CYBER STANDARDS DOCUMENT

NCSP Security Testing Standard v1.0

ABSTRACT:
This standard describes approaches to delivering comprehensive security testing (using a range of attack types) to support security and risk compliance monitoring.

It supplements National Community Security Policy Information Assurance core standard.

ISSUED	March 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

COPYRIGHT: Police Digital Service

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 for information security assurance, specifically IT security vulnerability testing, commonly referred to as Information Technology Health Checks (ITHCs.).

Introduction

This standard describes the requirements to help fulfil the National Community Security Policy (NCSP) Information Security Assurance Policy statement with regards to technical testing. It also provides specific details to support the Information Systems Assurance requirements as described in the NCSP Information Security Assurance standard.

Conducting security tests against IT systems provides essential assurance to the policing community of trust. This assurance includes;

1. Identifying vulnerabilities in policing systems through independent testing can uncover weaknesses in infrastructure, networks, systems or applications that could be exploited by threat actors.
2. Understanding and mitigating security risks is critical to the resilience and trust of policing systems. Testing allows for the proactive management of risks.
3. Regular (at least once a year and/or following any significant change) or, where possible, continuous testing, helps to validate that existing security controls are still effective and operating as required. It can be used to help prioritise improvements.
4. Testing can be used to simulate and test local incident detection and response procedures in a safe manner, thereby providing assurance that they will be effective during an active incident.
5. Cyber threats are continually evolving and regular testing helps ensure that the security environment is improving and ready to respond to new threats.

COPYRIGHT: Police Digital Service

6. Testing provides validation of the security controls in place within an IT environment and IT systems, ensuring they are suitably implemented and configured to provide the expected level of risk mitigation.

This standard is designed to enable members of the community of trust to scope and deliver effective deliver effective independent IT security vulnerability tests (at least annually) and additional security tests required for new or significantly changed systems. It describes what needs to be considered whilst scoping testing and how to make the most of the resources available to assure the security of policing IT.

Security testing (also sometimes referred to as Penetration Testing) is a crucial security assessment carried out by ethical hackers and experienced DevOps engineers. Its primary aim is to probe and uncover potential vulnerabilities within an organisation's security architecture. This type of testing is particularly essential during significant changes to the infrastructure or network, following the addition of new infrastructure or applications, and when there are changes or expansions in office locations within the network. This must be performed at least annually on your environment and is also referred to as an ITHC throughout policing and other businesses. It provides security teams and senior leadership with an understanding of their current risk exposure should they become compromised.

A vulnerability scan is a part of a security test and is a security management strategy to identify and report vulnerabilities in applications, servers and firewalls. This is a regular scan that should be performed to provide security teams with regular updates and understanding of your environment. See the NCSP Vulnerability Management standard.

Conducting regular testing will assist in providing evidence for the Security Assessment for Policing (SyAP) , Third Party Assurance for Policing and provide assurance for connecting to National Policing systems that have SyAP minimum maturity rating requirements.

Localised security tests or vulnerability scans on new implementations also help to provide assurance that the environment and/or system is robust and will protect the data held within it, ensuring public trust. This includes solutions on local corporate networks as well as Cloud services.

Consideration may also be given to conducting continuous automated testing within the environment, through use of an approved compliance tool.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard helps members of the policing community of trust demonstrate compliance with the following NCSP policy statements:

Information Assurance

- Implement a consistent and structured information security assurance programme, supported by comprehensive security testing (using a range of attack types), penetration tests, and regular security and risk compliance monitoring.

- To provide specific audiences, including representatives from executive management, Policing operations, and IT, with an accurate, comprehensive, and coherent view of information risk across the organisation. Conduct thorough, independent, and regular audits of the security status of target environments (e.g. critical operational environments, processes, applications, and supporting technical infrastructure).[1]

System Development

- Develop applications in accordance with a robust system development lifecycle, which includes applying industry good practice and incorporating information security during each stage of the lifecycle (secure by design); requirements gathering; design; acquisition (including purchase, lease and open-sourced); build; testing; implementation; and decommission.

