CYBER STANDARDS DOCUMENT

NCSP Vulnerability Management

ABSTRACT:
This standard supports the policy set out in the National Community Security Policy, providing requirements for those designing, building and running IT services, managing threats and vulnerabilities within PDS and policing systems.

Appendix 1
Further requirement clarification for threat intelligence requirements.

ISSUED	February 2025
PLANNED REVIEW DATE	February 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements threats and vulnerability management.

Introduction

Vulnerabilities are defects that weaken systems. All modern software contains vulnerabilities; either software defects that require patches or configuration issues that require administrative activity to resolve. These vulnerabilities must be addressed in a timely manner, to avoid disruption to organisation's operation and to preserve the confidentiality, integrity and availability of data and systems.

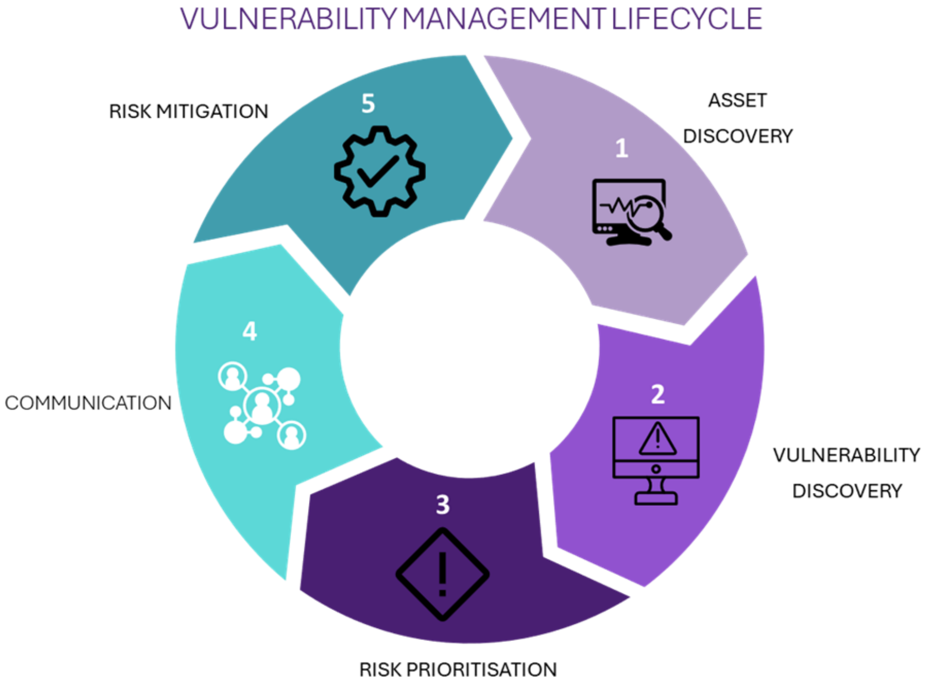
Vulnerability management is the lifecycle process that helps organisations identify, assess, prioritise, and minimise vulnerabilities in their system. Ultimately, the goal of vulnerability management is to reduce the risks posed by vulnerabilities by using techniques such as patching, hardening, and configuration management. This helps to ensure security while limiting risks that could potentially be exploited by malicious users.

This standard is aligned with the National Policing Cyber Security Strategy, objectives and outcomes have been derived directly from the Government Cyber Security Strategy 2022-2030 and adapted, where appropriate, for policing. Strategy supports wider work to ensure that policing is prepared and able to face current, new, and emerging threats from criminals and cyber incidents. The five objectives of the strategy are as follows,

- Managing information security risk.
- Protecting against cyber-attacks.
- Detecting cyber security events.
- Minimising the impact of cyber security incidents.
- Developing the right cyber security skill, knowledge, and culture.

