VULNERABILITY ~~& PATCH~~ MANAGEMENT PROGRAM (VMP)

City of Waukesha

INTERNAL USE
Access Limited to Internal Use Only

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Vulnerabilities pose a significant risk to the confidentiality, integrity, and availability to City resources, as well as those who access City 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 THE CITY OF WAUKESHA 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 the City of Waukesha. 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 City of Waukesha discover new security issues and verify that known issues are fixed in a timely manner.~~

TARGET AUDIENCE

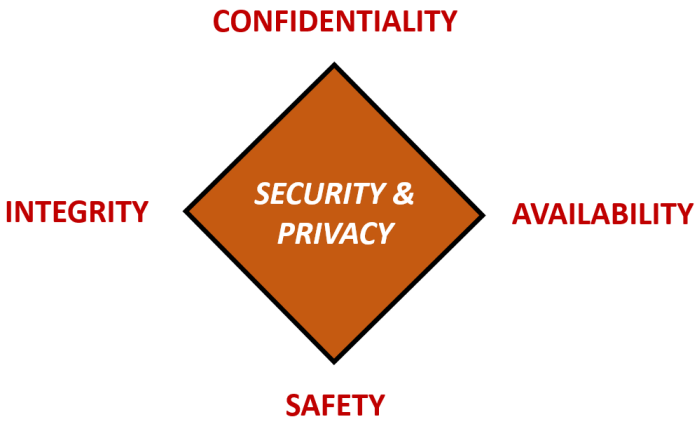
The target audience for this document includes both business process owners and IT personnel responsible for maintaining the networks, systems, databases, and applications that allow City of Waukesha to function.

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.

VULNERABILITY & PATCH MANAGEMENT PROGRAM OVERVIEW

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

City of Waukesha IT is committed to protecting employees, partners, clients and City of Waukesha from damaging acts that are intentional or unintentional. Protecting City 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 VMP 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 VMP. An effective VMP is a team effort involving the participation and support of every City of Waukesha user who interacts with data and systems. Therefore, it is the responsibility of every user to conduct their activities according to the VMP to reduce risk across the enterprise.

SCOPE

The scope of the VPMP encompasses all City of Waukesha networks, regardless of what entity "owns" or maintains the asset(s):

- City of Waukesha-controlled environments:
  - On-premises Data Centers
    - Production
    - Preproduction/Build
    - Development
    - Test
  - Revenue Streams
    - eCommerce
    - Point of Sale (POS) devices
  - Telecommunications
    - Voice over Internet Protocol (VoIP)
    - Instant Messaging (IM) solutions
    - 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 non-technical staff / end users;
  - 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 Programs (VMP) include the process of coordinating activities to prevent the exploitation of vulnerabilities. The alternative to vulnerability management is crisis management, so the preventative benefits of vulnerability management outweigh the reactive expenses, which include operational impacts, corrupted data, and negative client/public relations.~~

~~Like any organization, City of Waukesha 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 City of Waukesha can minimize VMP 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:

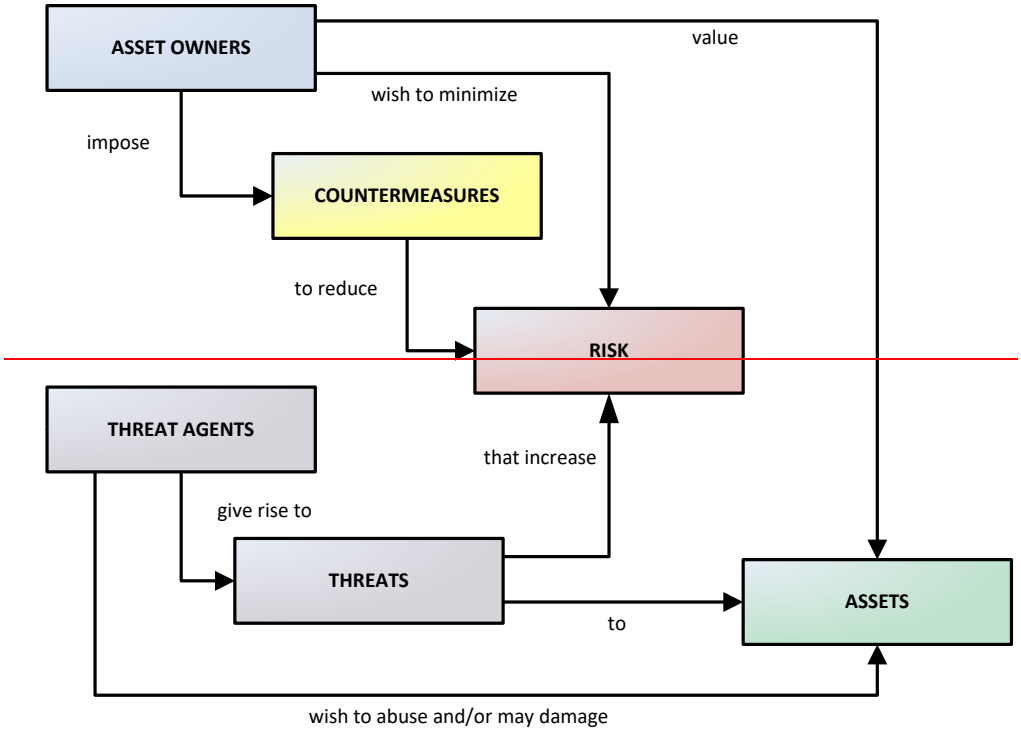


Figure 1: Understanding connected nature of managing risk - vulnerability management focuses on countermeasures.

