Your Logo
Will Be
Placed Here

CYBERSECURITY VULNERABILITY & PATCH MANAGEMENT PROGRAM (VPMP)

ACME Business Solutions, Inc.

VPMP
Vulnerability & Patch Management Program

Table of Contents

Executive Summary

Vulnerabilities pose a significant risk to the confidentiality, integrity, and availability of ACME resources, as well as those who access ACME systems. To reduce this risk, it requires a team effort to identify and remediate vulnerabilities in a timely manner.

What a Vulnerability Management Program is and Why ACME Needs One

A vulnerability management program is a systematic way to find and address weaknesses in information security defenses. Being systematic about seeking out flaws reduces the chance of surprises. Addressing security issues methodically gives you a better assurance that gaps have been closed as quickly as possible. This program reduces the chance of lost revenue and productivity that can result from intrusions or application failures.

Document Contents

This document contains a complete map of how information security vulnerabilities are addressed by ACME. First, it explains terms that stakeholders need to understand, such as the differences between "vulnerability" and "risk treatment." Then it shows what actions are required to find and classify issues. Next, you will learn how the software patching process works, as part of the overall vulnerability management program. Finally, this document describes the tools and processes that help ACME discover new security issues and verify that known issues are fixed in a timely manner.

Target Audience

The target audience for this document includes both business process owners and IT personnel responsible for maintaining the networks, systems, databases and applications that allow ACME to function.

The vulnerability management program document is for IT and information security personnel as well as those responsible for important business processes. Anyone responsible for the safe operation of applications in the business should understand the concepts explained here. Everyone obligated to safeguard employee and client information benefits from understanding this vulnerability management program.

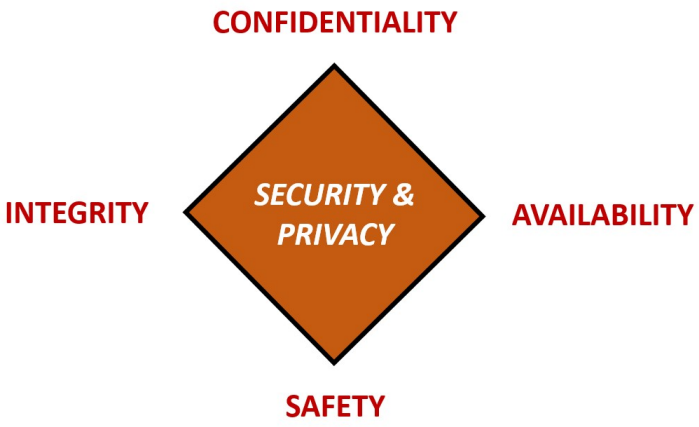
How To Use this Document

First off, review the table of contents and read through the document. Take your time to understand the terminology as it applies to vulnerability management - there are references at the end of the document to help with acronyms. When you finish reading this document, you should understand what action is needed from you and your team. If any part of those responsibilities is unclear, discuss this with ACME's sponsor of this program. Work with the sponsor to update this document for better clarity.

Thoroughly review this document at least once a year, since change is a constant and changes will impact how vulnerabilities are managed at ACME. Stakeholders in the program, like yourself, can continually improve this program by revisiting, discussing, and updating it.

The Vulnerability & Patch Management Program (VPMP) provides definitive information on the prescribed measures used to manage cybersecurity-related risk at ACME Business Solutions, Inc. (ACME). The main objective of the VPMP is to detect vulnerabilities to reduce possible exposure to harm in a timely manner.

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Protecting company data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure availability, integrity, confidentiality and safety:



- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited 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.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated to cause physical impact by nefarious actors.

As the VPMP matures, it will become increasingly efficient and streamlined while the quantity and severity of discovered issues decrease. Essentially, the overall resiliency of the IT infrastructure is strengthened by a mature VPMP. An effective VPMP is a team effort involving the participation and support of every ACME user who interacts with data and systems. Therefore, it is the responsibility of every user to conduct their activities according to the VPMP to reduce risk across the enterprise.

SCOPE

The scope of the VPMP encompasses all ACME networks and geographic locations, regardless of what entity "owns" or maintains the asset(s):

- ACME-controlled environments:
  - Corporate
    - Production
    - Stage
    - Development
    - Test
  - Retail
    - eCommerce
    - Brick & mortar (e.g., Point of Sale (POS) devices)
  - Telecommunications
    - Voice over Internet Protocol (VoIP)
    - Private Branch Exchange (PBX)
    - Instant Messaging (IM) solutions
    - Electronic mail (email)
    - Video teleconference
  - Physical Infrastructure
    - Heating, Ventilation and Air Conditioning (HVAC) systems
    - Physical access control systems (e.g., proximity badges)
    - Alarm & video surveillance systems
  - Bring Your Own Device (BYOD)
- 3rd party-controlled environments:

- Service providers
- Cloud hosting
- 3rd party developers
- Staff augmentation

What Are Common Vulnerabilities?

Vulnerabilities exist beyond unpatched software. Vulnerabilities can also take the form of:

- Technical Vulnerabilities
  - Open ports;
  - Incorrectly configured software (e.g., access permissions, password policy, user rights, encryption, etc.); and
  - Unnecessary services or unnecessarily installed software.
- Non-Technical Vulnerabilities
  - Weak physical access control to buildings or areas housing key IT infrastructure;
  - Untrained or poorly trained IT / cybersecurity personnel; and
  - Lack of formalized program documentation:
    - Enterprise security policies & standards;
    - Disaster recovery plans;
    - Business Continuity / Disaster recovery (BCDR) plans;
    - Data backup & recovery procedures;
    - Acceptable use standards;
    - Configuration management standards; and
    - Hardware and software inventories.

A vulnerability is any flaw that can be exploited by a malicious user to gain unauthorized access to an asset. Personnel responsible for managing vulnerabilities must not only be aware of evolving vulnerabilities and corresponding patches, but also other methods of remediation to reduce the exposure of assets to exploitation. Such personnel should also know that:

- A patch is an additional piece of code written by a vendor to remove "bugs" in software.
- A patch often addresses security flaws within software.
- Not all vulnerabilities have corresponding patches.
- Vulnerabilities without patches require compensating controls to reduce the risk of exploit.

