Your Logo
Will Be
Placed Here

CYBERSECURITY VULNERABILITY & PATCH MANAGEMENT PROGRAM (VPMP)

ACME Business Consulting, LLC

VPMP
Vulnerability & Patch Management Program

Table of Contents

Executive Summary 5

Vulnerability & Patch Management Program Overview 6

Scope 6

What Are Common Vulnerabilities? 7

What Is Meant By Managing Vulnerabilities? 7

When Should Vulnerabilities Be Managed? 7

Who Has The Authority To Manage Vulnerabilities? 8

Business Unit 8

Information Technology 8

Cybersecurity 8

Vulnerabilities In Layered Dependencies 9

Applications 10

Host 10

Infrastructure 10

Facility 10

Other Dependencies 10

Risk Treatment Options For Vulnerability Management 10

Reduce Risk 11

Avoid Risk 11

Transfer Risk 11

Accept Risk 11

Vulnerability Management Fundamentals 12

Vulnerability Management Methodology 12

Risk Management Maturity Levels 12

Target Vulnerability Management Level 12

Risk Considerations for Vulnerability Management 13

Black Risk 13

Gray Risk 13

White Risk 13

Risk Associated With 0-Day Patches 14

Risk Associated With 0-Day Exploits 14

Flaw Remediation (Patch Management) 15

Flaw Classification 15

Zone-Based Approach To Flaw Remediation 15

Recommended Timelines for Patching 16

Patching Strategy 17

Vulnerability Management Governance 19

Key Activities 19

Manage The Asset Inventory 19

Categorize Assets 20

Identify Vulnerabilities 20

Assess Risks 20

Remediate Flaws 21

Vendor-Maintained Systems 21

Vulnerability Analysis Process 22

Vulnerability Footprint 22

Deployment 22

Exposure 22

Impact 22

Simplicity 22

Assessing Impact 23

Impact Assessment Methods 23

Qualitative Assessments 23

Semi-Quantitative Assessments 23

Quantitative Assessments 23

System & Application Patching 25

Information Security Considerations for Patching Systems 25
Tool Selection 25
Patch Management Lifecycle 25
Assess 25
Identify 26
Evaluate & Plan 26
Deploy 26
Patching Process Overview 27
Patch Review Process 27
Issues to Consider 27
Testing 28
Archiving / Data Backups 28
Contingency 28
Regulatory Requirements 28
Implementing Patches 28
Remediation Operations & Enforcement 29
Exceptions 31

Vulnerability Scanning 32

Vulnerability Scanning Overview 32
External Scanning 32
Internal Scanning 32
Recurring Validation 32
Tool Selection 32
Scan Preparation 33
Associated risks 33
Scanning Operations 33
Discovery Scanning 33
Scan Frequency 33
External Scanning 33
Internal Scanning 34
Remediation Actions 34
Validation Phase 34

Penetration Testing 35

Establishing Goals for Penetration Testing 35
Stakeholder Business Analysis 35
Penetration Testing Methodology 35
Types of Penetration Testing 36
Black Box Penetration Testing 36
White Box Penetration Testing 36
Gray Box Penetration Testing 36

Information Assurance (IA) 37

Security Testing & Evaluation (ST&E) 37
Pre-Production Testing 37
Post-Change Testing 37
Security Control Assessment (SCA) Methodology 37
NIST 800-37 Risk Management Framework – Security Life Cycle 38

Appendices 40

Appendix A – VPMP Roles & Responsibilities 40
Chief Risk Officer (CRO) 40
Chief Information Security Officer (CISO) 40
Executive and Senior Management 40
Line Management 40
All Employees 41
Asset Owner 41

Internal Audit 41
Vulnerability Management Personnel 41
Asset Custodians 41
Appendix B: Compensating Controls **42**
Preventative Controls 42
Detective Controls 42
Corrective Controls 42
Recovery Controls 42
Directive Controls 42
Deterrent Controls 42
Appendix C – Plan Do Check Act (PDCA) Approach To VPMP Governance **43**
PCDA Approach to VPMP Governance 43
Project Management Approach to Patching & Vulnerability Management 43
Glossary: Acronyms & Definitions **47**
Acronyms **47**
Definitions **47**
Record of Changes **48**

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 cybersecurity 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 cybersecurity 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 cybersecurity 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.