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 VMP-related roles and responsibilities.

It is important to keep in mind that vulnerability management 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:

Department

- The department that requires the technology to be in place and function ultimately "owns" the risk associated with the ongoing operation of systems.
- Process Owners (POs) are individuals within Department 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.
- POs 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 departments 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 Department/Process Owner.

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.

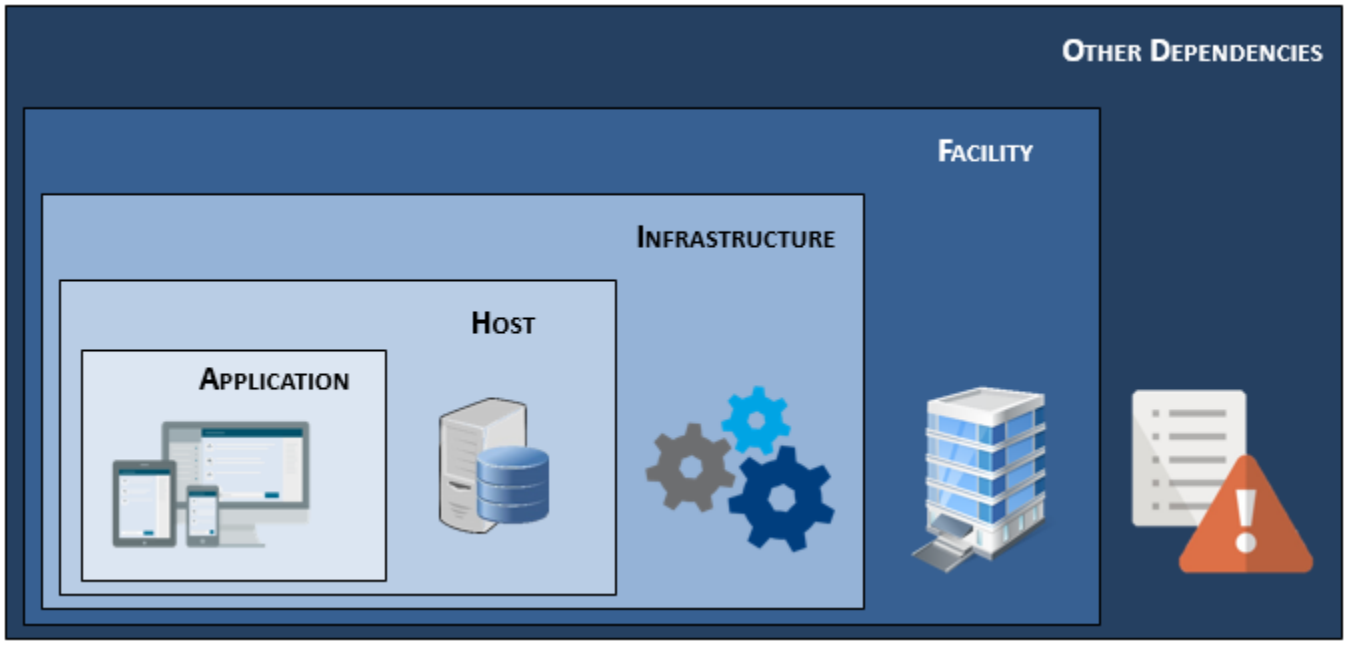


Figure 3: Layers of dependency-based vulnerabilities.

As part of overall vulnerability management, City of Waukesha will 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 will exist for:

- ~~Datacenters (including infrastructure risks)~~
- ~~Secure configurations for hosts (cloud & on-premises), and major applications (e.g., databases, email, Intranet),~~
- ~~Firewalls~~
- ~~Endpoints (including, but not limited to workstation and servers).~~

~~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~~

~~**Infrastructure**~~

~~Vulnerabilities associated with infrastructure include, but are not limited to:~~

- ~~Improper equipment (e.g., consumer-grade networking hardware vs. business/enterprise-grade)~~
- ~~Lack of system hardening~~
- ~~Default/weak credentials~~
- ~~Lack of encryption in transit~~
- ~~Lack of access control~~
- ~~Missing software patches~~
- ~~Logging/monitoring not being performed~~

~~**Facility**~~

~~Vulnerabilities associated with facilities include, but are not limited to:~~

- ~~Inadequate physical access controls~~
- ~~Inadequate environmental controls~~
- ~~Lack of redundant utilities~~
- ~~Poorly trained personnel (e.g., disaster recovery plan execution)~~

~~**Other Dependencies**~~

~~Vulnerabilities associated with other dependencies include, but are not limited to:~~

- ~~No software escrow agreements~~
- ~~Poor developer/vendor management~~
- ~~Undocumented/unauthorized international trans-border data transfers~~
- ~~Lack of stakeholder support~~

Risk Treatment Options For Vulnerability Management

Essentially, there are only four (4) options for managing risk, and it is management's responsibility to analyze available information and decide upon one of the following options:

- Reduce the risk to an acceptable level;
- Avoid the risk;

- Transfer the risk to another party; or
- Accept the risk.

Reduce Risk

When a risk is reduced, a strategy is implemented that is designed to remediate the risk to an acceptable level.

Risk reduction can be achieved through management controls or other arrangements which reduce the frequency of, or opportunity for, error – such as alternative procedures, quality assurance, testing, training, education, supervision, review, documented policy, and procedures.

Examples of reducing risk include, but are not limited to:

- *Apply compensating controls.*
- *Remediate vulnerabilities to correct identified deficiencies.*

Avoid Risk

When a risk is avoided, a decision is made not to proceed with the activity.