What Is Meant By Managing Vulnerabilities?

Vulnerability Management (VM) is the process of coordinating activities to prevent the exploitation of vulnerabilities. The alternative to vulnerability management is crisis management, so the preventative benefits of VM outweigh the reactive expenses, which include operational impacts, corrupted data, and negative client/public relations.

Like any organization, ACME needs to balance its security needs with usability and availability. For example, installing a new patch may "break" other applications. This can best be addressed by testing patches before deployment. Another example is that forcing application restarts, operating system reboots, and other host state changes can be disruptive to both internal and client-facing services. The good news is ACME can minimize VM-related impacts through testing solutions in a similar test/stage/dev environment and have scheduled maintenance windows when changes can be implemented.

WHEN SHOULD VULNERABILITIES BE MANAGED?

Vulnerabilities should be managed continuously since the risk associated with vulnerabilities is constantly changing.

Vulnerability-related risks can arise from both internal and external sources. While it is not possible to have a totally risk-free environment, it is possible to proactively manage vulnerabilities to maintain secure systems, applications, and websites.

The concept of managing vulnerabilities is summed up in the diagram below, showing the relationships involved:

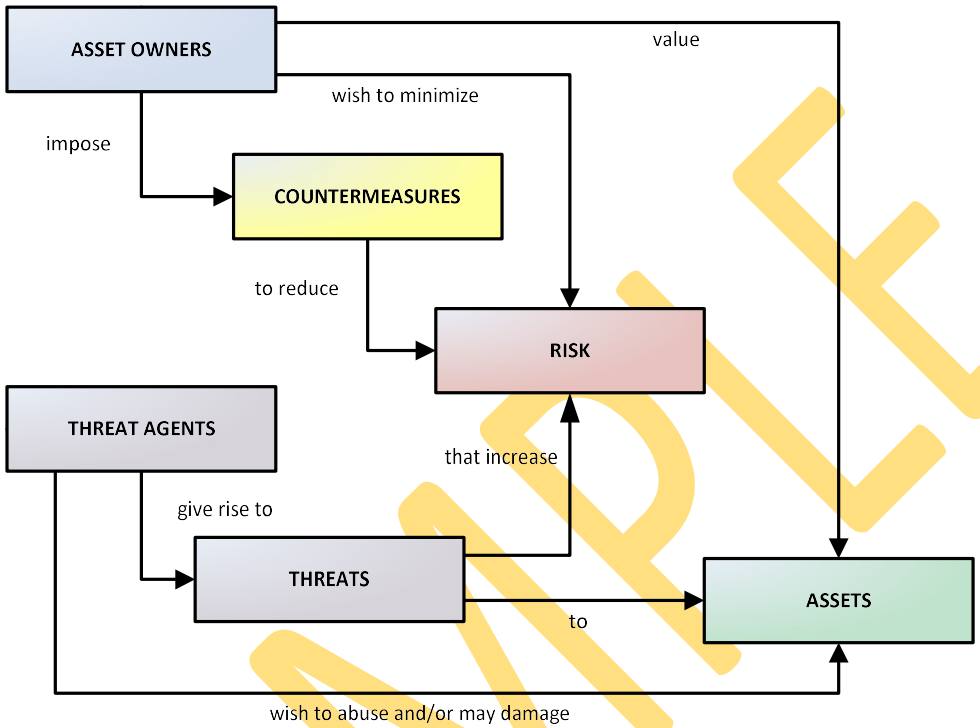


Figure 1: Understanding connected nature of managing risk - vulnerability management focuses on countermeasures.

Who Has The Authority To Manage Vulnerabilities?

Determining how to handle risk associated with vulnerability and patch management is always a management decision. Appendix A – VPMP Roles & Responsibilities provides more granular guidance on VPMP-related roles and responsibilities.

It is important to keep in mind that VM is far more than a "technology issue" and it requires the direct involvement of business process owners, IT personnel, and cybersecurity. Each has a role to play in vulnerability management operations:

Business Unit

- The Business Unit (BU) that requires the technology to be in place and function ultimately "owns" the risk associated with the ongoing operation of systems.
- Business Process Owners (BPOs) are individuals within BUs who are responsible for working with IT to identify mutually agreed upon maintenance windows that will allow for patching and other maintenance activities to be performed.
- BPOs are the central point of contact for IT and cybersecurity to work with on risk management decisions.

Information Technology

- IT has a shared responsibility with the BUs to securely operate and maintain systems.
- IT focuses on technology management through managing and executing vulnerability management tasks.

Cybersecurity

- Cybersecurity operates as a facilitator of risk-related vulnerability and patch management decisions.
- Cybersecurity focuses on providing expert guidance and support to both IT and the Business Unit.

Figure 2: Vulnerability governance model.

VULNERABILITIES IN LAYERED DEPENDENCIES

Dependencies are of critical importance when assessing vulnerabilities across the network since vulnerabilities can have a cascading effect.

Ideally, a vulnerability assessment for a specific application or host should leverage existing vulnerability assessments that address "upstream" risks. For example, a well-designed and securely coded application could be compromised if the host system it is running on is insecure. Similarly, the application could be made unavailable if the datacenter lacks measures to ensure uptime against natural or man-made threats.