For Vulnerability Management to be effective, it must be a continuous process. New vulnerabilities are consistently identified, security risks evolve, threat landscapes shift, and both risk appetites and business priorities are subject to change. Additionally, software and systems are frequently updated or replaced. This dynamic environment demands ongoing discovery of new or modified assets, vigilant monitoring of emerging vulnerabilities, and continual assessment and reprioritisation of threats, alongside effective reporting of progress. Consequently, effective Vulnerability Management involves a continuous process composed of a lifecycle consisting of strongly interdependent phases:

- **Asset discovery –** continuous process of identifying and cataloguing all the digital assets and creating an inventory.
- **Vulnerability discovery –** continuous and systematic approach to identify and uncover vulnerabilities within systems, applications, and networks.
- **Risk prioritisation and consolidation –** continuous and systematic process of determining the order in which vulnerabilities should be addressed, based on their potential business impact, severity, ease and likelihood of exploitation, and other factors.
- **Communication -** collaboration and communication between technology teams and business stakeholders is a vital component of a successful VM service.
- **Risk mitigation -** prioritised application of updates, considering prior testing of patches, available patch windows, and the potential impact of delay in patching.



Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to support the policy set out in the National Community Security Policy, providing requirements for those designing, building and running IT services and managing vulnerabilities within PDS & policing systems. This standard sets out the requirement to identify and address technical vulnerabilities in a timely and effective manner to reduce exposure to the risk of them being exploited, thereby reducing the risk of serious security breaches.

Furthermore, the requirements detailed in this standard are aligned with the following industry-standard frameworks and guidance:

- ISO 27002:2022
- CIS Controls
- NIST Cyber Security Framework
- Information Security Forum (ISF) Statement of Good Practice (SoGP)
- OWASP Vulnerability Management Guide (OVMG)

Audience

This standard is aimed at:

- Staff across PDS & policing to any person who builds & implements or maintains IT systems, either on behalf of National policing or at a local Force level,
- IT System managers, administrators and those who have escalated privileges to provide administrative functions.
- Information & cyber risk practitioners and managers.
- Information Asset Owners (IAOs), Platform Asset Owners (PAOs) and Senior Information Risk Owners (SIROs.)
- Suppliers acting as IT service providers or developing products or services for PDS or policing.
- Auditors providing assurance services to PDS or policing.

Scope

1. This standard is to cover systems handling data within the OFFICIAL tier including OFFICAL-SENSITIVE special handling caveat of the Government Security Classification Policy (GSCP). National and local policing IT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.
2. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.

Requirements

The requirements to deliver effective vulnerability management are described in the table below:

Reference	Minimum requirement	Control reference	Compliance Metric
1	Conduct continuous asset discovery exercises to identify assets, understand their business context, and analyse the results of scans or tests. Use these exercises to maintain visibility of the organisational asset landscape and apply appropriate security measures. Technology assets include all software, datasets, networks, servers, endpoint devices and peripherals. This also includes infrastructure, platform & software as a service (IaaS, PaaS & SaaS) infrastructure and DevSecOps environments. Record security-related details about assets, including hardware, software, and information, in accurate and up-to-date asset registers. Review these registers regularly and promptly investigate and resolve any discrepancies.	**ISF ISOGP** AM1.1 AM1.2 AM1.3 **NIST CSF 2.0** ID.AM-01 ID.AM-02 ID.AM-04 ID.AM-05 ID.AM-08 **ISO 27002:2022** 5.2 5.9 **CIS V8** 1.1 2.1 2.4	Validate the asset discovery process and assess the implementation of Asset Register Accuracy, Ownership Assignment, Discovery and Verification, as well as Criticality and Sensitivity measures.

Reference	Minimum requirement	Control reference	Compliance Metric
	Assign asset owners to take responsibility for managing and protecting assets throughout their entire lifecycle. Ensure organisation classify, maintain, and safeguard assets according to their criticality and sensitivity. **Linked Standards** - Physical Asset Management		
2	A process should be implemented to ensure the prompt identification, investigation, and resolution of technical vulnerabilities. Perform regular (automated where possible) vulnerability scans across all identified assets to detect known vulnerabilities. Evaluate information risk by analysing threats, threat events, vulnerabilities, existing controls, asset's business context and their potential impact on business operations.	**ISF ISOGP** TP2.1 IR2.4 AS2.1 **NIST CSF 2.0** ID.RA-01 DE.CM-06 DE.CM-09 ID.RA-05 **ISO 27002:2022** 8.8 8.18 5.35 **CIS V8** 7.1 7.5 7.6	Record of documented processes for identification, investigation and resolution of vulnerabilities Records of regular scans across IT assets Records of ITHCs audit reports, penetration test results and vulnerability assessments.