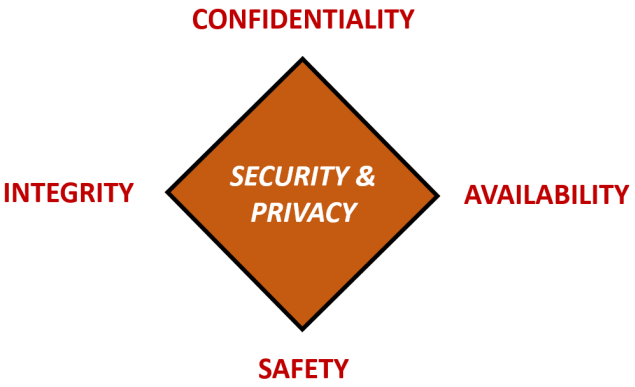
How To Use this Document

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 Consulting, LLC (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:

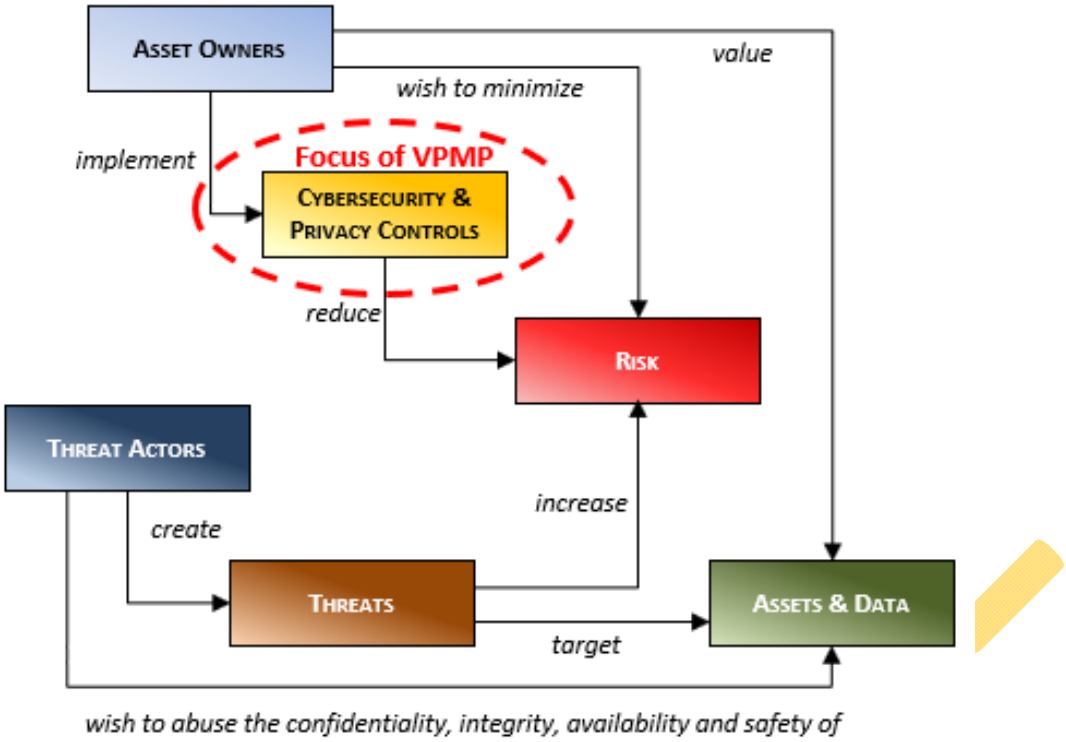


Figure 1: Understanding connected nature of managing risk - vulnerability management focuses on countermeasures.

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.