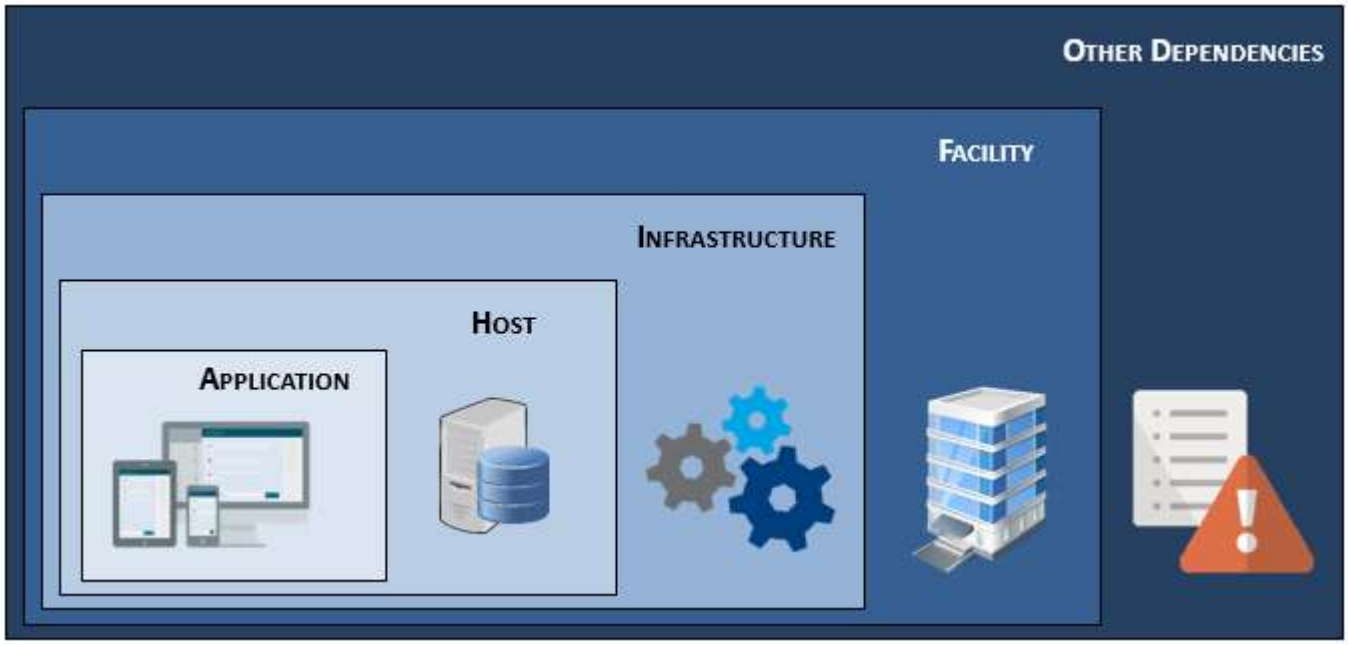


Figure 3: Layers of dependency-based vulnerabilities.

As part of overall vulnerability management, ACME should perform several formal vulnerability assessments, which are meant to be used as references for more detailed project-specific risk assessments. At a minimum, standing vulnerability assessments should exist for:

- Datacenters (including infrastructure risks)
- Secure configurations for hosts and major applications (e.g., databases, email, Intranet)

By being able to leverage those existing vulnerability assessments, it will allow for more efficient assessments of applications and systems.

APPLICATIONS

Vulnerabilities associated with applications include, but are not limited to:

- Insecure code (developers did not follow secure coding practices)
- Default/weak credentials
- Weak encryption
- Passwords/sensitive data stored in clear text
- Lack of access control
- Missing software patches
- Logging/monitoring not being performed

HOST

Vulnerabilities associated with hosts include, but are not limited to:

- Lack of system hardening
- Default/weak credentials
- Lack of encryption at rest
- Lack of access control
- Missing software patches
- Logging/monitoring not being performed
- Backups not being performed

Managers need to identify their role in contributing to ACME's wider goals, objectives, values, policies and strategies when making risk-based decisions about vulnerability management. This assists with defining the criteria by which it is decided whether a risk is tolerable or not, and forms the basis of controls and management options.

VULNERABILITY MANAGEMENT METHODOLOGY

ACME recognizes the National Institute of Standards and Technology (NIST) 800-115 *Guide to Security Testing and Assessment*.[1] as the reference framework for conducting vulnerability management operations. ACME also recognizes that no one technique can provide a complete picture of ACME's security posture, and therefore flexibility will be maintained to choose techniques that best meet stakeholder requirements.

NIST 800-115 consists of six (6) main sections that form the basis for vulnerability management activities. This methodology captures the entire process, in a manner that makes sense to stakeholders and provides value for ACME's security posture, including:

- Review techniques;
- Target identification and analysis techniques;
- Target vulnerability validation techniques;
- Security assessment planning;
- Security assessment execution; and
- Post-testing activities

RISK MANAGEMENT MATURITY LEVELS

The Vulnerability Management Capability Maturity Model (VM-CCM) provides standardized criteria by which organizations can benchmark risk management strategies to identify program maturity levels, strengths and weaknesses, and next steps in the evolution of an Enterprise Risk Management (ERM) program.[2]

The VM-CMM levels are organized progressively from "non-existent" to "optimized" and depict corresponding levels of vulnerability management competency. The VM-CMM helps the leadership team define a roadmap to the successful adoption of an ERM program. The ERM program is designed to govern risks across all areas of the business in order to identify strategic opportunities and reduce uncertainty. The VM-CMM is its applicability regardless of the specialized frameworks and standards that ACME uses.

