CYBER GUIDANCE DOCUMENT

NCSP Penetration testing and IT Health checks Guideline

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

It supplements National Community Security Policy Information Assurance core standard.

ISSUED	February 2024
PLANNED REVIEW DATE	January 2025
DISTRIBUTION	Community Security Policy Framework Members

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

Cyber guideline 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 guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements for information assurance specifically penetration testing and Information Technology Health Checks (ITHCs.)

Introduction

Conducting regular (at least once a year) or where possible continuous penetration tests against IT systems provides essential assurance to the policing community of trust. This assurance includes;

1. Identifying vulnerabilities in policing systems through 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) 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.

This guidance document is designed to support members of the community of trust to complete their annual IT Health Check (ITHC) and additional penetration tests. 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.

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 after applying security

patches, during significant changes to the infrastructure or network, following the addition of new infrastructure or web applications, and when there are changes or expansions in office locations within the network.. It can also be carried out continuously within your environment with an approved compliance tool. This should 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 penetration 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.

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

Localised penetration 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 Software as a Service (SaaS) or Cloud services.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This guidance helps organisations 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).

The purpose of this guidance is to help Police Forces and key partners provide assurance that your organisation is protected from unauthorised access or change, and they do not provide any unauthorised entry points into the network or systems that consume policing data.

Audience

This guidance is aimed at:

- Information Security Officers (ISOs), information security practitioners and any roles who plan, undertake and review penetration tests or ITHCs.
- Member Senior Information Risk Owners (SIROs), and Information Asset Owners (IAOs.)
- Third parties who act as service providers or suppliers to members.
- Auditors providing assurance services to members.

Scope

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

It applies whenever an annual ITHC or a penetration test is to be carried out on member systems or services that process or store policing information assets. It includes services not hosted or fully maintained by members such as Software as a Service (SaaS) solutions.

Guidance details

- This guidance document has been created with the NCSP objectives at its centre. The table below highlights the requirements within the NCSP that this guidance document meet this requirement.
- See appendix A for a template of ITHC submissions.
- All guidance details are relevant to SyAP reference RS.MI.3

Reference	Minimum Requirement	Compliance Metric
Governance and management		
CSP-ITHC-00 **Authority**	The Senior Information Risk Owner is accountable for ensuring that ITHCs are undertaken and managed. 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 penetration testing or 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.	Annual ITHC funded and undertaken. Records of SIRO authorities to test. Records of engagement with IT service management and scheduling sensitive to operational and IT service needs.
CSP-ITHC-01 **Frequency**	An ITHC must be carried out at least annually on your corporate network prior to the expiry of the previous test. Where possible, continuous assessments through an approved compliance tool can also be utilised to identify and assess vulnerabilities within your environments. The scope of your environment must be proportionate to the criticality of the environment and ensure the scoping requirements within this document are included. For example its is important that mission critical systems have more functions within scope than other less critical systems.	Evidence formal annual ITHC has been completed.
CSP-ITHC-02 **New Environments**	When a new environment has been created to hold Policing data, a test must be carried out to ensure it meets security specification.	Evidence that test has been completed on new environment.

Reference	Minimum Requirement	Compliance Metric
	Examples include but are not limited to: • New on premises environment. • New SaaS solutions. • New Cloud Implementation. You must ensure the entire network is assessed and implemented securely, including all routes into your environment if you have implemented a SaaS solution. This is expected to be a standalone ITHC separate to your annual ITHC. This must be carried out prior to any Policing or sensitive data being uploaded into the system/environment.	
CSP-ITHC-03 **Changes**	Changes to the environment or system shall also trigger consideration of an ITHC. 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.	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 ITHC and penetration testing that is undertaken on any network or system that contains policing data must be undertaken by a National testing framework member or NCSC approved CHECK testing company. This must be conducted by a CHECK Team Leader. As specified by NCSC guidance, any systems processing SECRET and above must be performed using 2 CHECK Team Leaders with appropriate clearances.	Selection of CHECK approved company. Verify suppliers - NCSC.GOV.UK