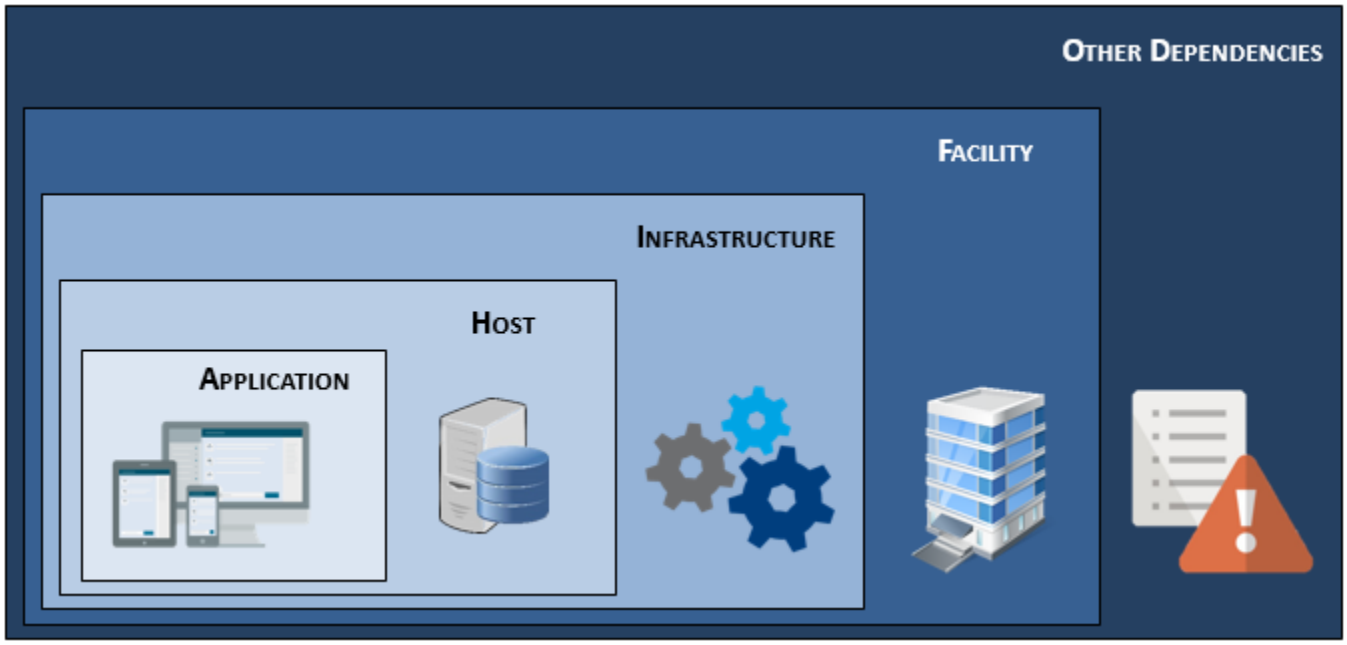


Figure 3: Layers of dependency-based vulnerabilities.

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)

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.

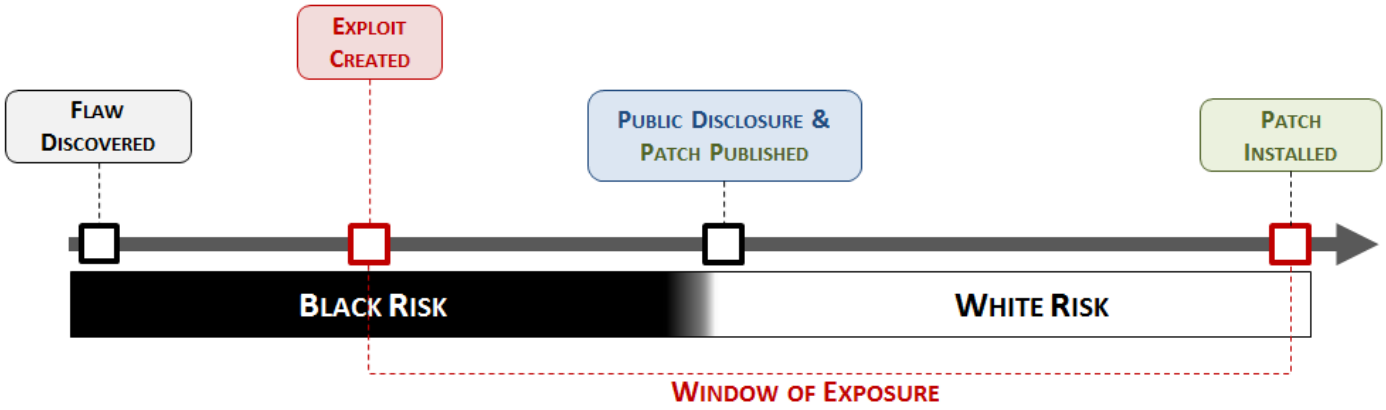


Figure 5: Zero-day patch – Black & White Risk.

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.