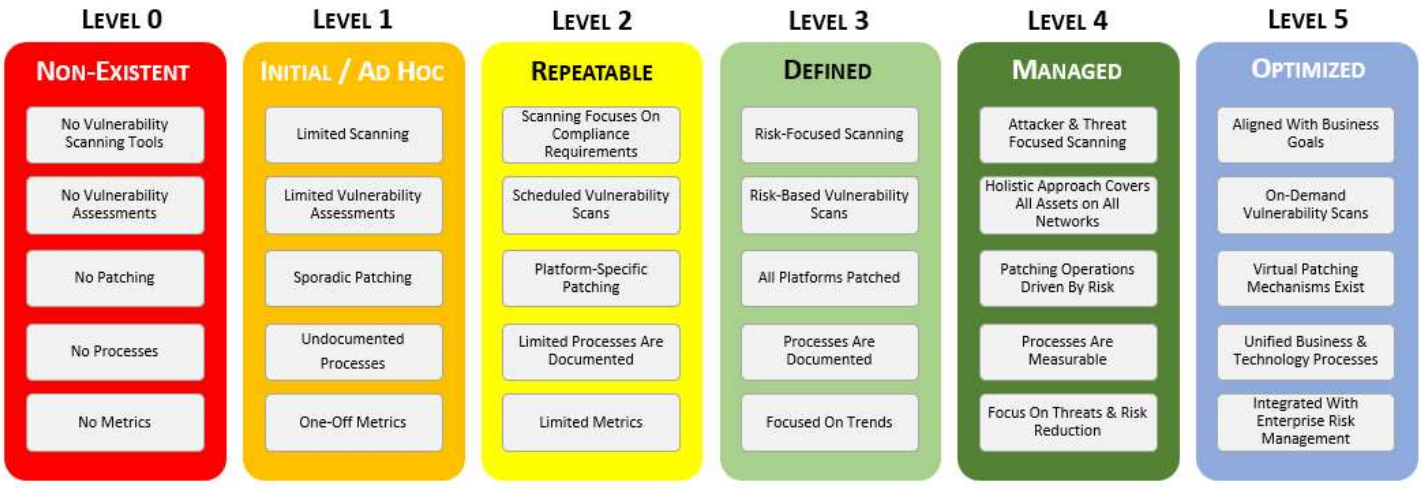


Figure 4 – Vulnerability Management Capability Maturity Model.

TARGET VULNERABILITY MANAGEMENT LEVEL

As part of ACME's multi-year strategy to reduce vulnerabilities, the target is to achieve at least a Level 3 (Defined) VM-CMM level of program maturity.

[1] NIST 800-115 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
[2] Risk Management Society - https://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx

Risk Considerations for Vulnerability Management

In terms of managing the risk associated with vulnerabilities and software patching, there are three time-based areas of risk to consider that address the window of exposure:

- Black Risk,
- Gray Risk, and
- White Risk.

When dealing with these areas of vulnerability-related risk, the goal is to minimize the window of exposure. The window of exposure for a system or application is the time period between an exploit for a specific vulnerability becoming available and when a counteracting patch is installed. In most cases, security patches exist because of a known exploit or the expectation that one will be created by vendors upon public release of the vulnerability notification.

Black Risk

Black Risk is the time between when a new vulnerability is first discovered and when it is publicly disclosed.

- Black Risk is the phase of a vulnerability cycle that is governed by malware researchers and hackers since the vulnerability information is not publicly known.
- Exploits may be developed during the Black Risk phase. If an exploit is developed during this phase, it is considered a 0-Day exploit, since patches are not available.
- Applying industry-recognized leading practices and a defense-in-depth strategy is the only defense against Black Risk.

Gray Risk

Gray Risk is the time between the disclosure of a unique vulnerability and the availability of a patch.

- Gray Risk is the phase of a vulnerability cycle that is governed by software vendors since the vendors are relied upon by end users to create the appropriate patch to address the vulnerability.
- Exploits may be developed during the Gray Risk phase. If an exploit is developed during this phase, it is not considered a 0-Day exploit.
- Applying vendor-recommended mitigation steps, in addition to applying industry-recognized leading practices and a defense-in-depth strategy, is the only defense against Gray Risk.

White Risk

White Risk is the time between the availability of a patch and when the patch is installed.

- White Risk is the phase of a vulnerability cycle that is governed by system administrators since the task of applying the patch is their assigned duty.
- Exploits may be developed during the White Risk phase. If an exploit is developed during this phase, it is not considered a 0-Day exploit.
- Applying vendor-recommended mitigation steps, in addition to applying industry-recognized leading practices and a defense-in-depth strategy, is the only defense against Gray Risk.

Risk Associated With 0-Day Patches

Most patches from vendors are considered a "0-Day Patch" which is when the disclosure of the patch is made at the same time the patch is released.

- Essentially, this eliminates the Gray Risk phase altogether since a solution exists from the vendor upon public disclosure of the vulnerability; and
- The focus of patch mitigation with 0-Day Patching is associated with evaluating and installing the patch in an expeditious manner.

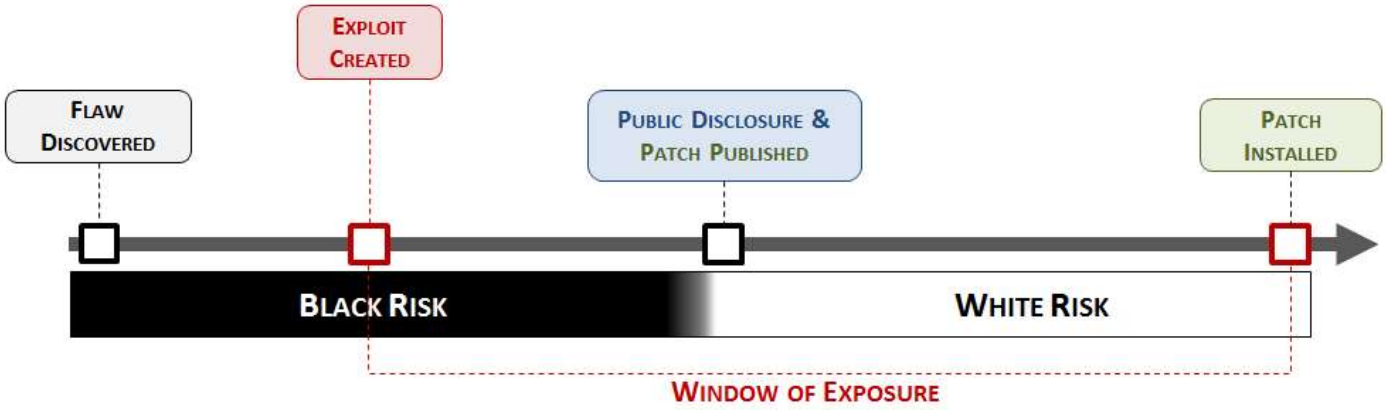


Figure 5: Zero-day patch – Black & White Risk.