Reference	Minimum Requirement	Compliance Metric
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	Evidence of NPPV3 vetting on all testers.
Scoping requirements		
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: • Windows Devices • Android • Apple • Hard Disk Encryption (HDE) NOTE: You are not required to test every single device, just a proportionate amount of each build (*providing that the builds are representative of the IT estate.)*	Evidence that all device builds are included within your scope. Evidence of output in findings.
CSP-ITHC-07 **Operation Systems**	As part of your scope, you must test all Operating Systems you use on your environment. Examples include but are not limited to: • Windows XP, 7, 10, 11 • Android OS • Apple iOS	Evidence that all device OS builds are included within your scope. Evidence of output in findings. Remediation plans
CSP-ITHC-08 **Mobile Device Management**	As part of your scope, you must test your Mobile Device Management (MDM) solution.	Evidence that MDM checks are included within your scope. Evidence of output in findings.
CSP-ITHC-9 **Firewall Review**	As part of your scope, you must test all perimeter firewalls, as well as a selection of your internal firewalls.	Evidence that firewall review and patching

Reference	Minimum Requirement	Compliance Metric
	Examples include but are not limited to: • Firewall Rule Review • A selection of all firewalls used (Cisco, Juniper, SonicWall, WAF etc.) • Patching • Any outbound connectivity	is included within your scope. Evidence of output in findings. Basic network overview diagram.
CSP-ITHC-10 **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. • The patching status of all infrastructure • Internal firewalls and routers • Cloud infrastructure • Email Servers • Proxy's • DNS Servers	Evidence that infrastructure reviews have been included within your scope. Evidence of output in findings. Basic network overview diagram.
CSP-ITHC-11 **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 • Data at Rest • Password hashing standards.	Evidence that encryption checks are included within your scope. Evidence of output in findings.
CSP-ITHC-12 **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 least daily.	Evidence that all device builds are included within your scope. Evidence of output in findings.
CSP-ITHC-13	Passwords must meet the NCSP National Password Standard and be tested against its requirements.	Evidence that check is being completed within your scope.

Reference	Minimum Requirement	Compliance Metric
Passwords and Authentication	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	Evidence of output in findings.
CSP-ITHC-14 **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 • Validate encryption strength • Test authentication mechanisms • Client isolation • Wireless intrusion detection • Resistance to attacks such as evil twin, flooding, denial of service.	Evidence that all device builds are included within your scope. Evidence of output in findings.
CSP-ITHC-15 **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	Evidence of solution covered in scope. Evidence of output in findings.

Reference	Minimum Requirement	Compliance Metric
CSP-ITHC-16 **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	DMZ reviews have been included within your scope. Network overview diagram. Evidence of output in findings.
CSP-ITHC-17 **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 internet connection from your SECURED environment.	Evidence that SECURED environments reviews have been included within your scope. Evidence of output in findings.
Threat based / scenario **CSP-ITHC-18**	Consideration should 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	Use of testing frameworks Information Security / Cyber incident response plan Threat modelling Scoping against threats

Reference	Minimum Requirement	Compliance Metric
Post testing		
CSP-ITHC-19 **ITHC Output**	All results from the ITHC must be: • Easy to analyse and prioritise, • Show current CVSS ratings for all identified vulnerabilities, • Contain a contextual explanation of the threat posed. **The test results must be afforded the appropriate security classification considering the impact of improper disclosure.**	Evidence of output in findings.
CSP-ITHC-20 **Remedial Action Plan**	A Remedial Action Plan (RAP) must be built off of the ITHC 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 and added to the relevant Risk Register until they have been mitigated or closed.	Evidence of output in findings. Evidence of Remedial Action Plan.
CSP-ITHC-21 **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. **See also:** NCSP Vulnerability Management Standard.	Evidence of Remedial Action Plan. Evidence of mitigated actions

Reference	Minimum Requirement	Compliance Metric
CSP-ITHC-22 **ITHC Reporting and management of findings**	The SIRO must be provided with a report of findings which articulate the risk in the overall context of the whole IT estate. The report should 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.	Reports provided to SIRO SIRO decision records. Risk registers & treatment plans. Board reports and minutes.
CSP-ITHC-23 **Future testing**	Future testing must include validation that remediations have been satisfactorily resolved. Test scopes should be reflective of threat, environment and organisational changes since the last test.	Tracking of remediations across tests.

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.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

This guidance should be distributed within IT 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.

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

Review Cycle

This guideline 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 guideline 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.)

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Daniel Reed, PDS	Initial Version	08/09/23
0.2	Daniel Reed, PDS	Update from peer review.	29/11/23
0.3	Daniel Reed	Final Version for approval. Incorporating NCPSWG comments.	19/01/24

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	07/02/24

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
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
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021