CYBER STANDARDS DOCUMENT

Third Party Assurance for Policing (TPAP)

ABSTRACT:
This Standard is to ensure that all third party suppliers are examined to fully understand their overall security posture and how that may impact upon Policing, ensure they fully understand the responsibilities they have in looking after policing data, that elements such as the importance of vetting and the cyber security of their systems is understood and they are aware of the requirements when handling and communicating that data.

ISSUED	May 2023
PLANNED REVIEW DATE	March 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	16/02/23
0.2	PDS Cyber	Internal initial peer review	09/03/23
0.3	PDS Cyber	For review by NCPSWG	10/03/23
0.4	PDS Cyber	Following initial NCPSWG reviews	17/04/23

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	25/05/23

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
NIST Cyber Security Framework	v1.1	04/2018

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

Policing has a requirement to ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers and third parties (including organisations in the supply chain).
This standard is intended to describe the requirements for a third party security management framework and to embed information security requirements into both the procurement process and formal third party contracts.
An example Third Party Assurance Process (TPAP) is included to inform Community Members' in their own implementation of this standard.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to describe the requirements to ensure that all third party are examined to fully understand their overall security posture to enable risk owners to take informed decisions during procurement activities.

It is important to define security requirements for products and services provided by external suppliers and specify how they will be met. This enables third parties to be risk assessed prior to engagement and as an ongoing assurance activity throughout the life of the engagement.

Defined security requirements provides transparency so that third parties fully understand their responsibilities.

Audience

This standard is aimed at:

- Staff across PDS and policing who are responsible for the selection, appointment or review of third parties either on behalf of National Policing or at a local force level.
- Information & Cyber risk practitioners and managers.
- Information Asset Owners (IAOs) and Senior Information Risk Owners (SIROs.)
- Any member of the Policing Community of Trust who may be engaged in the consumption or supply of a service to National or local policing.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors providing assurance services to PDS or policing.

Scope

1. The standard is applicable to all third parties to policing. This includes commercial and non-commercial organisations.
2. This includes suppliers providing services to members of the community of trust directly or those providing systems and/or services to Policing where PDS has responsibility for the information and Cyber assurance of those systems and/or services.

Requirements

1. Third parties should be required to undergo a structured security assessment as part of the tendering process. This should be stated at the beginning of any tendering / procurement activity.
2. The process should:

    - Provide a robust base upon which assurance of any specific service can be made.
    - Allow National Policing and force / member assurers to be aware of any non-compliances by a third party and decide if these are necessary for the security of the service.
    - Allow National Policing assurers or forces / members where there are non-compliances to either deselect bidders in a tendering process, risk assess any non-compliances where this is not necessary or possible and monitor and put mitigations in place where needed.
    - Allow National Policing assurers and forces to audit non-police users of policing services and ensure a common standard of operational security and awareness.

3. The following requirements help members of the Policing Community of Trust meet the needs of National Community Security Policy (NCSP.)

Reference	Minimum requirement	Control reference	Example Compliance Metric
TP 1.1	Ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers (including organisations in the supply chain).	*ISF SOGP SC1.1* *ISO 27001 15.1.1*	*Supplier assurance process in place, Risk register reflects identified / managed risks.*
TP 1.2	Identify and employ only those external suppliers that adequately meet security requirements.	*ISF SOGP SC1.2*	*Supplier assurance process in place, Security requirements in place. Records of third party reviews against requirements. Records of decisions re third parties. Risk register reflects identified / managed risks.*
TP 1.3	Define security requirements for products and services provided by external suppliers and specify how they will be met.	*ISF SOGP SC1.3* *ISO 27001 15.1.1*	
TP 1.4	Provide assurance that external suppliers are meeting security requirements.	*ISF SOGP SC1.4* *ISO 27001 15.1.1*	
TP 1.6	Ensure all necessary security arrangements are implemented for the use of cloud services, and that information risks are managed in cloud environments.	*ISF SOGP SC2.1*	*Records of all cloud service third parties and risk assessments & reviews undertaken.*
TP 1.7	Address weak or insufficient cloud security controls and help the organisation use cloud services securely in a heterogeneous, multi-cloud environment.	*ISF SOGP SC2.2*	*Risk register reflects identified / managed risks.*
TP 1.8	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	*NIST CSF ID.AM.6*	*Records including contract statements / clauses.*
TP 1.9	The organization's role in the supply chain is identified and communicated	*NIST CSF ID.BE.1*	

