetary authority over the system(s) with responsibility for the basic operation and maintenance of the system(s).
Asset Custodians	Under the direction of the ISO, asset custodians (e.g., system & network administrators) are responsible for the technical implementation and management of the PCI DSS Cybersecurity Policy. Party responsible for certain aspects of system security, such as adding and deleting user accounts, as authorized by the asset owner, as well as normal operations of the system in keeping with job requirements.
End Users	All employees (and contractors) are considered both custodians and users of the information systems and data on their issued information systems and are required to uphold all applicable PCI DSS Cybersecurity Policy policies, procedures, standards, and guidelines.

D-2: CYBERSECURITY RESPONSIBILITIES

Responsibilities shall be assigned based on "ownership" or stake-holding by the Information Security Officer (ISO).

Role	Description of Security Responsibility
Company Management	▪ Oversee and approve the company's information security program; ▪ Appoint, in writing, an Information Security Officer (ISO) to implement the information security program; ▪ Ensure an appropriate level of protection for all company owned or maintained information resources; whether retained in-house or under the control of contractors; ▪ Ensure that funding and resources are programmed for staffing, training, and support of the information security program and for implementation of system safeguards, as required; ▪ Ensure that persons working in an information security role are properly trained, and supported with the appropriate resources; and ▪ Provide a secure processing environment including redundancy, backup, and fault-tolerance services.
Information Security Officer (ISO)	▪ Oversee and approve the company's information security program including the employees, contractors, and vendors who safeguard the company's information systems and data, as well as the physical security precautions for employees and visitors; ▪ Ensure an appropriate level of protection for the company's information resources; whether retained in-house or under the control of outsourced contractors; ▪ Issue the PCI DSS Cybersecurity Policy policies and guidance that establish a framework for an Cybersecurity Management System (ISMS); ▪ Identify protection goals, objectives, and metrics consistent with corporate strategic plan; ▪ Ensure appropriate procedures are in place for Security Testing & Evaluation (ST&E) for all information systems; and monitor, evaluate, and report to company management on the status of

APPENDIX I: RISK MANAGEMENT FRAMEWORK (RMF)

ACME maintains an information security risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

I-1: RISK MANAGEMENT OVERVIEW

There is sometimes conflict between information security and other general system/software engineering principles. Information security can sometimes be construed as interfering with ``ease of use'' where installing security countermeasures take more effort than a ``trivial'' installation that works, but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.