Reference	Minimum requirement	Control reference	Compliance Metric
3	A formally approved threat intelligence lifecycle must be established, underpinned by a specialised threat intelligence team and appropriate technologies. Its purpose is to provide comprehensive situational awareness, thereby empowering well-informed decisions and effective actions in the management of vulnerability risk. A prioritised set of requirements should be established to guide the creation of threat intelligence, addressing the necessary needs of the organisation. **Note** : Detailed Threat process is covered in Appendix 1	**ISF ISOGP** SE1.2 SE1.3 IR2.3 SM2.2 **NIST CSF** ID.RA-02 ID.RA-03 ID.RA-04 DE.AE-07 **ISO 27002:2022** 5.7 **CIS V8** 13.1	Documented evidence of vulnerability threat feeds and reviews. Records of communicating threat intelligence, decisions, actions, reviews.
4	Vulnerabilities identified should be prioritised based on the context of assets criticality for the organisations business, exploit complexity, asset exposure (Internal/External) vulnerabilities, and threat intelligence, ensuring continuous assessment to effectively address emerging risks. Establish and maintain a severity rating system to support prioritisation, taking into account the criticality of assets to the business, as well as the associated threats, exploitability, and vulnerabilities of those assets. **Note**: See further information section for prioritisation and handling exceptions	**ISF ISOGP** SE1.2 SE1.3 IR2.3 SM2.2 TP2.1 **NIST CSF** ID.RA-01 ID.RA-02 ID.RA-03 ID.RA-04 DE.AE.07 **ISO 27002:2022** 5.7 **CIS V8** 13.1	Documented evidence the organisation has a severity rating system and process for prioritising the order vulnerabilities are mitigated.

Reference	Minimum requirement	Control reference	Compliance Metric
5	A formal process must be established and maintained to receive and address reports of vulnerabilities, including a clear mechanism for external entities to report. This process should encompass a vulnerability handling policy that defines the reporting procedure, designates responsibility for managing vulnerability reports, and outlines steps for intake, assignment, remediation, and remediation testing. Additionally, the process should specify expected response times and timelines for resolving identified vulnerabilities.	**ISF ISOGP** TP2.2 SM1.1 **NIST CSF** ID.RA-08 PR.PS-01 PR.PS-02 GV.PO-02 **ISO 27002:2022** 8.8 **CIS V8** 16.2	Reporting process to the stakeholders, who is responsible for handling vulnerability reports, a process for intake, assignment, remediation, remediation testing, and a vulnerability tracking system. Records of time to respond and time to fix. Operational Level Agreements for remediation.
6	Current and newly identified vulnerabilities are mitigated with effective prioritisation for the organisation's assets or documented as accepted risks. Review patching The patch management process should include conditions for temporary exceptions from patches being applied. Exceptions must be reviewed in regular interval **Note** : See further information section for handling exceptions	**ISF ISOGP** TP2.2 IR2.6.7 IR2.6.8 **NIST CSF** ID.RA-06 ID.RA-08 PR.PS-01 PR.PS-02 **ISO 27002:2022** 8.8 **CIS V8** 7.3 7.4	IAO/SIRO/PAO receives and reviews monthly vulnerability reports to ensure all vulnerabilities are mitigated within expected timeframes or risk accepted and documented.

Reference	Minimum requirement	Control reference	Compliance Metric
7	Handling unsupported / obsolete systems or applications: Establish a clear management plan, including tactical mitigations and timeline for the decommissioning, replacement or upgrade of obsolete systems. All risks should be recorded on the risk register. Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded Risk responses are chosen, prioritised, planned, tracked, and communicated **See also** • National Information Security Risk Management Framework	**ISF ISOGP** IR1 IR2.3 IR2.4 IR2.5 **NIST CSF** GV.RM-01 ID.RA-04 ID.RA-06	Corporate risk register (for national systems – Project risk register). Management plan to address.

