Technical Vulnerability Management Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	28/09/2017
V 0.2	Mick Jenkins	Formatting	03/10/2017
V 0.3	Andrew Clarke	Comments from Head of Development and Application Services re: consistency, change management and reference to SaaS and PaaS/Cloud	19/10/2017
V1.0	Andrew Clarke	Approved ISC	26/01/2018
V 1.1	Andrew Clarke	Addition of College IT and Network & Infrastructure Manager responsibilities. Remediation change from detected to reported detection (i.e. monthly)	07/09/2018
V 1.2	Andrew Clarke	Amend Severity CVSS scoring to align with current good practice (2.4) Add New system, service or network vulnerability management (2.1.1) Added Vulnerability Tools (2.9) Added Appendix A – Responsibilities matrix / Process Flow	01/04/2019
V 1.3	Andrew Clarke	2.1.1Secure by Design mandate 2.8 Exceptions management reporting	22/05/2019
V 1.4	Andrew Clarke	2.8 Exceptions management comments from Dev & Apps Addition of Reference BUL-PR-14.09 - Secure By Design Principles Exception protocols (AMP + segmentation)	03/06/2019
V 1.4	Andrew Clarke	Annual Review	17/08/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 26 Jan 2018
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 26 Jan 2018
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1.	About this document	4
1.1	Purpose	4
1.2	Responsibilities	4
1.3	ISO27001 Conformance	4
1.4	Scope	5
1.5	Policy Overview	5
1.6	Policy Maintenance	5
1.7	References	5
2.0	Vulnerability Management Policy	7
2.1	Vulnerability Testing	7
2.2	Penetration Testing	7
2.3	Vulnerability Monitoring	7
2.4	Vulnerability Management	8
2.5	Vulnerability Mitigation	9
2.6	Vulnerability Reporting	10
2.7	Remediation Management	10
2.8	Exceptions Management	12
2.9	Vulnerability Management Tools	13
4.0	APPENDIX A - Vulnerability Management process	15

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London (BUL) covering Technical Vulnerability Management and Penetration Testing controls.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Chief Information Security Officer	Is responsible for managing, coordinating, and scheduling Penetration Testing of the University networks - and reporting technical vulnerability management status and remediation to executive board.
Head of Infrastructure and Operations	Is responsible for overall technical vulnerability Management on all systems managed by IS.
Head of Development and Application Services	Is responsible for monitoring vendors' sites, bulletins, and notifications for releases of upgrades and new releases on server application software and all Corporate systems. Is responsible for installing server application software updates and testing software items updates and new implementations.
Systems Manager	Is responsible for monitoring vulnerabilities and vendors sites, bulletins, and notifications for releases of patches and fixes for vulnerabilities on the operational systems. Is responsible for testing software items updates and new implementations. Is responsible for the Operations and Production environments, known as 'Ops' & 'Prod' along with Development and test environments.
Network and Infrastructure Manager	Is responsible for monitoring vulnerabilities and vendors sites, bulletins, and notifications for releases of patches and fixes for vulnerabilities on the network systems. Is responsible for testing software items updates and new implementations.
Cyber & Information Security Manager	Is responsible for monitoring and aggregation of vulnerability risk assessment of University networks. And the collations of metrics to evidence and support technical vulnerability management.
College IT	Are responsible for monitoring vendors' sites, bulletins, and notifications for releases of patches, upgrades, new releases and fixes for vulnerabilities on the respective College systems not manged by IS. Are responsible for installing OS and application

	software updates and testing software items updates and new implementations not managed by IS.
IT System owners (business units)	Are responsible for monitoring vendors' sites, bulletins, and notifications for releases of upgrades and new releases on systems software. Are responsible for installing server application software updates and testing software items updates and new implementations.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.6 Technical Vulnerability Management

1.4 Scope

The scope of this policy applies to:

- Any server or client that IS manages or is responsible for, including servers which are managed by third parties on behalf of IS.
- Any server or client that College IT manages or are responsible for, including servers which are managed by third parties on behalf of Colleges.
- Any software on these servers or clients. In this document, "software" shall be taken to include firmware, BIOS, hypervisor, operating system, driver, library, middleware, application, service, and other digital capabilities.
- All public-facing Cloud systems and services that the University subscribes to including PaaS, SaaS, and IaaS.