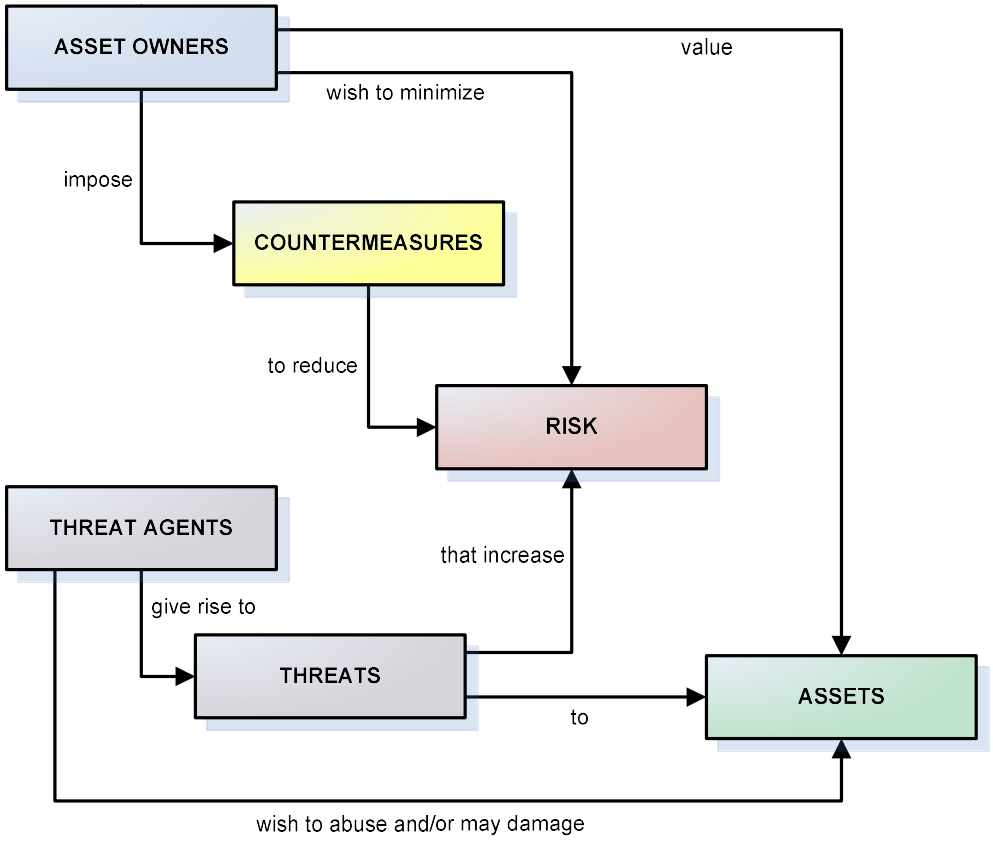

Figure I-1: Risk Overview

I-2: RISK MANAGEMENT FRAMEWORK (RMF)

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy information systems.

The Risk Management Framework (RMF) is based on NIST SP 800-37[257]:

- **Categorize**. The information system and the information being processed, stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk. The organization assigns a security impact value (low, medium, high) for the security objectives of confidentiality, integrity, or availability of the information and information systems that are needed by the organization to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

- **Select**. An appropriate set of security controls is selected for the information system after categorizing and determining the minimum security requirements. Organizations meet the minimum security requirements by selecting an appropriately tailored set of baseline security controls based on an assessment of risk and local conditions, including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

- **Implement**. Security controls must be properly installed and configured in the information system. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment.

- **Assess**. Security Testing & Evaluation (ST&E) is used to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Authorize**. Based upon a determination of the risk to operations, organizational assets, or to individuals resulting from the operation of the information system and the determination that this risk is acceptable.

- **Monitor**. Assessing selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

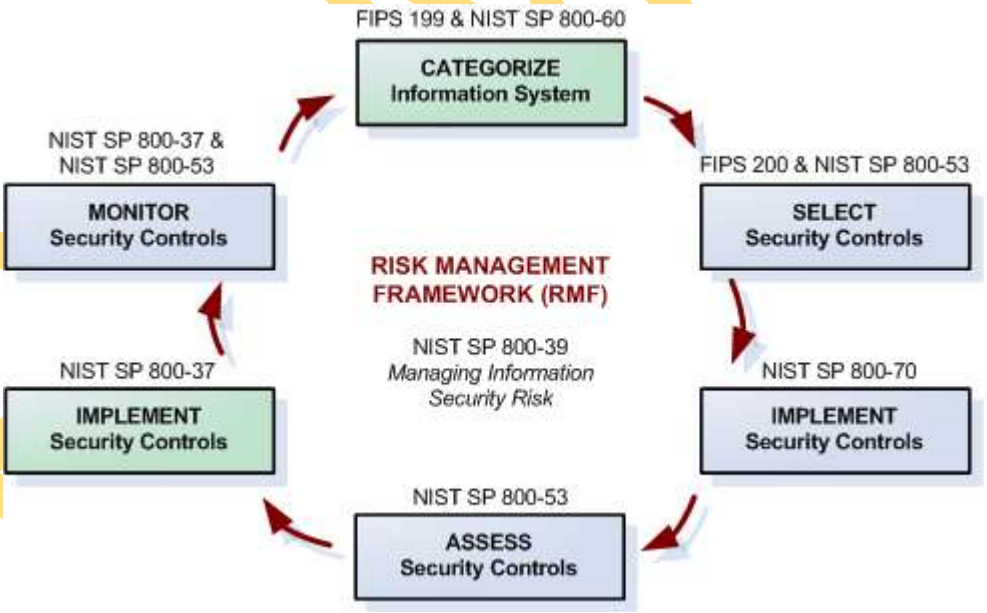

Figure I-2: Risk Management Framework (RMF)

[257] http://csrc.nist.gov/publications/PubsSPs.html

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

PLAN OBJECTIVES

The objective of Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, standards, procedures, and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

IRP ACTIONS

Incident Responders (IR) will be their experience and best judgment to respond to potential incidents in a manner consistent with the severity level posed by the incident. If necessary, the IR will obtain external assistance to help with the triage and cleanup operations.

INCIDENT DISCOVERY

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

Malicious Software (malware) Examples	You might be infected with malware if you see…
A virus that spreads through email infects a host.	• Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A worm that spreads through a vulnerable service infects a host.	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host.	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes
Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse.	• Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host.	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message.	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others