The purpose of this standard is to enable Police Forces and key partners provide assurance that their organisation is protected from unauthorised access, loss, change, exfiltration or service denial, and they do not provide any unnecessary access into the network or systems that consume policing data.

Audience

This standard is aimed at:

- Information Security Officers (ISOs), information security practitioners and any roles who propose, plan, scope, undertake and review security tests (ITHCs).

- Information Asset Owners (IAOs.)

- Digital Data and Technology / Information Communication Technology teams

- Project managers responsible for delivering new DDaT solutions into policing

[1] For further information, refer to the Vulnerability Management Standard

Scope

This standard applies to any member of the Policing Community of Trust. It is also applicable to third parties to the policing community.

It applies to systems or services that process or store policing information. This includes services not hosted or fully maintained by policing and law enforcement organisations, such as Software as a Service (SaaS) solutions, and includes:

- Annual Security Testing
- Continuous Testing
- Testing of any new system prior to its live deployment
- Testing of any significant change to live systems

Requirements

This section details the minimum requirements to implement a effective Information Security testing to assure systems and services that process policing information.

Please also refer to the Information Security Assurance and System Development (Sbd) standards.

It is intended that the requirements listed in this standard can be used to form scoping requirements when engaging security testing providers.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
Governance and management			
CSP-ITHC-00 **Authority**	The Senior Information Risk Owner is accountable for ensuring that security tests are undertaken and managed according to risk appetite. Information Asset Owners are responsible for ensuring that that their projects / systems are tested commensurate with risk appetite. Senior authority must be sought prior to engaging any security testing (IT health checks). Testing must be planned and scheduled in order to avoid operational IT service disruption. Consideration must be given to avoid testing during sensitive times such as peak service demands, major change programmes or during IT or security incidents. All testing engagements shall ensure that testing can be immediately suspended if there are operational reasons to do so.	NIST CSF ID.GV & ID.RM ISO 27001:2022 5.35, 8.16, 18.21 ISF SoGP AS2 NCSC CAF Principle B4 System security	Records of authorities to test (likely endorsed by SIRO, SRO, CTO or equivalent) Records of engagement with IT service management and scheduling sensitive to operational and IT service needs.
CSP-ITHC-01 **Frequency**	Security testing must be carried out at least annually on your network and/or systems, prior to the expiry of the previous test, and following any significant change Where feasible, continuous assessments through an approved compliance tool should be utilised, to identify and assess vulnerabilities within your environments.	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Evidence formal annual ITHC has been completed. Risk based decisions regarding scopes.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	The scope of testing must be proportionate to the criticality of the environment and ensure the scoping requirements within this document are included. For example, whilst it is important that mission critical systems have more functions within scope than other, less critical systems, consideration must be given to the likely routes of entry into a system or network and factor these into the scope of test		
CSP-ITHC-02 **New Environments /Systems**	When a new environment or system solution has been created to hold Policing data, a test must be carried out to ensure it meets security specification. Examples include but are not limited to: • New on premises environment. • New SaaS solutions. • New Cloud Implementations. • Proof of Concept (PoC) and pilot systems You must ensure the entire system is assessed and implemented securely, including all routes into your environment (e.g. if you have implemented a SaaS solution). Testing should be on production environments, or you should be able to evidence that the tested environment is technically identical to the deployed environment e.g. through Infrastructure as Code This is expected to be a standalone security test, and is separate to your annual security testing. Testing of PoC / pilot systems should consider the exposure of meta-data or configuration data. Testing must be carried out prior to any Policing or sensitive data being uploaded into the system/environment.	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Evidence that test has been completed on new environment.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
CSP-ITHC-03 **Changes**	Significant changes to the environment or system shall also trigger consideration of a security test. Examples of changes includes; • Upgraded components – software or hardware • Changes to connections to other systems or environments • New systems introduced (not covered at CSP-ITHC-02) • Increased risk exposure, such as increased threat or criticality / sensitivity. • Following a security incident or breach.	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Internal procedures Projects / Change Advisory Board artefacts. Records of decisions to test / not test Records of tests / reports Incident reviews
CSP-ITHC-04 **CHECK Testers**	All security testing that is undertaken on any network or system that contains policing data must be undertaken by a National testing framework member[2] or NCSC-approved CHECK testing company. This must be conducted by an accredited CHECK Team Leader (or, if testing conducted by a team, this must include a CHECK Team Leader). When engaging services of a test provider, security must be considered, to ensure provider-supplied equipment meets any required standards. Similarly, if host provides the equipment, it should be able to meet the requirements of the tester/s. Testers must be	NIST CSF ID.GV.2, ID.GV.3 & ID.BE.2 NCSC CAF Principle B4 System security	Selection of CHECK approved company. Verify suppliers - NCSC.GOV.UK