Further information

Requirement 4 : Vulnerability Prioritisation

Prioritising the remediation of vulnerabilities should be based on factors such as impact, severity, and exploit complexity. The decision to address or accept a vulnerability is fundamentally a business decision, and each organisation must balance this against its own risk appetite. Guidance, such as the National Police Information Security Risk Management Framework, can serve as a useful benchmark for making these decisions. Additionally, the Nationally available threat intelligence provides regular threat intelligence updates, which can inform and enhance the prioritisation process.

Effective vulnerability prioritisation can be achieved by integrating both vulnerability and asset risk ratings, which together provide a comprehensive view for informed decision-making. Vulnerability risk rating focuses on assessing threats to each asset, with added contextual components enhancing rating precision. This includes the inherent vulnerability risk rating, often guided by the Common Vulnerability Scoring System (CVSS) score, active threat intelligence tracking the exploitation of vulnerabilities Exploit Prediction

Scoring System (EPSS), and advanced data analytics that leverage machine learning to predict vulnerability risks.

On the other hand, asset risk rating defines the tangible business impact should an asset be exploited. This includes classifying data (such as PCI, PII, and confidential information) to assess sensitivity, evaluating existing mitigation controls like Endpoint Detection and Response (EDR) and Web Application Firewalls (WAF), and considering architecture risks based on asset exposure, whether external, internal, or APIs. Together, these factors allow for more actionable prioritisation, as they not only focus on vulnerability severity but also account for the business impact, active threats, and potential risk mitigations.

Requirement 6 : Handling exceptions

When handling exceptions in vulnerability management, it is crucial to adopt structured best practices to ensure that risk is managed effectively without leaving critical gaps. Here are best practices for handling exceptions:

1. Exception Request Process:

- Establish a process for requesting, reviewing, and approving exceptions. This should involve detailed documentation of why a vulnerability is not being remediated, including business justifications, risk assessments, and compensating controls in place.
- Exception requests should be reviewed by a cross-functional team, including stakeholders from security, IT, and business units.

2. Risk-Based Justification:

- Exceptions should only be granted after a thorough risk assessment. Use exploit complexity to the asset environment, EPSS and CVSS scores to justify the risk level, ensuring that decisions are based on the likelihood of exploitation, impact, and exploit complexity.
- Document the business impact and align it with the organisation’s risk appetite. For instance, a low-risk vulnerability with a low EPSS score may be more acceptable than a critical vulnerability with a high EPSS score.

3. Compensating Controls:

- When granting exceptions, consider implementing compensating controls to mitigate risk.
- Document these controls and regularly review their effectiveness to ensure they provide adequate protection.

4. Time-Bound Exceptions:

- Exceptions should not be open-ended. Set time limits for each exception, with a predefined review period. This ensures that vulnerabilities are reassessed regularly as the threat landscape evolves or new exploit information becomes available (e.g., updated EPSS scores).

5. Continuous Monitoring:

- Continuously monitor vulnerabilities under exception. As exploitability predictions change over time, particularly if EPSS scores increase, revisit the decision to defer remediation.

6. Documentation and Accountability:

- Maintain thorough documentation of all exceptions, including justification, risk assessments, compensating controls, and expiration dates. This ensures accountability and enables security teams to demonstrate compliance with internal and regulatory policies.
- Make these records available for internal audits and to ensure stakeholders are aware of outstanding risks.

7. Regular Reassessment:

- Exceptions should be regularly reassessed based on changes in the business environment, threat landscape, or vulnerability information. If the EPSS score increases or new exploits are discovered, security teams should reconsider whether the exception is still valid.
- Use this opportunity to review the organisation's risk posture and decide whether remediation is now necessary.

8. Alignment with Risk Appetite:

- Ensure that exception handling aligns with the organisation's overall risk appetite, as determined by frameworks like the National Police Information Security Risk Management Framework. IAO/SIRO/PAO play a critical role in ensuring that exceptions do not introduce unacceptable risks and that decisions around exceptions are consistent with the organisation's risk tolerance.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

This standard should be socialised with IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with your Force SIRO / Security Management Forum. Consideration should also be given to raising awareness amongst Force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

Review Cycle

This standard will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the standard continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

Appendix 1

Further requirement clarification for threat intelligence requirements.