1.5 Policy Overview

This document details the vulnerability management policies and controls required to maintain high levels of system and application security in a diverse IT environment. It outlines the technology and procedures necessary for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain maximum levels of security.

The development, implementation and execution of the vulnerability assessment policy is the responsibility of the Cyber & Information Security Operations area under the authority of the Chief Information Security Officer (CISO). Periodic or continuous vulnerability assessment

scans will be performed on all network assets deployed on Brunel University London IP address space.

A centrally managed aggregated vulnerability assessment system will be deployed. Use of any other network based tools to scan or verify vulnerabilities must be approved, in writing, by the CISO.

1.6 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

1.7 References

BUL Change Control Policy (ISMS 12.1.2)
BUL-POL-12.6 - Patch Management
BUL-PROC-12.6 - Vulnerability Management Exceptions Process
BUL-PR-14.09 - Secure By Design Principles

2.0 Vulnerability Management

Vulnerability testing and penetration testing is required for all systems (both University managed servers and clients) which should be subject to continuous monitoring for vulnerabilities and threats using automated and manual methods.

2.1 Vulnerability Testing

The Cyber & Information Security team will ensure that vulnerability testing on all public-facing systems, University Critical systems and systems hosting University Confidential data will be conducted on a regularly scheduled basis.
Internal Vulnerability Testing (scans) of systems must be conducted on a regularly scheduled basis

Failed vulnerability scans must be addressed and followed by a retest, repeating these steps until the vulnerability testing completes successfully

Upon identification of new vulnerability issues, perimeter defence comprising Firewall, Cisco Umbrella and other appropriate tools must be updated accordingly.

2.1.1 New or replacement Service, Server, System or Network

Any new or replacement service, server, system or network architectural change must include a vulnerability test before being introduced to the live or production environment.

Ref BUL-PR-14.09 - Secure By Design Principles

Secure by Design - Any new or replacement service, server, system or network with High or Medium (CVSS scores of >4.9) vulnerabilities identified in the vulnerability scan must be remediated or mitigated prior to acceptance in production or live environments.
If these cannot be “closed”, then the BUL-PROC-12.6 - Vulnerability Management Exceptions Process must be adhered to.

In addition, upon any major configuration change to the system, an internal scan must be performed.

If no vulnerability test is conducted, acceptance in to the Live or Production environment will not be accepted.

2.2 Penetration Testing

External and internal penetration testing shall be performed at least once a year on all systems.

External and internal penetration testing shall be performed after any significant infrastructure or application changes
Penetration testing shall minimally consist of network-layer and application-layer penetration tests.

2.3 Vulnerability Monitoring

The systems, development and network Administrators must maintain secure system/application configurations by routinely reviewing vendor sites, bulletins, and for releases of patches and fixes for vulnerabilities on the operational systems and implementing vulnerability mitigation strategies in accordance with the University vulnerability management program.

Service Owners shall regularly monitor the security status of their servers and/or software, including patch status, and shall use this information, along with information on mitigations in place, to update their Service Information Risk Registers. Information from internal scanning, manufacturers/suppliers and/or trusted source(s) shall be used to identify vulnerabilities.

All devices are scanned on a consistent scan schedule and also on a by-request or as-needed basis. The defined scan frequency makes provisions for an assessment at least once per month for servers and sensitive hosts, and once per quarter using a rolling scan for all other devices on the network.

- All server and sensitive host scans should be scheduled across all TCP/IP subnet address ranges. This accommodates critical patches released by vendors such as Microsoft.
- All desktop and other scans across all TCP/IP subnet address ranges.
- Inventory scans to identify any new assets run monthly on all subnets (excluding BYOD) – identified assets must then be included in subsequent host vulnerability scans.
- All new assets to be included as production for desktops or servers must be assessed and documented with no critical or high vulnerabilities.
- All scans should be allocated at 12 hours to complete.
- Ad hoc/individual system scans may be requested and performed at any time.
- All software images (operating systems) on the network devices (routers, switches, VPN, firewalls, wireless, and DNS/DHCP) are to be reviewed monthly.