[2] Details of national framework members can be provided via Blue Light Commercial, or the NMC

Reference	Minimum Requirement	Control Reference	Compliance Metric
	able to export data from equipment to include in their reports. As specified by NCSC guidance, any systems processing SECRET and above must be performed using 2 CHECK Team Leaders with appropriate clearances.		
CSP-ITHC-05 **Vetting**	All testers must be NPPV3 vetted by either your individual Force vetting team, or through National vetting through Warwickshire Constabulary. **See also:** • Vetting Authorised Professional Practice (APP) • NCSP Vetting requirements for policing guideline	NIST CSF ID.GV.2, ID.GV.3 & PR.AT.5	Evidence of NPPV3 vetting on all testers.
Scoping requirements[3]			
CSP-ITHC-06 **Device Builds**	As part of your scope, you must test all end user device builds your organisation uses. Examples include but are not limited to: • Desktops • Laptops • Phones • Tablets NOTE: You are not required to test every single device, but a proportionate amount of each build (*providing that the builds are representative of the IT estate.)*	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that all device builds are included within your scope. Evidence of output in findings.
CSP-ITHC-07 **Operating Systems**	As part of your scope, you must test all Operating Systems you use on your environment. Examples include but are not limited to:	NIST CSF ID.RA.1, DE.DP.3,	Evidence that all device OS builds are included

[3] Should be read in conjunction with the Physical Asset Management standard and IoT guidance documents

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Windows XP, 7, 10, 11 including server versions where used • Android OS • Apple iOS • Embedded systems • Industrial Control Systems	DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	within your scope. Evidence of output in findings. Remediation plans
CSP-ITHC-08 **Third Party Software**	As part of your scope, you must test your third party software versions, such as: • Browsers (incl. secure configuration) • Adobe • Java	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that vulnerability scans of third party software are included within your scope. Evidence of output in findings.
CSP-ITHC-09 **Mobile Device Management**	As part of your scope, you must test your Mobile Device Management (MDM) solutions. Including but not limited to; • Device Enrolment • Device Patching • Device compliance, security, and management	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that MDM checks are included within your scope. Evidence of output in findings.
CSP-ITHC-10 **Firewall Review**	As part of your scope, you must test all boundary devices (incl. perimeter firewalls, routers, gateways proxies etc.), as well as a selection of your internal firewalls. Examples include but are not limited to: • Firewall Rule Review • A selection of all internal firewalls used (Cisco, Juniper, SonicWall, WAF etc.)	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that firewall review and patching is included within your scope. Evidence of output in findings.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Patching • Any outbound connectivity		Basic network overview diagram.
CSP-ITHC-11 **Infrastructure**	You must test a selection of all your infrastructure builds. This testing must include, but is not limited to: • All different server builds and models • Virtual machines including underlying hypervisor. • Core network infrastructure including telephone systems and control systems. • The patching status of all infrastructure • Internal firewalls and routers • Cloud infrastructure (including SaaS applications) • Email Servers • Proxys • DNS Servers • AI servers (where applicable)[4] • File servers • Domain Controllers • Database Servers	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that infrastructure reviews have been included within your scope. Evidence of output in findings (including output from credentialed vulnerability scanning) Basic network overview diagram.
CSP-ITHC-12 **Encryption**	As part of your scope, you must test your encryption standards on your devices and network. Examples include but are not limited to: • Hard Disk Encryption (HDE) • Data in Transit	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Evidence that encryption checks are included within your scope.