Wherever possible, risk avoidance measures should be designed to be embedded in normal business processes, activities, and systems. They should not impede the logical and natural flow of processes and should be easy to understand and appreciate.

Examples of avoiding risk include, but are not limited to:

- *Terminate the project.*
- *Select a different solution that does not have the same risk.*

Transfer Risk

When risk is transferred, a strategy is implemented that shares or transfers the risk away from City of Waukesha.

Risk can be transferred by shifting the responsibility for a risk to another party. Risks may be transferred in full, or they may be shared with another party. Risks should be allocated to the party that can exercise the most effective control over those risks.

Examples of transferring risk include, but are not limited to:

- *Purchase additional cybersecurity insurance.*
- *Select a vendor that will accept indemnification for the risk associated with providing the service (e.g., PCI DSS payment processing).*
- *Move to a hosted solution.*

Accept Risk

While accepting risk is an option for management, the decision needs to be reasonably justified and documented.

Examples of reducing risk include, but are not limited to:

- *Continue with the project, being fully aware of the risks.*
- *Choosing not to remediate vulnerabilities, based on untenable remediation costs.*

Accepting and retaining the risk is the least desirable option for City of Waukesha. However, after careful analysis of the cost of risk treatments, management may determine that risk cannot be avoided, reduced or transferred, or where the cost to do so is not justified (usually, because the likelihood and consequences are low). These retained risks should be monitored, and it must always be remembered that all unidentified risks are retained risks.

Vulnerability Management Fundamentals

Managers need to identify their role in contributing to City of Waukesha'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

City of Waukesha 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. City of Waukesha also recognizes that no one technique can provide a complete picture of City of Waukesha'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 City of Waukesha'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 City of Waukesha uses.

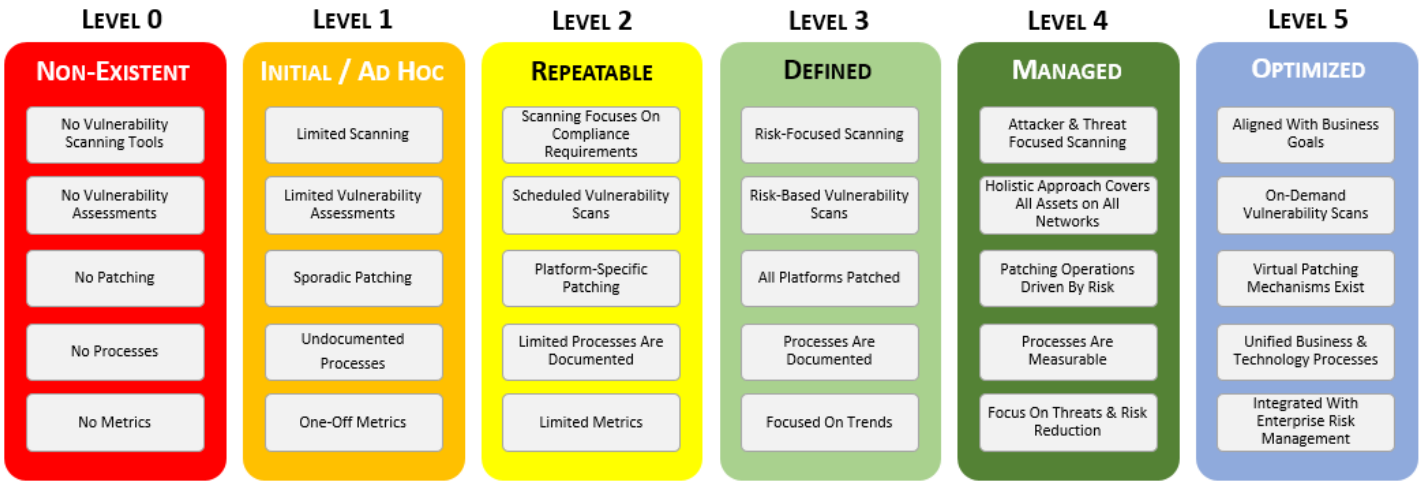


Figure 4 – Vulnerability Management Capability Maturity Model.

Target Vulnerability Management Level

As part of City of Waukesha's multi-year strategy to reduce vulnerabilities, the target is to achieve a blend of Level 4 (Managed) and level 5 (Optimized) on the VM-CMM end of year 2021.

[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 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.

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 City of Waukesha 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.

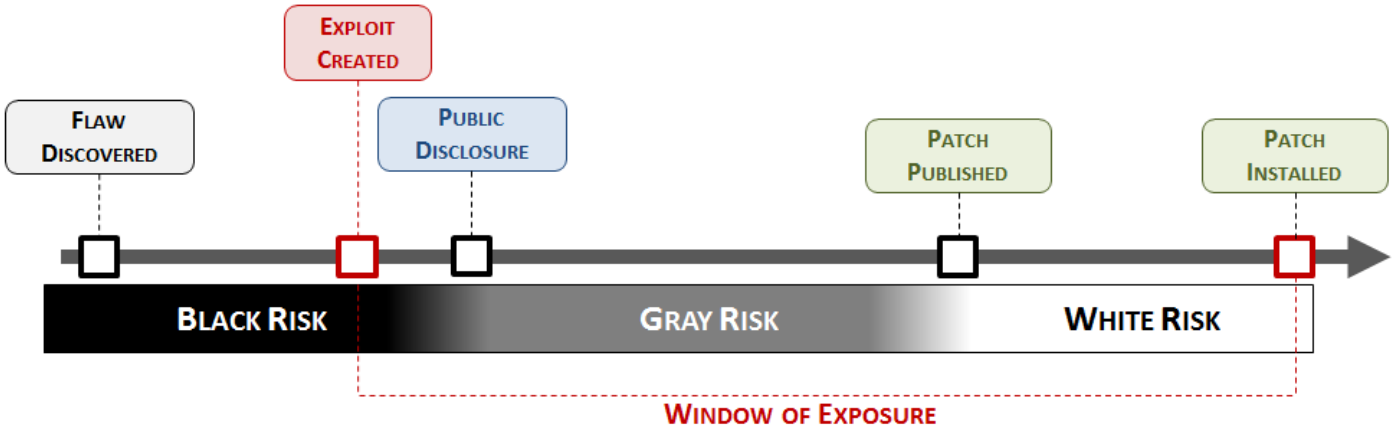


Figure 5: Zero-day exploit – Gray Risk.