Risk Associated With 0-Day Exploits

Several times a year, "0-Day Exploits" occur which is when there is:

- A disclosure of a new vulnerability (likely being exploited in the wild); and
- There is no corresponding patch available to remediate the flaw.

This creates the Gray Risk phase where the focus for ACME is risk mitigation through implementing a defense-in-depth approach that includes vendor-recommended remediation steps to decrease the likelihood of exploit.

- During the Gray Risk phase, a defense-in-depth approach to cybersecurity and compensating controls are the only defensive alternatives; and
- Risk must be managed during the Gray Risk phase to balance functionality vs. security.

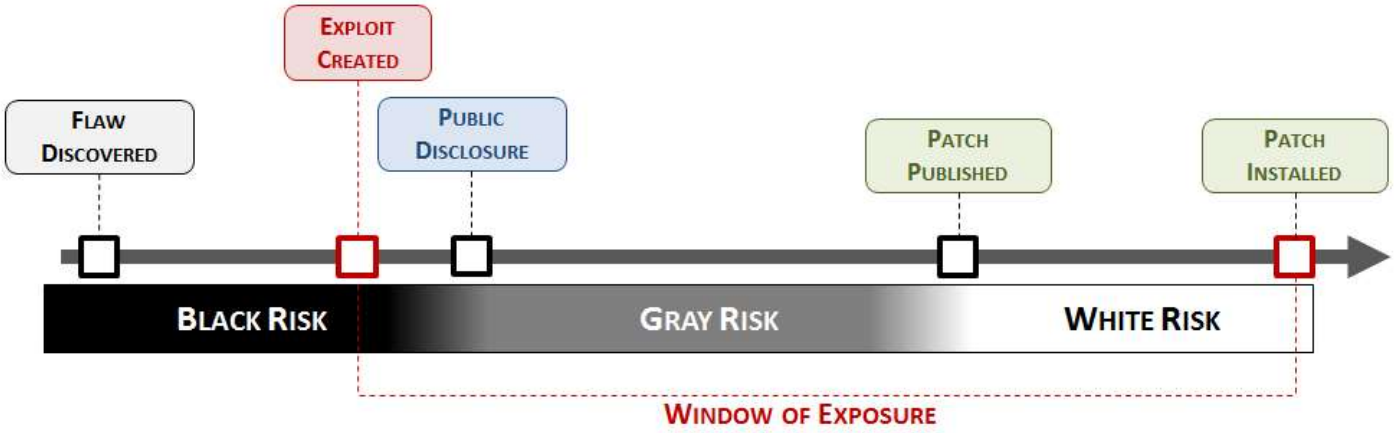


Figure 6: Zero-day exploit – Gray Risk.

Flaw Remediation (Patch Management)

Vulnerability management includes patch management as a core component. While a missing patch is always associated with a vulnerability, a vulnerability may not always have a patch associated with it. A vulnerability may simply be associated with a configuration and have nothing to do with a software patch.

Flaw Classification

Flaws, including software patches or other vendor releases to address vulnerabilities, are categorized into the following four (4) categories:

Rating	Flaw Rating Criteria
Critical	- Vulnerability is weaponized and automated, so it does not require user action. - Vulnerability is remotely exploitable.
Important	- Vulnerability is weaponized, but requires user action. - Vulnerability is not remotely exploitable.
Moderate	- Exploitation is published, but it is difficult to exploit. - Exploitability is mitigated to a high degree by defense-in-depth.
Low	- Exploitation is unpublished or extremely difficult. - Impact is minimal

Figure 7: Flaw classification model.

Zone-Based Approach To Flaw Remediation

Managing vulnerabilities in operating systems and applications rely, in great part, on the software vendor. All vendors differ in their approach to publishing software patches, and sometimes software fixes are not currently available. That means there are situations where alternate remediation steps may be required to minimize the risk to the organization. The goal of managing software patching operations is to minimize the window of exposure. Categorizing the network into "zones" is an efficient manner to approach patch management.

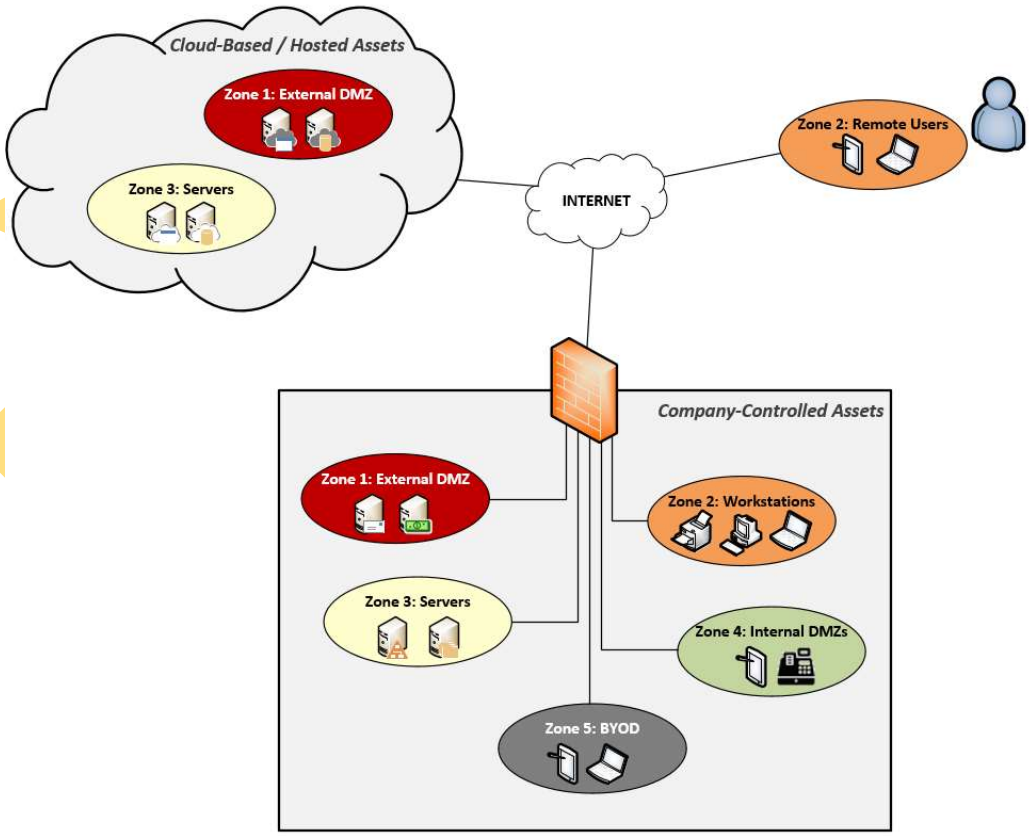


Figure 8: Zone-based patching model.