[4] For further guidance, refer to the NCSP Artificial Intelligence & LLM (Large Language Models) standard v1.1

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Data at Rest • Password hashing standards.		Evidence of output in findings.
CSP-ITHC-13 **Malware and Anti-Virus**	As part of your scope, you must test your malware and antivirus capabilities are receiving updates, cover your entire corporate environment and are receiving updates at an appropriate frequency, e.g. daily.	NIST CSF DE.DP.3, DE.DP.5, DE.CM.4, DE.CM.8 NCSC CAF Principle B4 System security	Evidence that all device builds are included within your scope. Evidence of output in findings.
CSP-ITHC-14 **Passwords and Authentication**	Passwords must meet or exceed the NCSP National Password Standard and be tested against its requirements. This includes, but is not limited to: • Password Security standards • Multi-Factor Authentication • Password Security on shared email accounts • Local, Application and System Administrators • All privileged access accounts • Root Accounts • Authorised Remote Access Authentication	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Evidence that check is being completed within your scope. Evidence of output in findings.
CSP-ITHC-15 **Wireless Networks**	Corporate and guest wireless networks must be tested, including; • Correct use of secure protocols such as WPA2, WPA3 • Identify all networks and wireless access points (APs)– discover any hidden / unauthorised networks or rogue Aps	NIST CSF DE.DP.3, DE.DP.5, DE.CM.8, PR.DS.2, PR.AC.5, PR.PT.4	Evidence that all device builds are included within your scope.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Wireless access point patching • Validate encryption strength • Test authentication mechanisms • Client isolation • Guest network isolation • Wireless intrusion detection • Resistance to attacks such as evil twin, flooding, denial of service.	NCSC CAF Principle B4 System security	Evidence of output in findings.
CSP-ITHC-16 **Remote Access Capabilities**	Remote access solutions such as Virtual Private Networks (VPNs) must be included in your annual ITHC including; • Authentication • Encryption • Firewall configuration • Segmentation	NIST CSF DE.DP.3, DE.DP.5, DE.CM.8, PR.DS.2, PR.AC.5, PR.PT.4 NCSC CAF Principle B4 System security	Evidence of solution covered in scope. Evidence of output in findings.
CSP-ITHC-17 **DMZ**	Demilitarised Zones (DMZ) and solutions held within it must be tested including; • Firewall(s) & network devices • Intrusion detection / prevention • Server & web application security • Segmentation	NIST CSF DE.DP.3, DE.DP.5, DE.CM.8, PR.AC.5, PR.PT.4 NCSC CAF Principle B4 System security	DMZ reviews have been included within your scope. Network overview diagram. Evidence of output in findings.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
CSP-ITHC-18 **SECURED Environments**	All SECURED Environments must be tested to the same principles as in this document. Additional checks are required, including: • Ensuring there is no direct internet connection from your SECURED environment. (e.g. allowing for internet connections via proxy solutions and for Intune-managed devices)	NIST CSF ID.RA.1, DE.DP.3, DE.DP.5, DE.CM.8, PR.AC.5, PR.PT.4 NCSC CAF Principle B4 System security	Evidence that SECURED environments reviews have been included within your scope. Evidence of output in findings.
CSP-ITHC-19 **Threat based / scenario**	Consideration must be given into completing separate scenario-based (or threat based) testing to test real-life scenarios. This will help to test the efficiency of local incident response processes against specific system/network threats and identify specific risks that attackers look for. Adopt a testing framework or methodology such as • OWASP application testing • Penetration Testing Execution Standard • MITRE attack framework • NIST Special Publication 800-115	NIST CSF DE.DP.3, DE.DP.5, DE.CM.8, PR.IP.10 NCSC CAF Principle B4 System security	Use of testing frameworks Information Security / Cyber incident response plan Threat modelling Scoping against threats
Post-testing			
CSP-ITHC-20 **ITHC Output**	All results from the security test: • Must be easy to analyse and prioritise, • Must show current CVSS ratings where possible for all identified vulnerabilities, • Should contain a contextual explanation of the threat posed,	NIST CSF DE.DP.3 & DE.DP.5 NCSC CAF Principle B4 System security	Evidence of output in findings.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Should include a machine-readable list of findings, such as CSV or Excel file, along with the written report. This is to ensure that the findings are traceable to the report summary / executive summary. **The test results must be afforded the appropriate security classification considering the impact of improper disclosure.**		
CSP-ITHC-21 **Remedial Action Plan**	A Remedial Action Plan (RAP) must be built from security test output. This output must include the findings, as well as; • Mitigations and actions being undertaken to remediate the task. • Initial target completion date. • Actual completion date. Any vulnerabilities identified must be risk assessed, added to the relevant Risk Register and actioned in a timely manner, according to their assessed impact until they have been mitigated or closed.	NIST CSF 2.0 ID.IM.01 & ID.IM.02 NCSC CAF Principle B4 System security	Evidence of output in findings. Evidence of Remedial Action Plan.
CSP-ITHC-22 **Remediation of Vulnerabilities**	Identified vulnerabilities must be mitigated across the entire estate, not just on the system, server, or application where the vulnerability was identified. Remediation should be based on criticality of the vulnerabilities identified. It is likely that one action will mitigate a number of identified vulnerabilities. Therefore, it is recommended that an action list supporting the RAP is created to enable senior leadership a clear picture of what is being undertaken to support the risk.	NIST CSF ID.RA.1, DE.DP.3 & DE.DP.5, PR.IP.12 NCSC CAF Principle B4 System security	Evidence of Remedial Action Plan. Evidence of mitigated actions (e.g. this may be evidenced through retesting and test result outputs)