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 6: 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.

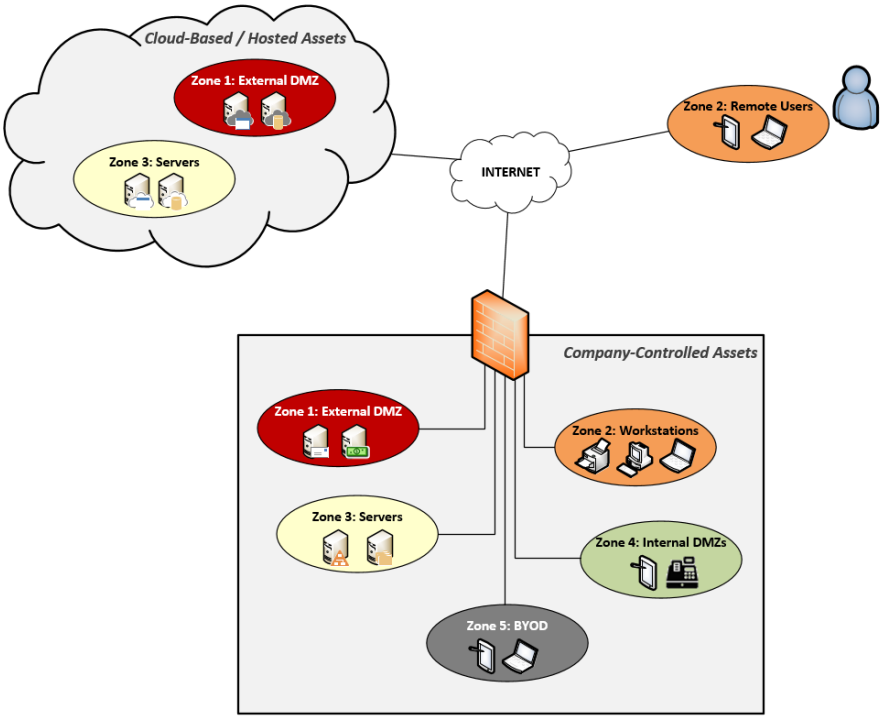


Figure 7: Zone-based patching model.

Zone	Definition of Patching Zones
1	Systems that are exposed to the Internet: - Assets in an external-facing Demilitarized Zone (DMZs) - Servers with a direct connection to the Internet
2	Network segments that are dedicated to workstations and end-user equipment: - Internal workstations - Mobile / remote users - End-user equipment (e.g., desktop printers, scanners, etc.)
3	Network segments that are dedicated to internal servers and infrastructure equipment: - Servers - Networking equipment (e.g. networked printers, switches, internal servers) - Networked printers/scanners

4	Internal DMZs are segmented for statutory, regulatory or special business requirements: - Highly sensitive data (e.g., CUI, Cardholder Data, sensitive PII, etc.) - HVAC / facility control systems - Test / development / staging environments
5	Encompasses all Bring Your Own Devices (BYOD) categories of equipment: - User-owned laptops - User-owned smartphones

Figure 8: Zone-based patching model zones.

Recommended Timelines for Patching

Remediation is prioritized on systems that are directly exposed to the Internet and are susceptible to published vulnerabilities.

City of Waukesha utilizes five (5) categories of prioritization for patch management. These timelines dictate when patching operations need to be initiated:

- **P1** – Patching must commence within 48 hours of vendor release.
- **P2** – Patching must commence within 72 hours of vendor release.
- **P3** – Patching must commence within 30 days of vendor release.
- **P4** – Patching must commence within 90 days of vendor release.
- **P5** – Patching is based on end user requirements for managing BYOD devices. Ideally, users should patch their personally-owned systems As Soon As Possible (ASAP).

No City of Waukesha asset should have a patch missing longer than ninety (90) days.

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 9: Recommended patching timelines by zone.

Patching Strategy

The current City of Waukesha 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. The exception is when the patch is not security related, or imposes more risk than not patching.