Reference	Minimum requirement	Control reference	Compliance Metric
1	Threat Intelligence - Each policing community member, PDS, Partner and 3rd party supplier should have a process in place to act with the nationally produced intelligence for cyber security which can effectively create, process, and manage threat intelligence. Threat intelligence utilised and created by policing should be: • relevant • insightful • contextual • actionable	**ISF ISOGP** SG1.2 SE1.2 SE1.3 IR2.3 SM2.2 **NIST CSF 2.0** ID.RA-02 ID.RA-01 ID.RA-03 ID.RA-04 DE.AE-07 **ISO 27002:2022** 5.7 **CIS V8** 13.1	NMC Cyber Liaison Officers can confirm if cyber incident response plans have been reviewed and / or tested. Artefacts produced by these requirement might include defined processes, a list of sources, threat assessments, reports. Records of communicating threat intelligence, decisions, actions, reviews.
2	Process - The threat intelligence capability should be supported by a documented intelligence cycle, which includes: • a prioritised set of requirements to direct the production of threat intelligence. • identified information sources. • collection of relevant information from selected sources • processing information to prepare it for analysis. • conducting analysis of information to produce threat intelligence.		

Reference	Minimum requirement	Control reference	Compliance Metric
	• communicating threat intelligence clearly and concisely • using threat intelligence to inform decisions related to information risk. • taking action to implement the decisions made. • reviewing and improving the threat intelligence capability.		
3	Collection - Information relating to potential risks and/or adversarial attacks should be collected from both internal and external sources: Internal: • event logs from infrastructure and a security information and event management (SIEM) system • alerts from security solutions • dedicated teams that perform information security-related activities External: • trusted threat information providers or advisors • government agencies or similar • publicly available information		Evidence of log /alert collections, analysis, reports. List of sources, trusted advisors, agencies worked with.
4	Prioritisation - The prioritised requirements should focus on providing threat intelligence with the organisation's specific needs and strategic objectives. This should: • provide an early warning system to identify threats		Threat assessments reports, early warning reports, vulnerability assessments, analysis of tactics, techniques and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric
	that are likely to target the organisation. • determine the motivation, capabilities and commitment of identified threats and the extent to which the organisation is at risk of a targeted attack. • identify threat events likely to be used to attack the organisation. • demonstrate how information, gathered during reconnaissance, could be used by attackers. • determine the prevalence of threat events used at different stages of the cyber-attack chain. • identify technical vulnerabilities in operating systems, applications, and other software, which could be exploited to perform attacks on the organisation. • identifies the techniques used by attackers to maintain control of compromised systems and conceal their activity.		
5	Technology - The intelligence cycle should be supported by: • analytical tools, such as threat intelligence platforms (TIPs), to support the production and analysis of threat intelligence.		Suite of tools/ sources/ partners.

Reference	Minimum requirement	Control reference	Compliance Metric
	• collaboration and the sharing of information with approved partners		
6	Decision making - There should be 3 layers of threat intelligence across policing: • Strategic Threat Intelligence: high level information about the threat landscape • Tactical Threat Intelligence: intelligence on tools, techniques, and attack methodologies • Operational Threat Intelligence: intelligence on specific attacks and indicators		Defined process including documented decision making.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial version	09/11/22
0.2	PDS Cyber	Internal review updates	25/11/22
0.3	PDS Cyber	Updated and circulated to PDS SMEs	16/12/22
0.4	PDS Cyber	Rebranded to NPCC PDS template	02/02/22
0.5	PDS Cyber	Updated following NCPSWG comments	27/04/23
2.0	PDS Cyber	Rebranded to NPCC PDS template and reworked based on **National Policing Cyber Security Strategy**	03/12/24

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for cyber standards	30/11/23
2.0	National Cyber Policy & Standards Board	National authority for cyber standards	06/02/25

Document References

Document Name	Version	Date
National Policing Cyber Security Strategy		2024
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8.1	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
OWASP Vulnerability Management Guide (OVMG)	June 2020	06/2020
ISF Vulnerability Management Briefing Paper 2023	V1	2023
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
National Police Information Security Risk Management Framework	V1	