Baldwin Wallace University Information Technology Standard

Issued by:	**Information Technology**
Title:	**Patch and Vulnerability Management**
Number:	**ITS-BW-22-01**
Publish date:	**June 1, 2022**

A. Vulnerability Management Life Cycle

This document defines the required components of a vulnerability management process to remediate, mitigate, or accept the risks associated with vulnerabilities in an effective, systematic, timely, and repeatable way. This process consists of three steps, as shown below:

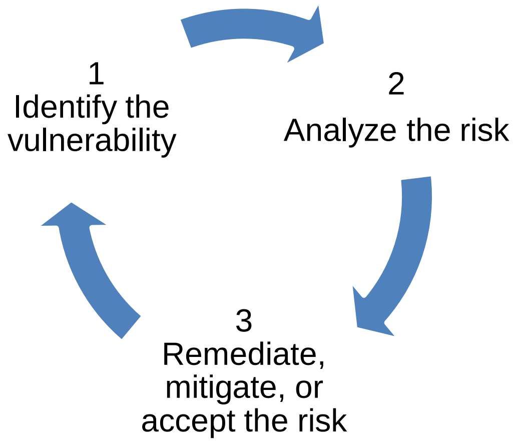
1
Identify the vulnerability
2
Analyze the risk
3
Remediate, mitigate, or accept the risk

Figure 1: Vulnerability Management Life Cycle

Step 1. Identify the vulnerability:

The goal of this step is to identify vulnerabilities associated with an IT resource. Identification of vulnerabilities may occur in multiple ways based upon the type of resource including, but not limited to:

- Commercial vulnerability scanning products.
- Subscriptions to vendor notification/alert and maintenance services.
- Vendor notification on the end of life or end of support.
- Penetration tests.
- Anti-malware (virus) subscription services.

University Standard for Vulnerability Identification:

Commercial Vulnerability Scanners:

The University's standard for Servers, Network Operating Systems, and Client Operating Systems is Nessus.

Step 2. Analyze the Risk:

Vulnerabilities identified in Step 1 must be assessed based on the probability of successful exploitation AND the potential damage/harm that could result. The University has adopted a five-point scale for assigning a criticality rating to identified vulnerabilities, which was issued as part of the Payment Card Industry Data Security Standards and has been adopted by many commercial risk vendors.

Rating	Key Aspect/Definition
Urgent (5)	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. Vulnerabilities at this level may include: full read and write access to files, remote execution of commands, and the presence of backdoors.
Critical (4)	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. Vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
Serious (3)	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. Vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, denial of service attacks, disclosure of filtering rules and security mechanisms, and unauthorized use of services, such as mail-relaying.
Medium (2)	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
Minimal (1)	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Step 3. Remediate, mitigate, or accept the risk:

The objective of remediation is to **eliminate**, **mitigate**, **transfer,** or **accept** the risks presented by an identified vulnerability. Common techniques include, but are not limited to, the following examples:

- Disabling unnecessary software capabilities/services.
- Maintaining proper configuration settings.
- Applying relevant software/firmware patches released by the vendor in a timely fashion.
- Employ up-to-date anti-malware products on susceptible systems.
- Maintain the software systems at the vendor “supported” release levels (maintenance).
- Network isolation (use of firewall technology to control/minimize access over the network).
- Risk acceptance: used when the cost of elimination/remediation is more than the value of the resource and/or its business benefit.

  NOTE: Risk acceptance for threats rated 5 requires:
    - Formal documentation of the vulnerability and resulting risk.
    - Approval by the Business Owner and IT Director.
    - Retention of the acceptance document by the IT Director until the vulnerability has been eliminated, or the IT resource is retired.

B. Value-Based Risk Assessment

The level of effort and resulting cost of performing appropriate vulnerability management processes must be balanced with the “value” of the services/information the IT resource(s) provides to the University. Value or business impact is based upon the potential cost to the business if the services/information provided by the resource is unavailable or compromised, such as defined in the BW DR plan. The greater the value of the services provided, the more stringent the process concerning frequency and completeness.

Asset categories will be assigned default risk classifications, per the table below. Individual assets, however, may be classified differently than the default based on the value it delivers and the impact of it having an issue.

Asset Category	Default Risk Classification
Desktops and Laptops	Orange
Servers	Orange
Firewalls, Routers, and other Network Equipment	Red
Devices never attached to the Network	Green
Printers and other peripherals	Yellow

The Business Owner for each IT resource is responsible for determining the appropriate classification. ITP-BW-04 Data Classification Policy can also guide the Business Owner in determining the value of the system by the label assigned to the information the system houses.