Server-Class Systems

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

- Microsoft Server 2012
- Microsoft Server 2016
- Microsoft Server 2019

Workstation-Class Systems

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

- Microsoft 10
- Windows 11

Network Devices

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

- Firewalls
- Switches & Routers
- Load balancers
- Wireless Access Points (WAPs)
- Printers & Multi-Function Devices (MFDs)
- HVAC

~~Mobile Devices~~

~~Mobile-class systems include, but are not limited to:~~

- ~~Tablets~~
- ~~Mobile phones~~
- ~~Other portable electronic devices~~

~~Databases~~

~~Database-class systems include, but are not limited to:~~

- ~~Windows SQL Server (City Standard)~~

~~Minor Applications~~

~~Minor Application-class applications include, but are not limited to:~~

- ~~Microsoft Office~~
- ~~Java~~
- ~~Adobe~~
- ~~Edge (Internet browser)~~
- ~~Chrome (Internet browser)~~
- ~~Firefox (Internet browser)~~

~~Major Applications~~

~~Major Application-class applications include, but are not limited to:~~

- ~~Pro Phoenix~~
- ~~Munis~~
- ~~Kronos~~
- ~~Vision~~
- ~~TRAKiT~~
- ~~Active Directory~~
- ~~DNS~~

~~Vulnerability Management Governance~~

~~Key Activities~~

~~Vulnerability management is comprised of the following key activities:~~

- ~~Manage the asset inventory;~~
- ~~Categorize assets;~~
- ~~Identify vulnerabilities;~~
- ~~Assess risks; and~~
- ~~Remediate flaws.~~

~~Manage The Asset Inventory~~

~~Without a current and accurate asset inventory, it is ad-hoc and problematic to properly address applicable vulnerabilities, since a comprehensive understanding of the environment is not known. Only through proactive management of asset inventories will VM personnel know what is applicable and how exposed those assets are to exploitation.~~

~~*Inventories are more useful when categorized into meaningful classes of systems as listed above.*~~

~~Categorize Assets~~

~~Asset categories or zones should be created from asset inventories (see Figure 9), but the categorization should also address criticality and exposure. These categories allow for vulnerability scan customization, addressing asset or business requirements, and assist with assigning risk rankings.~~

~~Identify Vulnerabilities~~

~~There are internal and external components to identifying vulnerabilities. This includes, but is not limited to:~~

- ~~Vulnerability assessments;~~
- ~~Penetration testing;~~
- ~~Threat feeds from Special Interest Groups (SIGs);~~

- Internal phishing attacks;
- Risk assessments; and
- Cyber Incident Response Team (CIRT) incidents.

Assess Risks

Vulnerabilities are assigned a business criticality rating based on City of Waukesha's Risk Management Program (RMP). When a vulnerability is discovered, the vulnerability needs a risk rating assigned to it, and remediation efforts are subsequently prioritized on a risk basis.

Based on the degree of exposure, these risk categories help enable City of Waukesha's leadership to make informed decisions at the appropriate level of management oversight.

Low Risk

Insignificant damage could occur from a low risk:

- The financial impact is negligible.
- The impact would not be damaging to City of Waukesha's reputation or impede business operations.
- There are no violations of contractual, statutory or regulatory requirements.

Medium Risk

Minimal damage could occur from a medium risk:

- The impact would not be damaging to City of Waukesha's reputation or impede business operations.
- The impact could impede core or supporting business systems or business operations.
- This may involve a violation of contractual requirements.
- There are no violations of statutory or regulatory requirements.

High Risk

Moderate damage could occur from a high risk:

- The impact could include damage to City of Waukesha's reputation.
- The impact could impede Business Essential (CL2) systems or business operations.
- This may involve a violation of contractual, statutory and/or regulatory requirements.

Severe Risk

Significant financial and brand damage could occur from a severe risk.

- The impact could include significant damage to City of Waukesha's reputation.
- The impact could impede Mission Critical (CL1), and below, systems or business operations.
- The impact could negatively affect City of Waukesha's short-term competitive position.
- This may involve a violation of contractual, statutory and/or regulatory requirements.

Extreme Risk

Extensive financial and long-term brand damage could occur from a critical risk:

- The impact could include extensive damage to City of Waukesha's reputation.
- The impact could impede Mission Critical (CL1) systems or business operations.
- The impact could negatively affect City of Waukesha's long-term competitive position.
- Risk scenarios involving potential physical harm or fatality are included in this category.

Remediate Flaws

Flaw remediation management is the process of identifying, acquiring, installing, and verifying patches for flaws in systems and applications. Patches correct security and functionality problems in software and firmware. From a security perspective, applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.

Patches serve other purposes than just fixing software flaws; they can also add new features to software and firmware, including security capabilities. There are several challenges that complicate patch management.

One issue that is particularly important for mobile devices is the acquisition of updates over low-bandwidth or metered connections; it may be technically or financially infeasible to download large patches over such connections. City of Waukesha should make provisions for ensuring that its enterprise patching solution works for mobile hosts and other hosts used on low-bandwidth or metered networks.

Patches should be tested in a non-production environment to determine if there are system compatibility issues. Patches that do not have negative impacts on functionality or security can then be installed in production environments.

Automation of patch deployment helps ensure timely remediation. However, patches may be applied through the following methods:

- Software defined automatic update; and
- User involvement (manual patch install or patch approval).

Vendor-Maintained Systems

Vendor-maintained servers and web applications hosted on City of Waukesha's network, as well assets hosted on vendor networks, are subject to the same requirements as City of Waukesha-maintained assets.

The department / Process Owner that contracted the vendor's services is responsible for vendor oversight to ensure the vendor is properly performing vulnerability management activities. The vendor must be made aware of City of Waukesha's remediation schedule and remediate vulnerabilities accordingly.

If the vendor is not able to follow this schedule, the department must provide an exception justification, signed by an appropriate level of management within the Department, to City of Waukesha's cybersecurity department for a risk assessment.

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 City of Waukesha'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 City of Waukesha'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 "false positive" 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
0	Threat is a false positive and is not applicable to the environment.
1	Threat is limited to information gathering. Exposure to 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 10: 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 City of Waukesha'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.

System & Application Patching

Vulnerability management includes patch management as a core component. Key concepts to be aware of include:

- 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.