2.4 Vulnerability Management

Any detected vulnerabilities must be remediated in accordance with the specific timeframes described below.

For purposes of remediation and mitigation, the severity rating assigned by CVSS will serve as the basis for classifying a vulnerability unless specifically indicated as an exception. The following classifications describe the severity levels that can be assigned to a vulnerability.

- **Critical** denotes a vulnerability through which an intruder can easily gain control at the administrator level of any affected host. This class of vulnerabilities poses the highest risk for a system-wide compromise of the University network. Critical vulnerabilities have a CVSS score of 10.0. They can be readily compromised with publicly available malware or exploits.

- **High** denotes a vulnerability through which an intruder could gain access to the host at the administrator level or could possibly access University Confidential Information stored on the host. While this class of vulnerabilities is extremely serious, the risk of a breach or compromise is not as urgent as with a critical vulnerability. High-severity vulnerabilities have a CVSS score of 7.0 to 9.9. There is no known public malware or exploit available.

- **Medium** denotes a vulnerability that may allow an intruder to gain access to specific information stored on the host, including security settings. While not immediately associated with a compromise of an affected host, these vulnerabilities allow intruders to gain access to information that may be used to compromise the host in the future. Medium-severity vulnerabilities have a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.

- **Low** denotes vulnerabilities that do not pose an immediate threat to the host or the University network. These vulnerabilities refer mostly to weaknesses in a device that allow an intruder access to information that may be used in the future to compromise the host. These vulnerabilities may often be mitigated through firewall and intrusion prevention systems that limit access by intruders from outside the University network. IS and Colleges may opt to mitigate these vulnerabilities based on their network architecture or set up a timeframe for remediation based on the information stored on the device. Low-severity vulnerabilities are defined with a CVSS score of 3.9 or less.

Information denotes advisory details. Information vulnerabilities have a CVSS score lower than 4.0. These are considered risks but are generally reference information for the state and configuration of an asset.

Any findings that need to be mitigated later than the service level must be approved by the management and documented as exceptions. These are to be reviewed and approved by the Chief Information Officer and the Chief Information Security Officer.

Any identified vulnerabilities, either related to missing patches or improper configuration, must be remediated within the timeframes specified below based on the degree of associated severity. For vulnerability remediation, System Administrators should perform appropriate testing and follow existing change-management procedures to ensure proper patch installation for affected systems.

Vulnerability Level	After reported detection (***monthly***), remediation required within less than	Exception Approval
critical	1 week	CISO / CIO
high	30 days	CISO / CIO
medium	90 days	Department Business Manager
low	At the discretion of the department	Department IT Manager

2.5 Vulnerability Mitigation

The preferred approach to remediate a vulnerability is by the Secure by Design principle 6 to minimise the attack surface area. (Ref Principle 6 - BUL-PR-14.09 - Secure By Design Principles), wherever possible, by removing the vulnerable software (such as an OS service or optional software component) - i.e. its absence has no business impact, since this will eliminate the existing risk and additionally ensures new issues with that software cannot create risk.

If minimising the surface area approach is not possible, a software update should be preferred if

(a) the alternative would be to inhibit functionality that would cause business impact, and
(b) the risk of the software update itself causing business impact is outweighed by the risk created by the presence of the vulnerability

Any security patches that cannot be applied within period dictated by the vulnerability level (i.e. 7 days, 30 days or 90 days) of release must be escalated to the Chief Information Security Officer with an explanation about why the patch cannot be applied and a recommended course of action.

Where patching is not possible or not feasible, a risk-based approach (using the University Information Risk Assessment processes) shall be used to identify the suitable alternative approach to manage a vulnerability. This may include physical or logical separation from network connectivity if no other option is available.

Vulnerabilities which cannot be mitigated to an acceptable level of risk shall be promptly escalated to the relevant Information Owner, and to the CISO as required, with proposed options for resolution or follow the exceptions management (2.8).