VULNERABILITY ANALYSIS PROCESS

Vulnerability analysis, in relation to patch management, is the process of determining when and if a patch should be applied to a system.

It is necessary that security personnel analyze and determine whether the system is vulnerable to identified attacks. A method used to determine if a system is vulnerable to an identified attack is the "vulnerability footprint," also known as the attack surface. The vulnerability footprint consists of four (4) key elements

- Deployment;
- Exposure;
- Impact; and
- Simplicity.

The assessment of risk should be in accordance with ACME's Risk Management Program (RMP).

VULNERABILITY FOOTPRINT

The following elements define the vulnerability footprint and can be used by vulnerability management personnel in determining the criticality of patching systems and applications:

DEPLOYMENT

The deployment component relates to the asset's location in the network. The zone-based categorization (see Figure 9) is an efficient way to determine the deployment of an asset.

- A higher deployment rating would be assigned to an asset that is exposed to the Internet (e.g., DMZ).
- A lower deployment rating would be assigned to an asset that is in an internal segment with limited Internet access.

EXPOSURE

The exposure component relates to the available layers of defense and existing controls.

- A higher exposure rating indicates that an attacker could gain unauthenticated access to the asset from another less-secure network (e.g., the Internet).
- A lower exposure rating indicates that an attacker could gain limited physical access.

IMPACT

The impact component relates to assessing the risk associated with the successful exploitation of a vulnerability (see Assessing Impact section below).

- A higher impact rating indicates that an attacker could successfully exploit a vulnerability and gain full system control.
- A lower impact rating indicates that an attacker could gain enough information for a preliminary reconnaissance effort on ACME's network architecture.

SIMPLICITY

This simplicity rating applies to the relative ease of the technical exploit.

- A higher simplicity rating indicates an exploit that is readily available and only requires basic hacking skills to use (e.g., script kiddie exploits).
- A lower simplicity rating indicates that the exploit requires a high level of computer skill and related knowledge.

Assessing Impact

When scanning for vulnerabilities, findings can be easily rated on a 1-5 severity scale, with 1 being "low risk" and 5 "high risk." Asset owners and asset custodians must prioritize the remediation of severity 4 and 5 vulnerabilities before addressing lower severity vulnerabilities.

One important concept to understand is that risk is variable - it is able to be changed and is not static. This is important to keep in mind since the "risk rating" is subject to change as the risk environment changes. What is crucial to understand is that risk represents exposure to harm or loss. This is commonly quantified as a combination of potential impact, likelihood and control effectiveness.

Impact Level	Vulnerability Impact Severity Description
1	The threat is limited to information gathering. Exposure includes information about the host (e.g., open ports, services, etc.) that may be useful to find other vulnerabilities. This can include software versions, directory browsing and security mechanisms being used.
2	Service / application / host is susceptible to a denial of service attack.
3	It is reasonable to assume a dedicated and competent threat can gain control of the host. *Note: Exposure includes read/write access to data and privileged access to the host and its applications.*
4	Widely available tools exist that can allow threats to gain control of the host. *Note: Exposure includes read/write access to data and privileged access to the host and its applications.*

Figure 11: Vulnerability impact assessment

Impact Assessment Methods

Methods used in analyzing impact can be:

- Qualitative;
- Semi-Quantitative; or
- Quantitative.

The degree of detail required to assess impact will depend upon the application, the availability of reliable data and ACME's decision-making needs.

Qualitative Assessments

Qualitative assessment defines consequence, probability, and level of impact by significance levels such as "high," "medium" and "low," may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-Quantitative Assessments

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic or have some other relationship.

Quantitative Assessments

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context.

Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analyzed, influence of human factors, or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Issues to Consider

The following issues should be considered when creating the patch management plan and the processes and policies related to it:

Testing

It is always recommended that ACME maintain a duplicate of critical systems in a testing environment.

For some scenarios, it is adequate to simulate application functions without absolute system replication accuracy. The primary function of a test bed/simulator is to mitigate risk prior to implementing changes to the operational environment. An additional benefit from a test bed/simulator is to allow operator training on new configurations, checklist development, and evaluate procedures prior to deployment on production systems.

Archiving / Data Backups

An archive image or data backup of the existing stable operating system must be captured before production patching is conducted to create a valid restoration point. It is recommended that asset custodians backup the operational system and restore it on the test bed/simulator system. This activity validates that the restore point is usable for disaster recovery.

Contingency

Asset owners should consider the worst-case scenario in developing contingencies. Assuming a worst-case scenario where patch installation does not restore the system to a stable condition or patch installation and/or removal activity affects other applications, determine if the disaster recovery point restores the system to a stable configuration.

Asset custodians, in coordination with the asset owner, should establish criteria (e.g., System Security Plan (SSP) or memorandum of understanding) based on the system's functionality over a specific duration that incorporates timing considerations. An operational test plan should be developed to exercise, validate, and document proper operation of primary applications running in the same environment. This is to ensure stable, functional system operations prior to a return to service.

Regulatory Requirements

A growing number of statutory and regulatory bodies require organizations to develop and maintain means of identifying vulnerabilities and remediating them in a timely manner. To demonstrate compliance, documentation containing the identification and eradication of the vulnerability must be kept.