Information Security Considerations for Patching Systems

Managing vulnerabilities in operating systems and applications rely, in great part, on to the software vendor. Since all vendors differ in their approach to publishing software patches or when software fixes are not currently available, there are situations where alternate remediation steps may be required to minimize the risk associated with the organization. The goal is to minimize the window of exposure in managing software patching operations.

Tool Selection

City of Waukesha recognizes that Patch Manager Plus is the authoritative tool for conducting system patching operations on servers and workstations.

Patch Management Lifecycle

Regardless of the type of patch to be installed, the patch management process consists of four (4) distinct steps that must be followed:

- Assess;
- Identify;
- Evaluate & Plan; and
- Deploy.

Figure 11: Lifecycle for Patch Management

Assess

Processes:

- Create and maintain a baseline of systems;
- Assess patch management architecture;
- Review infrastructure / configuration;
- Discover assets; and
- Inventory clients.

Questions to Answer:

- Are there any threats or vulnerabilities in the environment?
- Has anything changed in production?
    - New operating systems and applications;
    - Changes to network or management infrastructure;
    - Accurate and up-to-date inventory information is essential to the process; and/or
    - Is the management infrastructure able to support patch management?

Identify

Processes:

- Identify new patches;
- Determine patch relevance (including threat assessment); and
- Verify path authenticity & integrity.

Questions to Answer:

- Is the patch relevant to the organization?
- Which systems need to be patched?
- Do all systems need to be patched with the same level of priority?
- Which systems are most vulnerable?
- Has the patch been downloaded and checked to be virus free?
- Does the patch install successfully on a trial system?
- Has a Request For Change (RFC) been submitted for this patch?

Evaluate & Plan

Processes:

- Test the patch, if possible;
- Perform a risk assessment for possible repercussions from patching or not patching;
- Obtain approval from the Change Advisory Board (CAB) to deploy the patch; and
- Plan the patch release process and notify affected parties.

Questions to Answer:

- Can the patch be combined with other changes to minimize downtime?
- Do business-critical functions still work after the patch is installed?
- How and when is best to install the patch?
- What are considerations for mobile clients and connections across slow or unreliable networks?

Deploy

Processes:

- Distribute and install the patch(es);
- Report on progress to the CAB;
- Handle exceptions with a coordinated mitigation plan; and
- Review deployment for future process improvement.

Questions to Answer:

- Does the production environment need to be prepared for new patches?
- Are users fully informed of possible downtime or issues?
- Have "lessons learned" from previous deployments been successfully implemented?

Patching Process Overview

Below depicts the basic decision process in determining the process to patch assets.

- Documented roles and responsibilities need to be assigned to vulnerability management personnel to monitor for new vulnerabilities.
- When a vulnerability is identified, the vulnerability management team, in conjunction with the asset owner and IT staff, should determine if it affects any assets.
    - Factors that are considered in the analysis include the key elements of the vulnerability footprint measured against the potential impact on the business operations.
    - If the risk is high, then an immediate patch may be required.
    - Alternatively, if there are strong business constraints or operational concerns related to implementing the patch at a specific time, then it may be necessary to hold off on patching the system until the scheduled maintenance window.
- If a patch does not exist, then a workaround should be analyzed to determine if compensating controls should be implemented.

Once the patch has been implemented all applicable documentation and patch records should be updated.

Patch Review Process

A patch must be reviewed by all applicable stakeholders (e.g., IT, cybersecurity, process engineering, operations, and the asset owner) to determine if there is an immediate need to patch the asset (e.g., "out of band" patching) or if the patch should follow the standard patching cycle.

Below are a few considerations to address when making the final patch decision:

- Can the patch be deployed at a later date within a routine maintenance window?
- Is there a workaround that would provide adequate protection without patching?
- Does the exploit allow an intruder access to other restricted systems?
- What is the impact if the entire system had to be reloaded using disaster recovery backup procedures?
- Does the affected system have to remain in continuous operation?

The Change Advisory Board (CAB) will provide the authorization and timeline for implementing patches.

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 City of Waukesha 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 City of Waukesha's computing environment where there is no definitive timeline for remediating vulnerabilities by a statutory or regulatory requirement, the City of Waukesha 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.

The schedule for patching server operating systems can be found on the this SharePoint site: Windows Updates (sharepoint.com)

For patching workstation operating systems, ManageEngine Patch Manager Plus is set to automatically deploy Microsoft's biannual feature updates, along with any patches that may be released throughout the year. Additionally, limited 3rd party apps are patched as recommended by the manufacture or ManageEngine Patch Manager Plus.

Remediation Operations & Enforcement Exceptions

If an exception is requested, the asset owner must provide the cybersecurity team with a risk exception form with:

- All appropriate vulnerabilities listed;
- Justification and mitigation steps; and
- Exceptions signed by the appropriate level of management from the Department.

Vulnerability Scanning

Vulnerability Scanning Overview

Vulnerability scanning is an important part of any Defense-in-Depth (DiD) strategy since it provides situational awareness of both technical flaws and strengths.

By reviewing vulnerability scan reports, it is straightforward to uncover if maintenance activities are being performed. By scanning regularly, the overall security posture of City of Waukesha can be measured through metrics reporting.

Issues identified through both internal and external vulnerability scanning should be captured in City of Waukesha's risk register. False positives need to be documented.

External Scanning

To fully understand City of Waukesha's exposure, external vulnerability scans must be performed on an ongoing / recurring basis, so that new vulnerabilities can be identified and assessed for risk to City of Waukesha.

- External vulnerability scanning should use unauthenticated scan profiles.

