CYBER STANDARDS DOCUMENT

NCSP Security Governance

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

ISSUED	September 2024
PLANNED REVIEW DATE	August 2025
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 for security governance.

Introduction

This standard describes the requirements to fulfil the National Community Security Policy (NCSP) Security Governance Policy statement. By implementing this standard forces, and those delivering IT services on behalf of UK policing, will be able to demonstrate an effective governance framework and a clear commitment to information security and risk management.

The application of this standard supports the delivery of the objectives and outcomes described in the National Policing Cyber Security Strategy.

> Outcome 1 - Policing has established governance arrangements with clear accountability, enabling effective management of cyber risks across all levels of policing.

As part of this, the creation and management of an information security strategy and programme is required.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard helps organisations demonstrate compliance with the following NCSP policy statements:

Security Governance

- To Establish, maintain, and monitor an information security governance framework, which enables Policing's information assurance governing body to set clear direction for, and demonstrate their commitment to, information security and risk management.

- To ensure that the governing body either directly or through its delegated representatives defines the maximum level of risk or impact that Policing is prepared to accept in any given situation, i.e., risk appetite.
- To Support the information security governance framework by creating an information security strategy and implementing an information security programme.

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

1. This standard applies to any member of the Policing Community of Trust. It is also applicable to third parties to the policing community.
2. For the purposes of National Police systems, these are defined as an IT system, infrastructure or application (including Software as a Service (SaaS)) where police information is processed, or where an operational service is provided to police organisations, and the risk is shared across police organisations. This is the definition agreed at the Police Information Assurance Board (PIAB) on the 11th June 2024.
3. This standard should be considered the baseline for information security governance for organisations accessing, handling policing information or providing services to such organisations.

Requirements

This section details the minimum requirements to implement an effective Cyber Security Governance structure to assure Policing systems and information.

Reference	Minimum requirement	Control reference	Compliance Metric
1	**Information Security Governance Framework**		
1.1	Members shall identify and communicate their place in the Community of Trust, recognising the clear link between policing's ability to maintain and improve its own cyber resilience and the achievement of wider policing outcomes and public trust.	NIST CSF ID.BE.2	Records to evidence requirements being met. PCAF assessments.
1.2	A cyber security policy should be in place which is owned by a senior leader. The policy must be regularly reviewed considering organisational and regulatory requirements and changes. The policy must be communicated across all areas of the organisation with regular reminders to all personnel.	NIST CSF ID.GV.1 ID.GV.2 ID.GV.3	Cyber security policy in place owned by senior officer. Regular reviews. Records of communication & reminders.
1.3	A governance framework should be in place describing the overall governance structure inclusive of cyber security roles and responsibilities aligned with internal and external roles (The National Community Security Policy Framework serves this purpose at a National Level and can be referenced by Forces). This should be supported by a strategy and delivery programme which encompasses the alignment of physical, cyber and information security requirements of National policing. The local information security governance framework shall be owned by the Chief Officer Group / Board, who provide leadership in its delivery and effectiveness – the information security board.	NIST CSF ID.GV.2 ISO 27001:2022 5.01	Cyber security policy in place owned by senior officer. Regular reviews. PCAF review.

Reference	Minimum requirement	Control reference	Compliance Metric
	The board should evidence their commitment by exercising their authority and direction over the framework, strategy, programme and policies.		
2	**Strategy and Programme**		
2.1	Aligned to the National NPCC Cyber Security Strategy, a cyber security vision shall be in place which includes missions, objectives, and activities to deliver them. A process shall be in place to set, review and prioritise these on a regular basis. The cyber security vision will be communicated across all areas of the organisation.	NIST CSF ID.BE.1 ID.BE.2 ID.BE.3	Records to evidence requirements being met.
2.2	A senior role must be assigned the mission and resources to coordinate, develop, implement, and maintain the organisation wide cyber security program. See also NCSP Security Management standard	NIST CSF ID.BE.2	Senior role assigned. Role description includes responsibilities.
2.3	Cyber and information security documentation shall be regularly reviewed and updated to ensure it meets the needs of the organisation and effectively meets the strategic vision and objectives.	NIST CSF ID.BE.3	Records to evidence requirements being met.
2.4	The cyber security policy shall include guidance for privacy and civil liberties. A programme of improvements shall take account of legal and National requirements or changes and address compliance gaps. Senior management should be appraised regularly so that they understand requirements and impacts.	NIST CSF ID.GV.3 ID.DV.1 ISO 27001 A.5.1.1	Records to evidence requirements being met.
2.5	Processes should include appropriate contact and escalation with National Policing bodies with regards to compliance issues and security events.	NIST CSF ID.BE.2 ISO 27001	Records to evidence requirements being met.
2.6	The status and performance of the Cyber security programme shall be assessed and reported to the information security board or equivalent on a regular basis.	NIST CSF ID.BE.3 ISF SG1.2	Meeting minutes. Report records.

Reference	Minimum requirement	Control reference	Compliance Metric
3	**Risk Management**		
3.1	The cyber security programme shall be focussed upon managing and reviewing cyber risks and supporting the National Information Risk Management Framework.	NIST CSF ID.GV.4 ISF SG1.3	Programme in place and reviewed. Risk register or similar with evidence of risk management practices.
3.2	The management of cyber risks will consider National Policing and Force objectives. See the definition of National police systems described in the scope above.	NIST CSF ID.RM.1 -3	Records to evidence requirements being met.
3.3	Cyber risk shall be considered alongside other organisational risks as part of risk management during operations, projects and change initiatives.	NIST CSF ID.RM.1 -3	Records to evidence requirements being met.
3.4	In line with the National Information Risk Framework, risk management processes must be in place. Risk appetite shall be communicated appropriately to enable effective risk management. A process shall be in place to review and handle exceptions or accepting risks above the agreed risk appetite. This should include risk balance cases and risk treatment plans with defined timed, objectives.	NIST CSF ID.RM.2 ISF SG1.3	Records to evidence requirements being met.
3.5	The National Community Security Policy applies and needs to be supported by local policies, standards or procedures which must be regularly reviewed and have defined responsibilities supported by processes, resources, and metrics.	NIST CSF ID.RM.1 ISF SG1.2	Cyber security policy in place owned by senior officer. Regular reviews. Evidence of supporting processes.
3.6	The information risk governance structure aligned to the National Information Risk Management Framework shall be in place for reporting and owning cyber risks.	NIST CSF ID.GV.4 & ID.RM.1	Records to evidence requirements being met.

Reference	Minimum requirement	Control reference	Compliance Metric
3.7	There shall be a clear approach to consistently identify, assess, record and manage cyber risks across the organisation. This can be achieved through effective communication and the use of a risk management tool across the organisation.	NIST CSF ID.GV.4 & ID.RM.1	Records to evidence requirements being met. These will include threat & vulnerability and business impact assessments.
3.8	The performance of cyber risk management shall be reported and monitored by senior management on a regular basis.	NIST CSF ID.GV.4 & ID.RM.1 ISF SG1.2	Meeting minutes. Report records.

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.

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.)

Document Information

Document Location

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

Revision History

Version	Author	Description	Date
1.0	PDS Cyber	Initial approved version	28/09/23
1.1	PDS Cyber	Annual refresh and port to 2024 template	

Approvals

Version	Name	Role	Date
1.1	National Cyber Policy & Standards Board	National approving authority	26/09/24

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
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021