Technical Vulnerability Management Exception Process

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	22/05/2019
V 0.2	Andrew Clarke	Approved PWG	10/06/2019
V 1.0	Andrew Clarke	Approved CISO	18/06/2019
V 1.0	Andrew Clarke	Annual Review	30/07/2020

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: 18 Jun 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 18 Jun 2019
Distribution:	

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

Contents

1. About this document

1.1 Purpose of Document

Brunel University is committed to safeguarding its information and computing infrastructure upon which the teaching and research functions rely. Additionally, the University is strongly committed to maintaining the security and privacy of confidential personal information and other data it collects or stores.

In order to guide the University community in achieving these objectives, the University has established Technical Vulnerability Management standards, procedures, and policies that all users are required to follow. However, the University also recognises that there may be urgent business needs or academic pursuits that require deviations from the Technical Vulnerability Management standards, procedures, and policies. Therefore, the University has developed this exceptions process that users may utilise to justify such deviations.

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 and reporting technical vulnerability management status and remediation to executive board. Responsible for decision making on exception acceptance based upon Quorum advice.
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 overall technical vulnerability Management on all server application software and all Corporate systems managed by IS.
Systems Manager (Quorum member)	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 (Quorum member)	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.
Software development Manager (Quorum member)	Is responsible for monitoring vendors' sites, bulletins, and notifications for releases of upgrades and new releases on systems software. Is 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 Process 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 Process 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.

1.6 References

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

2.0 Vulnerability Management Exceptions

2.1 Exceptions Management (extract from BUL-POL-12.6 - Vulnerability Management 2.8)

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.

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.

2.2 Vulnerability Exceptions Quorum comprises:

- Cyber & Information Security manager (or delegate)
- Cyber & Forensics Analyst
- Software Development manager (or delegate)
- Corporate Systems Manager (or delegate)

- Systems Manager (or delegate)
- Network & Infrastructure Manager (or delegate)
- Client Computing Infrastructure Manager (or delegate)

2.3 Exceptions Process

Any staff who wishes to be granted an exception from the Vulnerability Management Policy must provide the following information relevant to the request:

- Date
- Requestor's name, email address and department
- Name of Vulnerability
- Risk classification (High, Medium, Low)
- The classification of data sensitivity (e.g. University Confidential data)
- Length of time (one, three, six, or 12 months) for which the exception is requested
- Exception Type (2.1)
- Explanation as to why this exception is being requested
- List of the systems, networks, and/or data for which the exception will apply. The list must include the fully qualified name of any servers (e.g. abc.brunel.ac.uk)
- Details regarding any mitigating factors and compensating controls that will be used to offset the risk during the length of the exception
- Proposed remediation or mitigation plan to close risk
- Urgency of Service

For example, the risk associated with storing University Confidential information on an individual use device is considered a Medium impact (risk), however, if the probability (likelihood) of the risk being exploited, as mitigating actions are not sufficient, is Probable, then the overall risk rating is Medium (see below).

Service Impact

Probability	Extreme Complete loss of service	High Severe loss of operating capability, where at least 50% of users would be affected	Medium Noticeable but limited operational impact	Low Minimal to service operations
Almost Certain We are bound to expect these incidents, or they are happening right now	ECAB	HIGH/ECAB	MEDIUM/HIGH	LOW/MEDIUM
Probable We are likely to experience incidents of this nature soon	HIGH/ECAB	HIGH	MEDIUM	LOW
Possible There is some evidence to suggest we may be affected, nothing substantial	MEDIUM/HIGH	MEDIUM/HIGH	MEDIUM	LOW
Unlikely Incidents of this nature are uncommon but there is a chance we may experience them in the future	LOW/MEDIUM	LOW	LOW	VERY LOW

Requesting an Exception

Anyone can initiate an exception request by using the Request an Exception to a Vulnerability form (also Appendix B).