For areas of ACME's computing environment where there is no definitive timeline for remediating vulnerabilities by a statutory or regulatory requirement, ACME will document its own timeline. [Company Name} will focus on good security and continue to show a trend associated with remediating vulnerabilities as measured against its internal goals.

Implementing Patches

It is always recommended to deploy patches in order of less critical to more critical. This can be accomplished by first deploying patches to test environments, followed by staging environments, and finally to production environments.

A sample flow chart implementing patches is shown below:

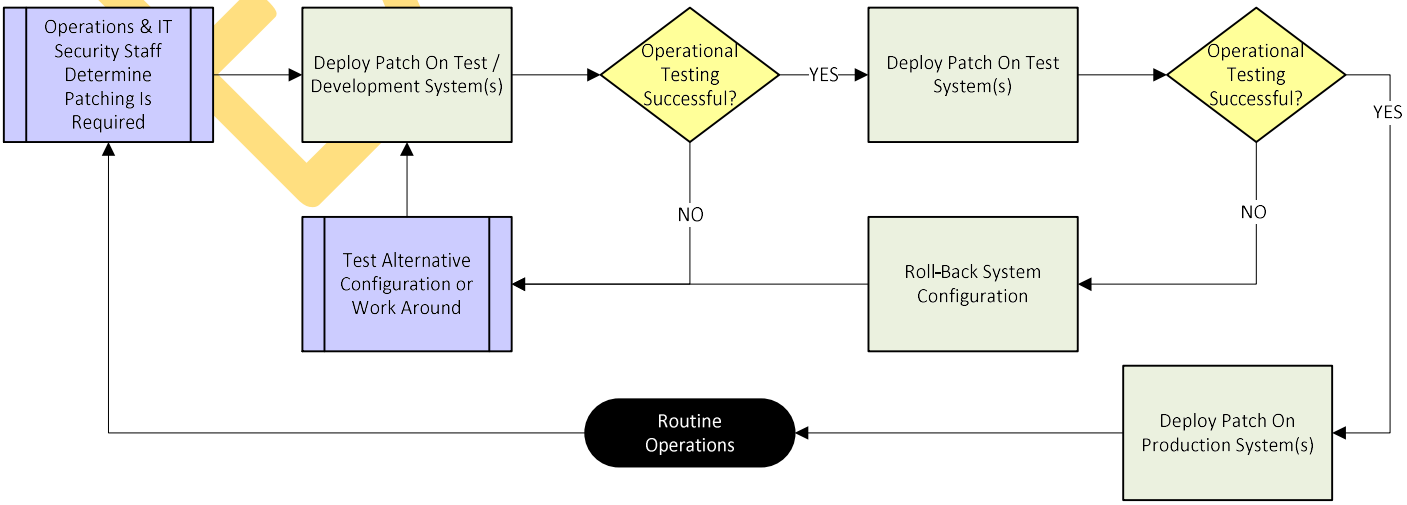


Figure 14: Patch deployment overview.

The flowchart shown below (see Figure 15) depicts a more detailed approach to patch management, including stakeholder involvement.