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric
	See also: NCSP Vulnerability Management Standard.		
CSP-ITHC-23 **Security Testing Reporting and management of findings**	The SIRO (or relevant risk owner) must be provided with a report of findings which articulate the risk in the overall context of the whole IT estate. The report must include suggested remediations, owners and timescales to resolve. The SIRO has the authority to accept or decline risks in accordance with risk appetite as described in the **National Information Security Risk Management Framework.** Outstanding remediations must be reported to and tracked by the appropriate governance forum such as the information security management board or equivalent.	NIST CSF ID.RM.1, ID.GV.4, ID.RA.6 NCSC CAF Principle B4 System security	Reports provided to SIRO SIRO decision records. Risk registers & treatment plans. Board reports and minutes.
CSP-ITHC-24 **Future testing**	Future testing must include validation that remediations have been satisfactorily resolved. Test scopes must be reflective of threat, environment and organisational changes since the last test.	NIST CSF ID.RA.1, DE.DP.3 & DE.DP.5, PR.IP.12 NCSC CAF Principle B4 System security	Tracking of remediations across tests.

COPYRIGHT: Police Digital Service

Reference	Minimum Requirement	Control Reference	Compliance Metric

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 distributed with information security officers (ISOs) and Digital Data and Technology (DDaT) / ICT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / 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.)

COPYRIGHT: Police Digital Service

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
1.0	PDS Cyber	Standard created from initial guideline version	06/12/2024

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	27/03/25

COPYRIGHT: Police Digital Service

Document References

Document Name	Version	Date
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	05/2021
NIST Cyber Security Framework	v1.1	04/2018
NCSC Cyber Assessment Framework (CAF)	v3.2	04/2024
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
Physical Asset Management Standard	v1.0	02/2024
Artificial Intelligence & LLM (Large Language Models) Standard	v1.1	09/2024

COPYRIGHT: Police Digital Service