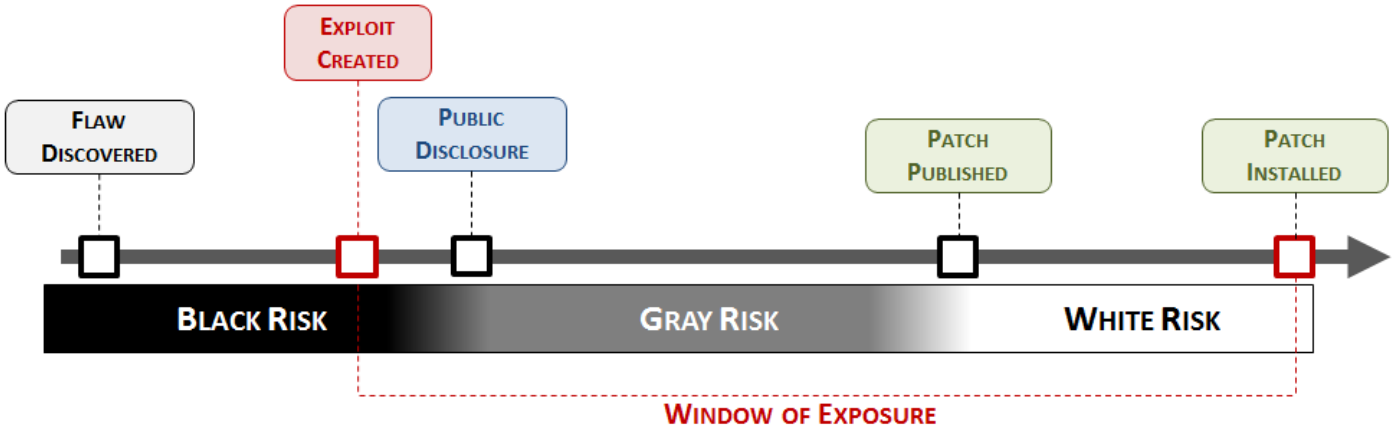


Figure 6: Zero-day exploit – Gray Risk.

When the concepts of zones, patch severity ratings and patch priorities is combined, the logical standard for patching the enterprise is established:

<table>
<tr><th rowspan="2">Zone</th><th rowspan="2">Patch Severity Rating</th><th colspan="3">Recommended Timeline To Commence Patching</th></tr>
<tr><th>Workstations</th><th>Servers</th><th>Other Equipment</th></tr>
<tr><td rowspan="4">1</td><td>Critical</td><td rowspan="4">N/A</td><td colspan="2">P1 < 48 Hours</td></tr>
<tr><td>Important</td><td colspan="2" rowspan="3">P3 < 30 days</td></tr>
<tr><td>Moderate</td></tr>
<tr><td>Low</td></tr>
<tr><td rowspan="4">2</td><td>Critical</td><td>P1 < 48 Hours</td><td rowspan="4">N/A</td><td>P2 < 72 Hours</td></tr>
<tr><td>Important</td><td>P2 < 72 Hours</td><td rowspan="3">P4 < 90 days</td></tr>
<tr><td>Moderate</td><td rowspan="2">P3 < 30 days</td></tr>
<tr><td>Low</td></tr>
<tr><td rowspan="4">3</td><td>Critical</td><td rowspan="4">N/A</td><td>P2 < 72 Hours</td><td>P3 < 30 days</td></tr>
<tr><td>Important</td><td rowspan="3">P3 < 30 days</td><td rowspan="3">P4 < 90 days</td></tr>
<tr><td>Moderate</td></tr>
<tr><td>Low</td></tr>
<tr><td rowspan="4">4</td><td>Critical</td><td colspan="3" rowspan="4">P3 < 30 days</td></tr>
<tr><td>Important</td></tr>
<tr><td>Moderate</td></tr>
<tr><td>Low</td></tr>
<tr><td rowspan="4">5</td><td>Critical</td><td rowspan="4">P5 - ASAP*</td><td rowspan="4">N/A</td><td rowspan="4">P5 - ASAP*</td></tr>
<tr><td>Important</td></tr>
<tr><td>Moderate</td></tr>
<tr><td>Low</td></tr>
</table>

Figure 10: Recommended patching timelines by zone.

Patching Strategy

The current ACME standard is that software patches will be installed within 30 days from the date of the vendor release. This includes operating systems, applications and firmware.