1. Enter the required information in the fields provided. (see 2.3 above) Requesters may also upload supporting documentation.
2. Submit the form to the Vulnerability Exceptions Quorum to review (2.2).
    - andrew.clarke@brunel.ac.uk;
    - peter.curling@brunel.ac.uk;
    - peter.elson@brunel.ac.uk;
    - Senani.Thotabaduge@brunel.ac.uk;
    - alan.charie@brunel.ac.uk; simon.furber@brunel.ac.uk;
    - peter.harrison@brunel.ac.uk;

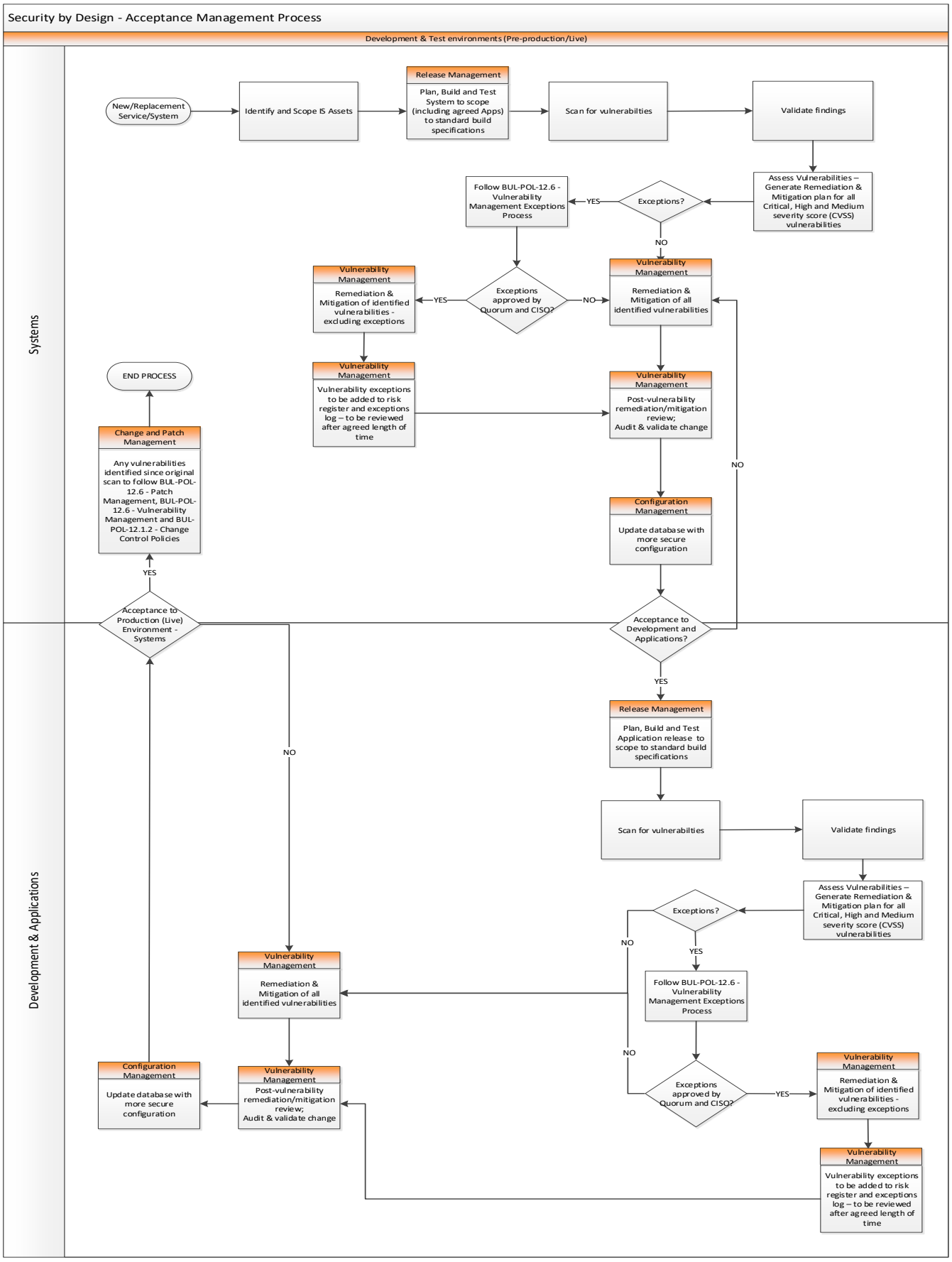
Note: Exceptions will not be granted when feasible alternatives exist or risks outweigh projected benefits.

All exception requests must present justification for the request and an expiration date. No exception can be permanent and each must be reviewed and extended using an expiration date to ensure no exceptions are permanently ignored.
The request should clearly state the exception type and be recorded using the exception features in the vulnerability management solution
False Positives identification will be escalated for solution improvement and then re-assessed. If no correction can be made, the exception is logged within the solution.