Internal Scanning

Internal vulnerability scanning is equally important to City of Waukesha, since advanced malware is capable of bypassing perimeter defenses (e.g., phishing attacks) and can attack internal systems.

- Internal vulnerability scanning should use authenticated scan profiles.

Through assessing the state of the internal network(s) through authenticated internal scanning, City of Waukesha can identify areas of weakness with patching, configuration management and users' adherence to policy, in terms of the use of unauthorized software.

Recurring Validation

Rescanning is required to validate that deficiencies were corrected. The "trust but verify" approach is important, since it is possible that patches intended for a production system could be applied to a test/development/staging environment, and the intended target systems were not remediated.

Regular scanning ensures new vulnerabilities are detected in a timely manner and allows them to be patched faster. Having this process in place significantly reduces the risks of an organization.

Vulnerabilities not detected by a scan may leave systems vulnerable for a long period of time, depending on the frequency of scans. When implementing a vulnerability scanning schedule, regular scans must be scheduled to reduce possible exposure time.

Tool Selection

City of Waukesha recognizes that Tenable is the authoritative tool for conducting vulnerability assessment operations. However, other tools such as CIS Benchmarks, SSL Labs, and SSLYZE are used as well.

City of Waukesha's vulnerability management team is solely responsible for approving and overseeing the use of any enterprise scanning and assessment tools. The use of any other vulnerability scanner is prohibited without prior, written approval by the vulnerability management team.

Scan Preparation

The scan preparation phase is primarily the responsibility of the vulnerability management team. This generally involves the following steps:

- Define the scope for scans;
- Obtain an agreement on which systems will be included or excluded from vulnerability scans; and
- Determine the characteristics of the scans in distinct scan profiles (tool dependent).

Associated Risks

There is risk involved with vulnerability management, or more specifically, vulnerability scanning. Since vulnerability scanning typically involves sending a large number of packets to systems, it sometimes triggers unusual effects, such as disrupting network equipment. In order to prepare for these risks, it's always important to inform various stakeholders of City of Waukesha when new assets are added to scanning or when scan profiles change.

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

Scanning Operations

Once the scan preparation phase is complete, the next phase of the process begins, and the initial vulnerability scans are performed.

Discovery Scanning

Discovery scans are limited to scanning systems and web applications residing on the City of Waukesha network. A discovery scan is non-intrusive and intended to identify servers, workstations, or web applications, which may be unaccounted for from regularly scheduled vulnerability scans. Discovery scans should be conducted every 30 days.

Scan Frequency

The following timeline exists for scanning City of Waukesha assets, based on the zone (see Figure 9) the asset is deployed in:

Zone	Minimum Recommended Scanning Frequency	
	Discovery Scans	Vulnerability Assessment Scans
1	Weekly to Monthly (depends on environment)	Weekly
2	Monthly	Monthly
3	Weekly to Monthly (depends on environment)	Weekly
4	Weekly to Monthly (depends on environment)	Weekly
5	N/A - No permissions to scan BYOD assets.	

Figure 12 – Vulnerability scanning frequency. See list of Zones here.

Note - New vulnerability scans should be launched following the announcement of potentially damaging vulnerabilities, regardless of what the minimum recommended frequencies dictate.

External Scanning

External vulnerability assessment scans need to:

- Cover the entire scope of assets that reside in Zone 1 deployments.

- Utilize unauthenticated scanning profiles.

Internal Scanning

Internal vulnerability assessment scans need to:

- Cover the entire scope of assets that reside in Zones 2-4 deployments.
- Utilize authenticated scanning profiles, wherever possible.

Remediation Actions

Asset owners, in conjunction with asset custodians and security personnel, will define remediating actions. This follows a similar methodology as patching remediation. The planned remediating actions should be executed in line with the agreed timeframes. If a problem occurs with implemented remediation, it should be documented accordingly.

Validation Phase

Once a vulnerability is remediated, a rescan must be scheduled to verify the remediating actions have been implemented. This scan will be performed using the same vulnerability scanning tools and configuration settings as the initial scan.

This step is very important to prevent inaccurate results due to configuration errors when applying remediation actions. If the vulnerability still exists, the asset custodians must be made aware and tracked until remediation is complete and validated.

Penetration Testing

The purpose of penetration testing is to identify specific vulnerabilities that lead to a compromise of the business or mission objectives of the stakeholder:

- It is not about finding unpatched systems.
- It is about identifying the risk that will adversely impact City of Waukesha in the event of a data breach.

City of Waukesha recognizes the Penetration Testing Execution Standard (PTES)[3] as the reference framework for conducting penetration testing, which The PTES consists of seven (7) main sections and can map directly to the four (4) main sections of the NIST 800-115 *Guide to Security Testing and Assessment*

For compliance-related activities (e.g., Payment Card Industry Data Security Standard (PCI DSS)), penetration tests are typically performed as either white-box or grey-box assessments.

Information Assurance (IA)

Security Testing & Evaluation (ST&E)

Security Testing & Evaluation (ST&E) is a component of Information Assurance (IA) operations and is a holistic approach to assessing the management, operational, and technical safeguards used to protect the confidentiality, integrity, and availability of systems and data.

The City IT Department uses NIST Special Publication 800-115 – *Technical Guide to Information Security Testing and Assessment*[4] as the definitive guide to performing security testing and technical assessments. This guide is used for:

- Pre-production testing: and
- Post-change testing for significant changes.

Security Control Assessment (SCA) Methodology

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.

[3] The Penetration Testing Execution Standard (PTES) - http://www.pentest-standard.org
[4] NIST 800-115 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NIST's Risk Management Framework (RMF) is specified in NIST Special Publication 800-37 - *Guide for Applying the Risk Management Framework to Federal Information Systems.*[5] This framework is a tactical approach that City of Waukesha will utilize for specific projects.