Classification Category		Key Aspects based upon value to the University in any of the dimensions of Confidentiality, Integrity, or Availability
🟥	**RED** System Label: “Critical” Information Label: “Restricted”	The most valuable information or IT resources. Requires a high level of assurance that vulnerabilities rated 3, 4, or 5 are identified and addressed per the time schedule documented in Section C.1. Examples include: • IT resources hosted in any DMZ are subject to a significant risk of attack. • Active Directory (AD) domain controllers. • Domain Name Service (DNS) servers. • Firewalls and Core Routers. • IT resources requiring a high level of security. • Systems that are holding level 3 data as defined in ITP-BW-04 Data Classification Policy.
🟧	**ORANGE** System Label: “Essential” Information Label: “Confidential”	Valuable information or IT resources. Requires assurance that vulnerabilities rated 4 or 5 are identified and addressed per the time schedule documented in Section C.2. Examples include: • IT resources deemed essential to meeting the University’s business, operational, or reporting goals.
🟨	**YELLOW** System Label: “Default” Information Label: “Internal”	Information and IT resources that have not been formally classified into another category. It does not require vulnerabilities to be addressed per a schedule but requires routine patching is as documented in Section C.3. Examples include: • IT resources deemed significant to meeting the University’s business, operational or reporting goals. • Desktop/laptop systems.
🟩	**GREEN** System Label: “Low Value” Information Label: “Public”	It does not require assurance that vulnerabilities are identified and addressed. IT resources classified as “green” will be rare. Examples include: • IT resources that are “stand-alone” and have NO connection to internal University networks.

C. Vulnerability Management Standards

The following sections define the standards that are to be applied to the vulnerability management lifecycle for IT resources based upon the “Classification Category” assigned by the Business and Technical Owners of the resource:

C.1 resources Classified as Critical (RED)

Step 1: Identification

- The resource is to be scanned for vulnerabilities weekly and immediately upon completion of a Change Control.
- Vendor services should be subscribed to in order to identify relevant patches and/or security alerts within 30 days of their release.

Step 2: Analysis

- Vulnerabilities (identified by any method) are to be evaluated weekly.

- Each shall be ranked by criticality using the 5-point scale defined in Section A.2.

Step 3: Remediation

- All vulnerabilities rated 3, 4, or 5 shall be mitigated within 30 days of discovery
- Implement using the Change Management procedure.
- The Business Owner of the IT resource may override the remediation time so long as they have defined and documented.
- All vulnerabilities rated 1 or 2 may be handled at the discretion of IT.

C.2 resources Classified as Essential (ORANGE)

Step 1: Identification

- the resource is to be scanned for vulnerabilities weekly and immediately upon completion of a Change Control.
- Vendor services should be subscribed to in order to identify relevant patches and/or security alerts within 30 days of their release.

Step 2: Analysis

- Vulnerabilities (identified by any of method) are to be evaluated at least monthly.
- Each shall be ranked by criticality using the 5-point scale defined in Section A.2.

Step 3: Remediation

- All vulnerabilities rated 4 or 5 shall be mitigated within 60 days of discovery.
- Implement using Change and Release Management procedures.
- The Business Owner of the IT resource may override the remediation time so long as they have been defined and documented.
- All vulnerabilities rated 1, 2, or 3 may be handled at the discretion of IT.

C.3 resources Classified as Significant (YELLOW)

Step 1: Identification

- the resource is to be scanned for vulnerabilities at least quarterly.
- Vendor services should be subscribed to in order to identify relevant patches and/or security alerts within 60 days of their release.

Step 2: Analysis

- Vulnerabilities do not need to be evaluated.

Step 3: Remediation

- Vendor-issued patches shall be applied at least semi-annually unless the Business Owner of the IT resource has defined a different timeline to be used, and it is documented.
- Implement using Change and Release Management procedures.

C.4 resources Classified as Needed (GREEN)

There are no vulnerability management standards for this class of resource.

D. Summary Matrix

The standards above are presented here in tabular form to aid in understanding.

System Category (information Classification)	Critical (Restricted)	Essential (Confidential)	Default (Internal)	Low (Public)
Tasks:	Red	Orange	Yellow	Green
Scan for vulnerabilities	Weekly	Weekly	Quarterly	no req.
Evaluate vulnerabilities	Weekly	Monthly	Patch Semi-Annually	no req.
Mitigate level 4 & 5 vulnerabilities	30 days	60 Days		no req.
Mitigate level 3 vulnerabilities	30 days	no req.		no req.
Mitigate level 1 & 2 vulnerabilities	no req.	no req.		no req.