CYBER STANDARD DOCUMENT

INFORMATION ASSURANCE

ABSTRACT:
This Standard defines the requirements to implement Information Assurance as mandated in the National Community Security Policy.

This document describes the requirements to help 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.

ISSUED	October 2023
PLANNED REVIEW DATE	July 2024
DISTRIBUTION	Community Security Policy Framework Members

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

Members should ensure that they are consulting the currently valid version of the documentation.

COPYRIGHT: Police Digital Service

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial version	05/10/22
0.2	PDS Cyber	Alignment with CIS / NIST / ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	31/03/23
0.3	PDS Cyber	Reworking	24/05/23
0.4	PDS Cyber	Final updates for NCPSWG	15/06/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National approving body	28/09/23

COPYRIGHT: Police Digital Service

Document References

Document Name	Version	Date
Authorised Professional Practice for Information Assurance - link		16/06/20
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
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

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.

Introduction

This standard describes the requirements to fulfil the National Community Security Policy (NCSP) Information Assurance Policy statement. By implementing this standard Forces will be able to demonstrate an effective information assurance and compliance framework and a clear commitment to information security and risk management.

This standard also describes the National Police Cyber Assurance Framework (PCAF).

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard 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).

Audience

This standard is aimed at:

- Member Senior Information Risk Owners (SIROs), Information Security Officers (ISOs), information security practitioners, Information Asset Owners (IAOs.)
- Third parties who act as service providers or suppliers to members.
- Auditors providing assurance services to members.

Scope

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

This Security Assurance Standard applies to police information whether it is locally owned or part of a national police information system.

Requirements

This section details the minimum requirements to implement an effective Information Assurance framework to assure Policing systems and information. Please also refer to the Security Governance Standard.

Reference	Minimum requirement	Control reference	Compliance Metric
1	**Information Security Assurance programme requirements**		
1.1	Provide evidence to stakeholders on the effectiveness of security controls that protect Force / member target environments (e.g. critical operational environments, processes, applications, and supporting technical infrastructure).	ISO 27002:2022 5.35	
1.2	Provide identified audiences (including senior leaders) with a relevant, accurate, comprehensive and coherent assessment of information security performance, so that corrective actions can be taken on a timely, cost-effective basis.	ISO 27002:2022	Annual reporting (e.g. SIRO report) Regular senior leadership reports.
1.3	Ensure security audits are performed using an agreed methodology, can be completed within acceptable timescales and that no audit steps or activities are missed.	ISO 27002:2022 5.35	Agreed published methodology. Audit programme Audit plans, scopes, reports and findings. Management agreed Corrective action plans. Audit closure reports.
1.4	Ensure compliance activities include processes and management systems that support information & cyber risk controls.	ISO 27002:2022 5.35 NIST CSF DE.DP.3	Audit plans, scopes, reports and findings. Management agreed Corrective action plans. Audit closure reports.
1.5	Identify both non-compliances and information risks associated with target environments. Ensure the risks identified during security audits are treated effectively,	ISO 27002:2022 5.35	Audit plans, scopes, reports and findings. Corrective action plans. Audit closure reports.

Reference	Minimum requirement	Control reference	Compliance Metric
	compliance requirements are being met, and agreed security controls are being implemented within agreed timescales.		Risk register with audit findings and management actions.
1.6	Ensure that stakeholders are informed about the risks associated with target environments and enable owners for Corrective actions to be identified and agreed.	ISO 27002:2022 5.35	Regular senior leadership reports.
1.7	Record and monitor compliance using the National PCAF Security Assurance for Policing (SyAP) tool.	ISO 27002:2022 5.35	SyAP assessments completed and current. Regular updates as evidence changes or matures.
2	**Information Systems Assurance**		
2.1	Ensure that the National Systems Development Standard is applied to National policing and critical Force IT systems.		Local system development policy / process. Project plans Statements of assurance. Project Risk registers.
2.2	Ensure on an ongoing basis, that security controls have been implemented effectively, that risk is being adequately managed in accordance with the National Information Risk Framework and to provide the owners of target environments and senior leaders with an independent assessment of their security status.	ISO 27002:2022 5.35	Risk register. Security controls catalogue. Schedule of Control reviews. Corrective action plans. Management reports.
2.3	Implement comprehensive security testing including; Conduct risk based IT Health-checks & vulnerability scanning in target environments in accordance with assurance programmes and vulnerability management standards to	ISO 27002:2022 NIST CSF DE.DP.3	Reports from ITHCs, remediation plans and evidence of remediation.

Reference	Minimum requirement	Control reference	Compliance Metric
	identify security weaknesses. Ensure that test scopes and frequency are commensurate with risk and threat profiles. Undertake a variety of tests including 'black box', Red-team, control based and scenario-based testing to and determine their resilience under attack conditions.		
3	**Physical & Environmental Security**		
3.1	Undertake regular reviews and inspections of physical security controls to critical & sensitive sites and facilities and their supporting infrastructure. Specifically including controls such as automated access controls (AACS), CCTV, intrusion detection and perimeter controls. Consider undertaking random checks regarding access to premises to validate controls and local behaviours (e.g. check for challenge for ID).	ISO 27001:2022 5.35 & 7.1	Schedule of reviews / inspections Finding reports Corrective action plans
3.2	Consider undertaking office security checks such as clear desk, security furniture appropriate use, locked computers etc.		Schedule of reviews / inspections Finding reports Corrective action plans
3.3	Undertake on-site security audit where police networking / IT equipment is in third party accommodation (buildings / offices)		Schedule of audits PASF reports Corrective action plans
4	**Third Party Assurance**		

COPYRIGHT: Police Digital Service

Reference	Minimum requirement	Control reference	Compliance Metric
4.1	Ensure that the National Third-Party Assurance Standard is applied to National policing and critical Force suppliers.	ISO 27001:2022 5.21 & 5.22	Local policy Standard contractual terms
4.2	Undertake Police Assured Secure Facility (PASF) audits of third parties who have access to National Police systems, assets, or critical Force systems.	ISO 27001:2022 5.21	Schedule of audits PASF reports Corrective action plans
4.3	Undertake regular reviews of assets shared with suppliers including the mechanisms by which they are shared.	ISO 27001:2022 5.21 & 5.22	Information Asset Registers Supplier confidentiality / non-disclosure agreements Service reviews

Communication approach

This standard will be communicated as follows:

1. Internal peer review by the members of the National Cyber Policy & Standards Working Group, which includes PDS and representatives from participating forces.

2. Presentation to the NCPSB for approval.

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

For external use (outside PDS), this standard should be distributed with information security officers (ISOs) and Information Management 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.

COPYRIGHT: Police Digital Service

Review Cycle

This Policy 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 policy 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.)