NIST 800-37 RISK MANAGEMENT FRAMEWORK – SECURITY LIFE CYCLE

At a project level, 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.

Figure 13: NIST 800-37 Risk Management Framework (RMF) security lifecycle.

CATEGORIZE

City of Waukesha shall assign a potential security impact value for all information systems, including the information being processed, stored, and transmitted by the system, based on the potential impact to City of Waukesha

SELECT

An appropriate set of security controls is selected for the information system after categorizing and determining the minimum security requirements.

City of Waukesha will 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 City of Waukesha'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.

[5] NIST 800-37 - http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

~~***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***~~

~~Information systems are authorized based on a determination of the risk to operations, assets, or to individuals resulting from the operation of the information system and the determination that this risk is acceptable.~~

~~***MONITOR***~~

~~Assess selected security controls in the information system on a continuous basis (e.g., metrics reporting, annual control testing, etc.).~~

APPENDICES

APPENDIX A – VPMP ROLES & RESPONSIBILITIES

CHIEF RISK OFFICER (CRO) – THE TECHNICAL OPERATIONS MANAGER PERFORMS THE ROLE OF THE CRO

The Chief Risk Officer (CRO) is accountable to City of Waukesha's executive management for the development and implementation of the risk management program.

The CRO's responsibilities include, but are not limited to:

- Protecting City of Waukesha from unacceptable risk or losses associated with operations; and
- Developing and implementing mechanisms for effectively managing the risks that may affect the achievement of City of Waukesha objectives and operational outcomes.

CHIEF INFORMATION SECURITY OFFICER (CISO) – THE IT DIRECTOR PERFORMS THE ROLE OF THE CISO

The CISO is accountable to City of Waukesha's executive management for the development and implementation of the cybersecurity program. The CISO will be the central point of contact for setting the day-to-day direction of the cybersecurity program and its overall goals, objectives, responsibilities, and priorities

The CISO's responsibilities include, but are not limited to:

- Oversee and approve the company's cybersecurity program, including the employees, contractors, and vendors who safeguard the company's 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 cybersecurity policies, standards, and guidance that establish a framework for an Information Security 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 systems; and
- Monitor, evaluate, and report to company management on the status of cybersecurity within the organization.

EXECUTIVE AND SENIOR MANAGEMENT

The effectiveness of risk management is unavoidably linked to management competence, commitment, and integrity, all of which forms the basis of sound corporate governance. Corporate governance provides a systematic framework within which the executive management group can discharge their duties in managing City of Waukesha.

Executive and Senior Management responsibilities include, but are not limited to:

- Considering and documenting new and existing risks and their impact on proposed plans as part of the annual planning cycle.
  - Risk records must be maintained up-to-date on an on-going basis to reflect any changes which may occur;
- Providing direction and guidance within their areas of accountability so that staff best utilize their abilities in the preservation of City of Waukesha's resources;
- Successfully promoting, sponsoring and coordinating the development of a risk management culture throughout City of Waukesha;
- Guiding the inclusion of risk management in all strategic and operational decision making;
- Possessing a clear profile of major risks within their area of control, incorporating both opportunity and negative risks;
- Maintaining a framework to manage, monitor and report risk;
- Managing risks to meet City of Waukesha objectives, goals, and vision; and
- Improving corporate governance.

MANAGEMENT

Managers at all levels are responsible for the adoption of risk management practices and are directly responsible for the results of risk management activities, relevant to their area of responsibility.

ALL EMPLOYEES

All employees are responsible for:

- Acting at all times in a manner which does not place at risk the health and safety of themselves or any other person in the workplace;
- Identifying areas where risk management practices should be adopted and advising their supervisors accordingly;

- Meeting their obligations under relevant statutory, regulatory and contractual requirements; and
- Taking all practical steps to minimize City of Waukesha's exposure to contractual, tortuous and professional liability.

Asset Owner

The asset owner "owns" the process, application, service or asset in question.

Risk/asset owner responsibilities include, but are not limited to:

- Ensuring that the risks they are assigned are managed appropriately;
  - Management of individual risks may be delegated to a person with relevant expertise to undertake the task of managing the risk on behalf of the risk owner.
  - The risk owner retains ultimate responsibility
- Monitoring progress against treatment plans;
- Ensuring that the risk review process is carried out in a timely fashion, within their areas of responsibility; and
- Ensuring the currency of the risk register and responding to any risk register actions that have been assigned to them.

Internal Audit

The internal audit function supports City of Waukesha risk management by providing advice and support on risk management, and through an annual independent review of risk management practices and procedures to provide assurance on their efficiency and relevance to the Audit Committee.

Vulnerability Management Personnel

The internal vulnerability management function supports City of Waukesha vulnerability management by implementing and executing the controls associated with a Vulnerability & Patch Management Program (VPMP).

Vulnerability management responsibilities include, but are not limited to:

- Conducting vulnerability assessment scans;
- Conducting penetration tests;
- Maintaining vulnerability management tools;
- Generating metrics to report on the status of vulnerability management and remediation operations; and
- Consulting with asset owners and custodians on remediation activities.

Asset Custodians

Asset custodians maintain assets for asset owners.

Asset custodian responsibilities include, but are not limited to:

- Implementing assets according to secure configuration standards;
- Performing proactive, recurring maintenance activities;
- Maintaining situational awareness on evolving threats; and
- Collaborating with asset owners and vulnerability management personnel for remediation actions.