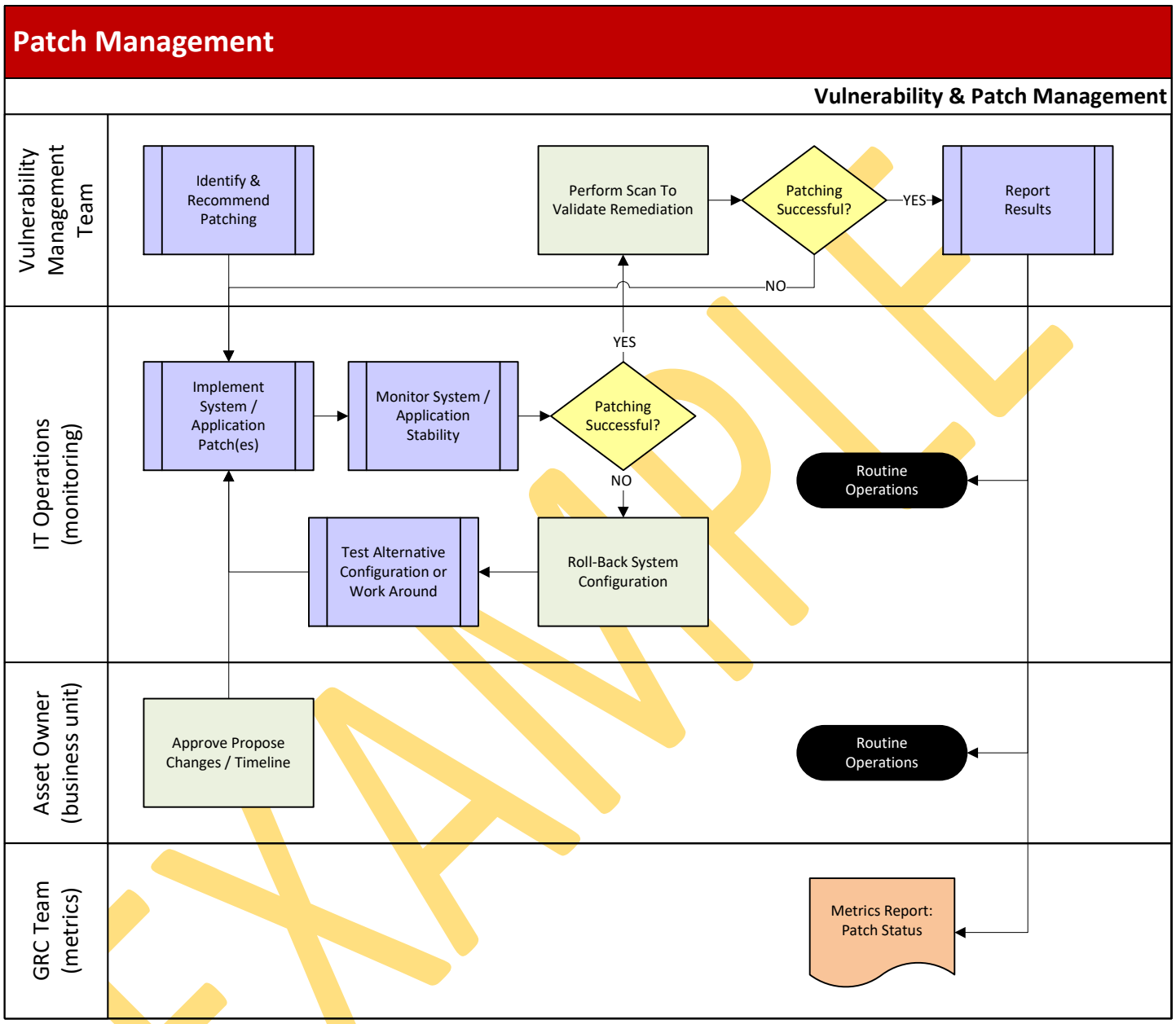


Figure 15 – Patching process flowchart.

REMEDIATION OPERATIONS & ENFORCEMENT

Systems and applications not remediated within the required remediation schedule or timeframe will be classified as non-compliant and will be quarantined. Under normal circumstances, non-compliant system and application owners will be provided a warning seven (7) days prior to removal from the network and quarantined.

If quarantining is not technically feasible, compensating controls will need to be implemented to mitigate the risk.

The assessment of risk should be in accordance with ACME's Risk Management Program (RMP).

Appendix C – Plan Do Check Act (PDCA) Approach To VPMP Governance

PCDA Approach to VPMP Governance

The Vulnerability & Patch Management Program (VPMP) fits nicely into the Plan-Do-Check-Act (PDCA) model. Each process aligns with a component of the VPMP as shown below.

Plan

The planning phase of the VPMP involves gathering internal and external requirements for detecting vulnerabilities and addressing the associated risk.

Do

The risk treatment plan is implemented in this phase. Risks are mitigated to the company's acceptable levels. The plan may include patching systems to acceptable levels, decommissioning systems (removing them from the environment), or applying compensating controls.

Check

Systems are monitored regularly to ensure vulnerability compliance requirements are met. Companies may choose to run the minimum number of scans required to meet compliance requirements.

Act

The data generated from previous phases is used to improve the VPMP. Changes may apply to company security policies, practices, and procedures. These changes may result in organizational risk reduction, increased process efficiency, and improved regulatory compliance. Common areas of improvement are:

- Asset management;
- Configuration management; and
- Assessment management.

Project Management Approach to Patching & Vulnerability Management

While not all patching & vulnerability management activities will raise to the level of project management-level initiatives, the project phases defined in the Project Management Body of Knowledge (PMBOK) apply well to the VPMP for complicated patching environments. This is most applicable when internal and external environments must be governed to ensure patch management is being conducted in a professional manner.

In accordance with PMBOK practices, every project begins with a plan.[7] The plan serves as the roadmap or guideline needed to complete the objective and can aide in large, complex remediation efforts that include:

1. Initiating;
2. Planning;
3. Executing; and
4. Controlling & Monitoring.

1. Initiating Phase

The first project phase is the initiating phase, and it includes:

- Identifying stakeholders;
- Project charter;
- Project objective;
- Project scope;
- Assumptions;
- Constraints;
- Change management;
- Risks; and
- Communication strategy.

[7] A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2008).

Identifying Stakeholders

Common stakeholders in a VPMP are:

- IT management and business unit representatives;
- IT security, compliance or audit team;
- IT infrastructure teams including:
    - Server team (Windows, Linux, Unix, Virtualization platform, etc.)
    - Network team (internal and perimeter equipment)
    - Storage team, and
- IT application and operating system support teams.

Project Charter

The project charter authorizes the project and documents the initial project and stakeholder requirements. This includes regulatory or contractual requirements for a VPMP and what the project hopes to achieve. In addition, the project charter contains the project objective (acceptance/success criteria), scope, assumptions, constraints, risks and the communication strategy.

Project Objective

The project objective provides a high-level statement of the desired outcome or success criteria of the project. It answers the question, "What is deemed project success?" Success criteria are written as a specific and measurable way to quantify the delivery of project requirements.

Project Scope

The charter's project scope provides the high-level details required to meet the project objectives. It provides project parameters – what is both inside and outside of the project's scope. Project details may be unknown when the project character is created. Known items are included in scope with a process to clarify scope as further information becomes available. Project charter scope provides the foundation for the evolving project plan and more detailed scope. The project is complete when all in-scope items have been satisfied.

Assumptions

Assumptions are documented in the project charter. Assumptions may exist throughout the project. However, most assumptions will be evaluated and adjusted during the more detailed planning and execution phases. Common examples of project assumptions may include:

- Management support for this project will remain constant.
- Funding for this project will not be affected by other organizational changes or priorities.
- Resources for this project will be available until project completion.

Constraints

Constraints may exist that cannot be changed. The project may be limited by organizational structure, company priorities, and corporate culture. Any known constraints should be documented in the charter.

Change Management

Changes occur in every project. A process is required to evaluate the change, assess its impact and ultimately approve requested changes. Stakeholders must review and approve all change requests because project time, cost and budget may be affected. Changes must not be implemented without written stakeholder approval.

Risks

Stakeholders identify high-level risks, which are subsequently documented in the project charter. Regulatory risk and competitive risks are included in this section, both examples of strategic risk. Other elements to include:

- How much risk is acceptable?
- How is risk managed (e.g., avoid, reduce, transfer or accept)?
- What are the financial and legal consequences of project failure?

Communication Strategy

Effective communication is critical to the success of every project. This section documents the frequency, type of communication (reports, status meetings, etc.) and participants (if known at the time of project charter creation). Common communication items include:

- Stakeholder review and approval of project documents.
- Formal presentation and approval of milestones. (Approval facilitates proceeding to the next phase.)
- Status reports.
- Tasks planned and completed during the reporting period.