2.6 Vulnerability Reporting

A flexible reporting schedule that works in tandem with system administration patching cycles will be implemented to manage resources and potential outages. A report will always be generated as proof that an assessment occurred.
Below is a listing of key reports that will be automatically generated and delivered to implement this process:

Status Reports	Frequency	Purpose
Threat Analyser	Monthly	Report provides all technical vulnerability updates by configuration & patching
Executive Dashboard	Quarterly	Provides executive team members with a status dashboard of vulnerability management.
Regulatory	Six monthly	To support audits and evidence pf technical vulnerability management to support regulations such as GDPR. Also includes evidence to support cyber essentials and ISO 27001.
Exceptions	Monthly	Provides all team members a listing of exceptions and expiration dates for findings throughout the environment.

Actionable Reports	Frequency	Purpose

Vulnerability	Monthly	Remediation plans for system owners
Patch Report	Monthly	For systems to undertake regular patching activity.

These reports will be generated with an allowance for change control windows and system change control freezes (e.g. holiday season).

2.7 Remediation Management

Vulnerability reports provide system owners and administrators the opportunity to understand the potential risk to which their systems may be exposed, and to take proactive steps to address the identified vulnerabilities.

Between each official reporting period, the security team, system administrators, vendors, or other sources may identify vulnerabilities. The initiation of this process begins with the dissemination of actionable system reports as generated by the monthly scan cycle or by custom reporting - based on requests or new asset deployments. Unplanned reports and alerts are made for issues regarding industry-wide or zero-day vulnerabilities and are treated by risk.

For example, out-of-cycle critical vulnerabilities should be reported immediately with a custom assessment and remediated within the guidelines of this document.

The table below outlines the general responsibilities by role:

Cyber & Information Security Team	
The Cyber & Information Security Team maintains the vulnerability management solution, generates reports, and monitors the vulnerability posture of the University. The team ensures that systems are scanned for vulnerabilities on a regularly scheduled basis and that identified vulnerabilities are brought to the attention of the appropriate personnel.	• Disseminate vulnerability reports • Manage reports and vulnerability database • Issue resolution recommendations and guidance • Track the vulnerability resolution progress • Report unmitigated vulnerabilities of significance to executives • Respond to requests for vulnerability reviews
System Owner	
System owners work with the system administrators to authorise, prioritise, and schedule changes to their systems, or implement acceptable mitigating controls to reduce the risk to an acceptable level. Corrective actions such as patches are considered normal business maintenance. However, if other mitigating controls are used, teams should review and approve the	• Review vulnerability reports • Assess the degree of risk that the vulnerabilities represent • Review and approve proposed corrective actions or mitigating controls • Schedule changes with the users and the system administrators

controls as appropriate to address the vulnerability. It is ultimately the system owner's responsibility to accept any unmitigated risk that remains	• Formally accept unmitigated risk
System Administrator	
System administrators implement the corrective actions authorised by the system owners. They are technical resources that may research and propose various resolutions and mitigating controls	• Review vulnerability reports • Assess the risk of vulnerabilities to the system • Propose corrective actions or mitigating controls to the system owner(s) • Request vulnerability exceptions where appropriate • Implement changes authorised by the system owner(s)

The Chief Information Security Officer has the authority to take action, with appropriate communication with system owners in advance, to ensure that un-remediated systems do not pose a threat to University information resources. Risk reduction actions, beyond the norm, and requiring critical action (such as blocking systems from the campus data network) shall require the joint approval of the CISO and CIO (or in their absence, CISO/CIO delegates).

In support of this policy, the CISO shall publish needed controls, standards, and procedures. Such standards shall include processes for determining remediation exceptions for systems and types of systems based on (at least): compensating controls, prohibitive technical and operational obstacles, or other system-specific circumstances.

2.8 Exceptions Management (ref BUL-POL-12.6 - Vulnerability Management Exceptions Process)

Vulnerabilities may exist in operating systems, applications, web applications, or in the way different components interoperate together. While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that are not patched, services may be exposed for proper application operations, and systems may still be live that are considered end-of-life by the developer and manufacturer.

In these cases, additional protections may be required to mitigate the vulnerability and these would be considered normal vulnerability management.