Server-Class Systems

Server-class systems include, but are not limited to:

- Microsoft Server 2000
- Microsoft Server 2003
- Microsoft Server 2008
- Microsoft Server 2012
- Redhat Enterprise Linux (RHEL)
- Unix
- Solaris

Workstation-Class Systems

Workstation-class systems include, but are not limited to:

- Microsoft XP
- Microsoft Vista
- Microsoft 7
- Microsoft 8
- Microsoft 10
- Apple
- Fedora (Linux)
- Ubuntu (Linux)
- SuSe (Linux)

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

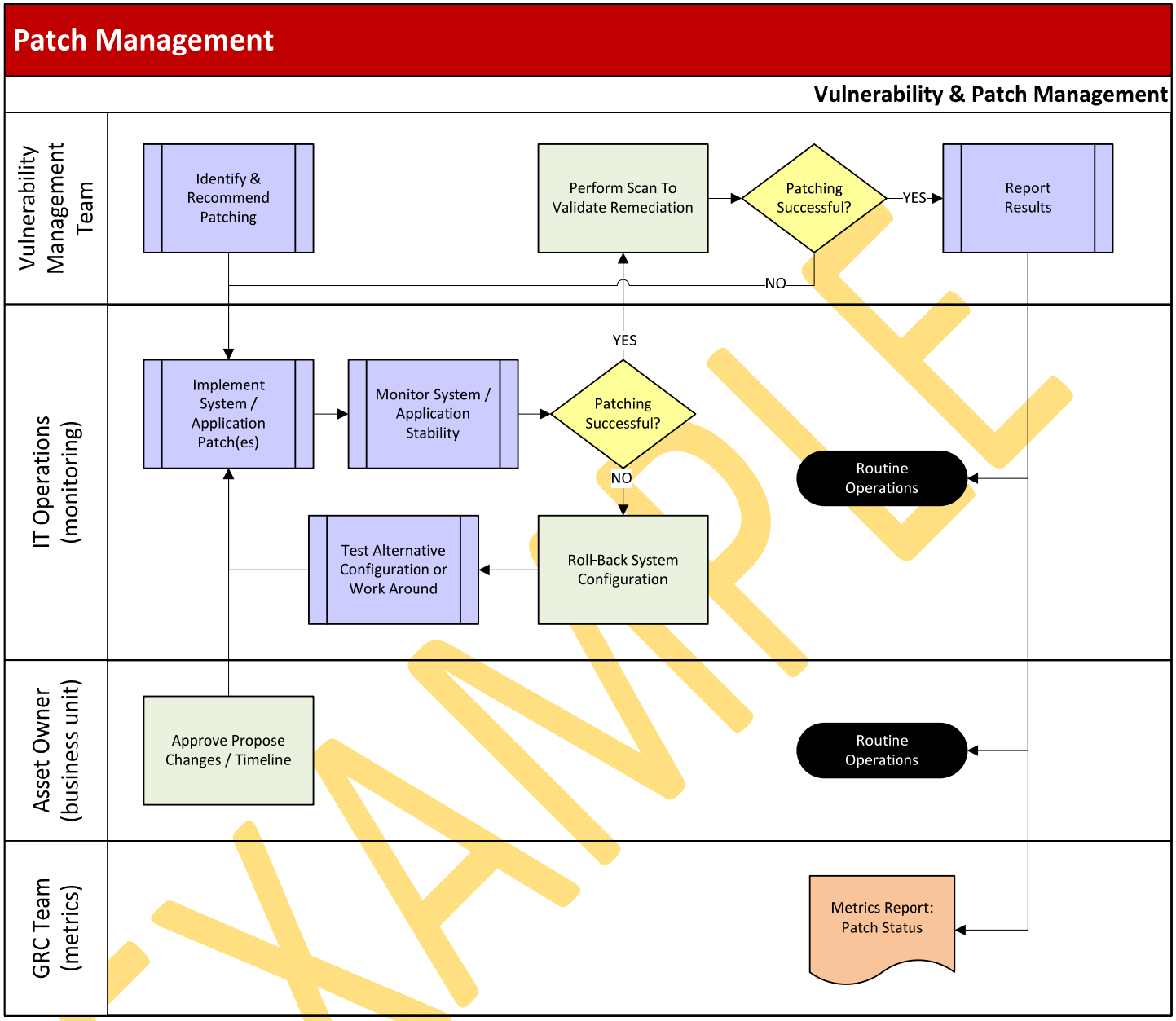


Figure 15 – Patching process flowchart.

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).