3. The Vulnerability Exceptions Quorum will either meet or communicate via email to discuss the exception request(s).
4. Once a decision has been made by the Vulnerability Exceptions Quorum. The University CISO will be advised to either accept or deny the exception request(s).
5. The Cyber and Information Security team will maintain a spreadsheet of all requests and the outcome.
6. Once the appropriate approvals are obtained, a Vulnerability Exceptions Quorum team member will reply via email with documented approval or denial of the request (along with request details) to the requestor and/or user for whom the exception was requested, copying the department head as well as the University CISO.
7. If the exception is granted and approvals obtained, the Cyber and Information Security team will provide the requester with any additional assistance as needed, such as coordinating with the relevant data steward(s) or other individual(s) who have a role in fulfilling the exception request and ensuring the length of time of the request is not exceeded.
8. If the exception is not granted, the Cyber and Information Security team will work with the user to define a reasonable deadline for compliance.
9. If the exception is not granted, the user may appeal the decision to the University CISO.
10. The user will be notified prior to expiration that the exception duration is ending. The user must then submit a new exception request or notify Vulnerability Exceptions Quorum that the exception is no longer needed.

Note: The requester(s) may not approve their own exception requests.

APPENDIX A – EXCEPTIONS PROCESS FLOW



APPENDIX B – EXCEPTIONS FORM

Request an Exception to a Vulnerability	
Date	
Exception submitted By: name, email, department	
Name of Vulnerability	
Risk classification (High, Medium, Low)	
Classification information sensitivity (Protect, University Confidential)	
Length of time (one, three, six, or 12 months)	
Exception Type: (False Positive, Acceptable Risk, Critical, Delayed Action)	
Explanation of exception	
List systems, networks, and/or data for which the exception will apply	
Details regarding any mitigating factors and compensating controls that will be used to offset the risk during the length of the exception	
Proposed remediation or mitigation resolution plan	
Urgency of Service	

This form must be sent to andrew.clarke@brunel.ac.uk; peter.curling@brunel.ac.uk; peter.elson@brunel.ac.uk; Senani.Thotabaduge@brunel.ac.uk; alan.charie@brunel.ac.uk; simon.furber@brunel.ac.uk; peter.harrison@brunel.ac.uk;

APPENDIX C – RESOURCE

Vulnerability Management					
	Scan owners	Vulnerability Allocation	Vulnerability Owner	Remediation	InfoSec Oversight
Systems	ALTAF JAMADAR IAN TARRAN PETER POLKINGHORNE RICHARD PERRY RICHARD WITHERSTONE SHWETA PATIL	ALAN CHARIE	TBC	ALTAF JAMADAR IAN TARRAN PETER POLKINGHORNE RICHARD PERRY RICHARD WITHERSTONE SHWETA PATIL	MICK JENKINS PETER CURLING ANDREW CLARKE
Dev & Apps	NAVEED IQBAL	PETER ELSON SENANI THOTABUGE	KEVIN WILKINSON	ALEX FRASER PETER HART	MICK JENKINS PETER CURLING ANDREW CLARKE
Networks	SIMON FURBER	SIMON FURBER	TBC	SIMON FURBER ANDY CRIPPS	MICK JENKINS PETER CURLING ANDREW CLARKE
College IT		JEREMY BAXTER NEIL NEWLAND STEPHEN MIDDLEHURST	PAUL WORTHINGTON MIKE KEIGHLEY AMANDA OLIVER	JEREMY BAXTER NEIL NEWLAND STEPHEN MIDDLEHURST	MICK JENKINS PETER CURLING ANDREW CLARKE
CCTV			TERRY VAAS	TERRY VAAS	PETER CURLING ANDREW CLARKE MICK JENKINS
Telephones		DAN REEVES	TBC	DAN REEVES	PETER CURLING ANDREW CLARKE MICK JENKINS
Clients / EndPoints	PETER HARRISON	PETER HARRISON	TBC	PETER HARRISON PAUL KIRK	PETER CURLING ANDREW CLARKE MICK JENKINS
Printers		ALAN CHARIE	TBC	IAN TARRAN RICHARD PERRY	PETER CURLING ANDREW CLARKE MICK JENKINS
Estates		CHRIS LICENSE	TBC	CHRIS LICENSE + TEAM	PETER CURLING ANDREW CLARKE MICK JENKINS