A suitable mitigation shall be applied within the identified vulnerability level or a dispensation be formally approved in writing by the CIO and CISO. Where the risk is deemed to be very high (e.g. where attacks on the University are known to be plausibly imminent or taking place) then the vulnerability must be addressed swiftly.

In rare cases, the vulnerability scanner may falsely identify a vulnerability that can't be correct by the scan vendor. These shortcomings do not accurately reflect the risk of the system and require an exception process.

Exceptions may be made so that the vulnerabilities are not identified as items of risk to the system and University.

This elaborates itself in the form of multiple exception types:

- False Positives arise when the scan has identified a host as being vulnerable when, in fact, it is not. This can occur because some vulnerabilities are inferred from advertised or identified version numbers; it may be possible to more accurately identify the vulnerability, but only disruptively (such as sending a particular request to a server application to see if it crashes, thereby confirming a DoS vulnerability) and may have been remediated by other means, such as backported fixes, that do not affect the version number; – this allows for remediation by configuration change in addition to backporting. It uses the accepted software development term, “backport”. It removes the incorrect implication that backporting is done by an application; it is done by a person (often acting on behalf of some organisation). Backporting is a standard practice in the maintenance of GNU/Linux distributions with long support cycles (such as RHEL). These findings have subsequently been reported back to the scan vendor and no improvements can be performed to the automated check
- Acceptable Risk vulnerabilities are those where the vulnerability is real, but compensating controls are in place to mitigate the risk; Ref Principle 2 Defense in Depth - BUL-PR-14.09 - Secure By Design Principles
- Critical, the service or business impact of applying the remediation or mitigation has been deemed too critical for intervention at this time
- Delayed Action are real vulnerabilities that cannot be remediated or mitigated in the time frame specified due to business impact (downtime to apply remediation) or because of testing that is required to ensure operations are not affected by the recommended remediation.

Delayed Action exceptions require a plan to test the recommended remediation and a date that corrections can be implemented by without impacting the business.

Any exception must be identified along with the Length of time (one, three, six, or 12 months) for which the exception is requested. During the exception period, mitigating protocols must be implemented comprising Advanced Malware Protection (AMP) on the server(s) and/or service along with segmentation and/or quarantine of the server(s) and/or service based on trust.

Exploitable vulnerabilities noted during penetration testing shall be corrected and an adequate retest performed to demonstrate that identified exploit is addressed.

The Cyber & Information Security team will collate and distribute the recorded exceptions within the vulnerability scanning tool and a spreadsheet of all exception requests and the outcome from the Vulnerability Exceptions Quorum.

2.9 Vulnerability Management Tools

Vulnerability management is a continuous process of discovering, prioritising and mitigating vulnerabilities in an IT environment.

The tools that the University uses for vulnerability management must include the following:

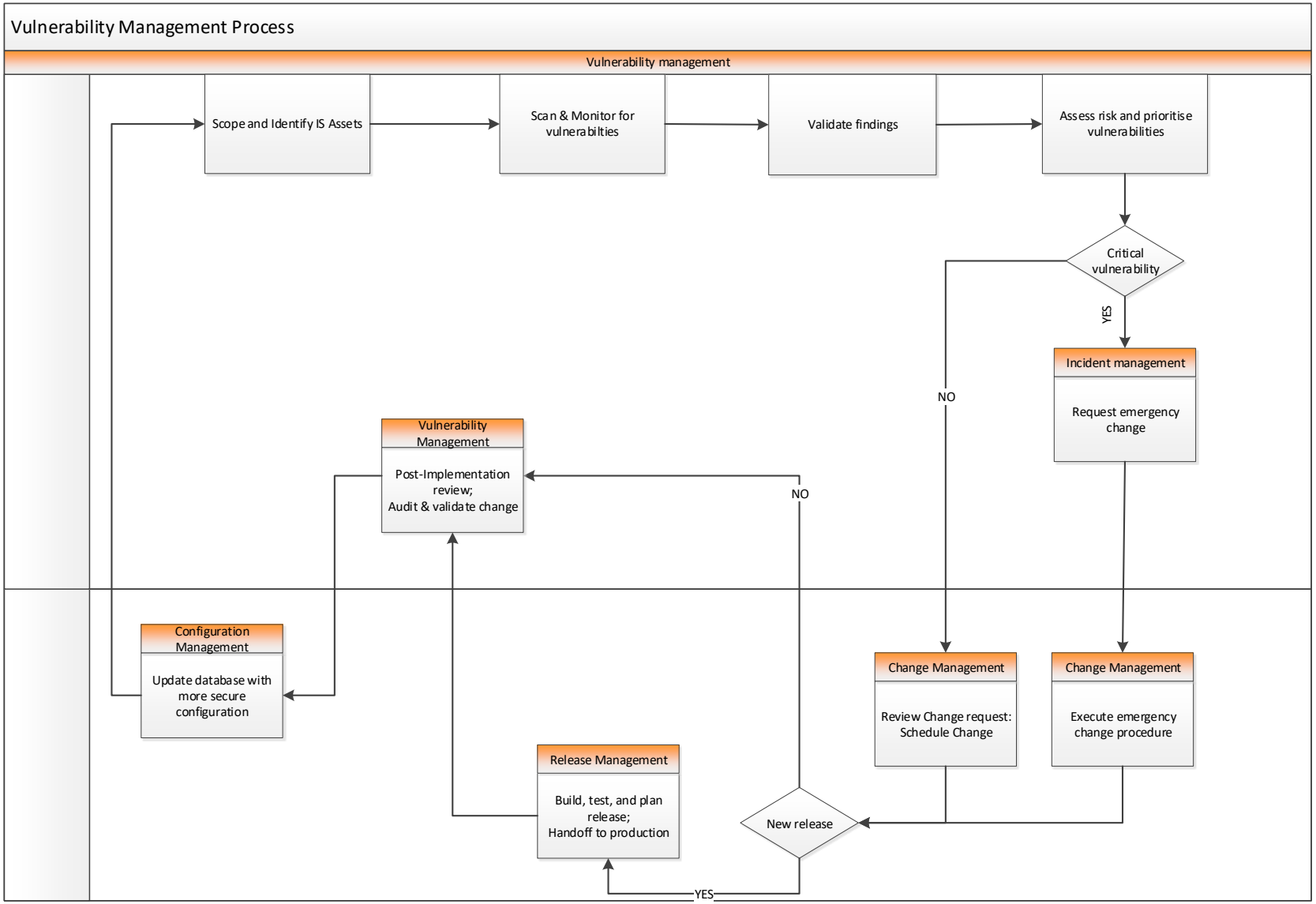
- Discovery: The process of identifying and categorising every asset in a networked environment and storing attributes in a database. This phase also includes discovering vulnerabilities associated with those assets.
- Prioritisation: The process of ranking known asset vulnerabilities and risk. Vulnerabilities must be assigned a severity level based upon the CVSS (Common Vulnerability Scoring System) ranking 10 - 01, which can then translate to High – Low respectively.
- Remediation/Mitigation: The system must provide links to information about each vulnerability discovered, which includes recommendations for remediation and vendor patches, where applicable. These links must include third-party resources such as The MITRE Corporation's Common Vulnerabilities and Exposures database, the CVSS and/or the SANS/FBI Top 20.

Vulnerability management tools come in three primary forms: stand-alone software, a physical appliance with vulnerability management software or a cloud-hosted service and provide preconfigured scans, along with the capability to modify those templates to save customised scans that run on demand or on a scheduled basis.

The University has evaluated a number of vulnerability management tools and has adopted two tools that provide the listed capabilities and forms.

Greenbone Security Manager (GSM) 400

NCSC (National Cyber Security Centre) - WebCheck (identify and fix common web security issues)


Vulnerability Management Process
Vulnerability management
Scope and Identify IS Assets
Scan & Monitor for vulnerabilties
Validate findings
Assess risk and prioritise vulnerabilities
Critical vulnerability
YES
NO
Incident management
Request emergency change
Vulnerability Management
Post-Implementation review;
Audit & validate change
NO
Configuration Management
Update database with more secure configuration
Change Management
Review Change request: Schedule Change
Change Management
Execute emergency change procedure
Release Management
Build, test, and plan release;
Handoff to production
New release
YES