COPYRIGHT: Police Digital Service

Reference	Minimum requirement	Control reference	Example Compliance Metric
TP 2.0	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	*NIST CSF ID.GV.2*	*Records including contract statements / clauses.*
TP 2.1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders Third parties will often not be fully compliant with every requirement, even after consultation with them. The contract service manager needs to consult with the Information Asset Owner (IAO) to decide whether the non-compliances are within risk appetite and can be managed as risk cases or not. These risk cases may need to be presented to the Senior Information Risk Owner (SIRO) as required to consider whether the supplier fails the assessment.	*NIST CSF ID.SC.1*	*Supplier assurance process in place,* *Records of decisions re third parties.* *Risk register reflects identified / managed risks.*
TP 2.2	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed. Third parties should be assessed in context as not all questions may be relevant for every service. Individual services to be performed may have particular requirements and third parties nominally of one rating may have additional requirements placed upon them. This should be done in consultation with the assurance manager, for the system, service manager or person who has the best understanding of the risk environment for the service.	*NIST CSF ID.SC.2* *ISO 27001 15.1.2, 15.1.3*	*Supplier assurance process in place,* *Records of decisions*

COPYRIGHT: Police Digital Service

Reference	Minimum requirement	Control reference	Example Compliance Metric
	For example addition of an in person audit or a Police Assured Secure Facilities (PASF) audit may be required.		
TP 2.3	Risks should be assessed using a cyber supply chain risk assessment process that covers the following areas (aligned to the NCSP headings): • Security Governance • Information Risk Assessment • Security Management • People Management • Information Management • Physical Asset Management • System Development • Application Management • System Access • System Management • Networks and Communications • Third Party Management • Technical Security Management • Threat and Incident Management • Physical & Environmental Management • Business Continuity • Information Assurance	*NIST CSF ID.SC.2* *ISO 27001 15.1.2, 15.1.3*	*Supplier assurance process in place,* *Records of assessments* *Records of decisions re third parties.* *Risk register reflects identified / managed risks.*
TP 2.4	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	*NIST CSF ID.SC.3* *ISO 27001 15.1.2, 15.1.3*	*Records including contract statements / clauses.*
TP 2.5	Upon selection, contracts shall incorporate agreed measurable security requirements or key performance indicators to ensure continuous monitoring and review.	*NIST CSF ID.SC.4* *ISO 27001 15.2.1, 15.2.2*	*Key Performance Indicators / Metrics and reviews in contracts.*

Reference	Minimum requirement	Control reference	Example Compliance Metric
TP 2.6	Security points of contact shall be established with the contracted third party to enable regular dialogue to support reviews, performance monitoring and escalation of issues.	*NIST CSF ID.AM.6* *ISO 27001 15.1.2*	*Records including contract statements / clauses.*
TP 2.7	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.		*Supplier assurance process in place,* *Records of assessments* *Records of decisions re third parties.* *Risk register reflects identified / managed risks.*
TP 2.8	Contracts should include a requirement of the third party to inform the contracting authority of any security event, incident or breach that relates to the contract regardless of whether it has a material effect.	*NIST CSF PR.AT.3* *NIST CSF ID.GV.2* *ISO 27001 15.1.1*	*Records including contract statements / clauses.* *Records of notifications.*
TP 2.9	Response and recovery planning and testing are conducted with suppliers and third-party providers.	*NIST CSF ID.SC.5*	*Records of tests / exercises* *Records of findings or learning including risks identified.*
TP 2.10	Third-party stakeholders (suppliers, customers, partners) understand their roles and responsibilities.	*NIST CSF PR.AT.3*	*Records including contract statements / clauses.*

Communication approach

This standard will be communicated as follows:

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

2. Presentation to the Nation Cyber Policy & Standards Board (NCPSB) for approval.

3. Formal publication and external distribution to Policing Community and associated bodies.

For external use (outside PDS), this standard should be distributed with procurement, business change and Information Security 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 member 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.

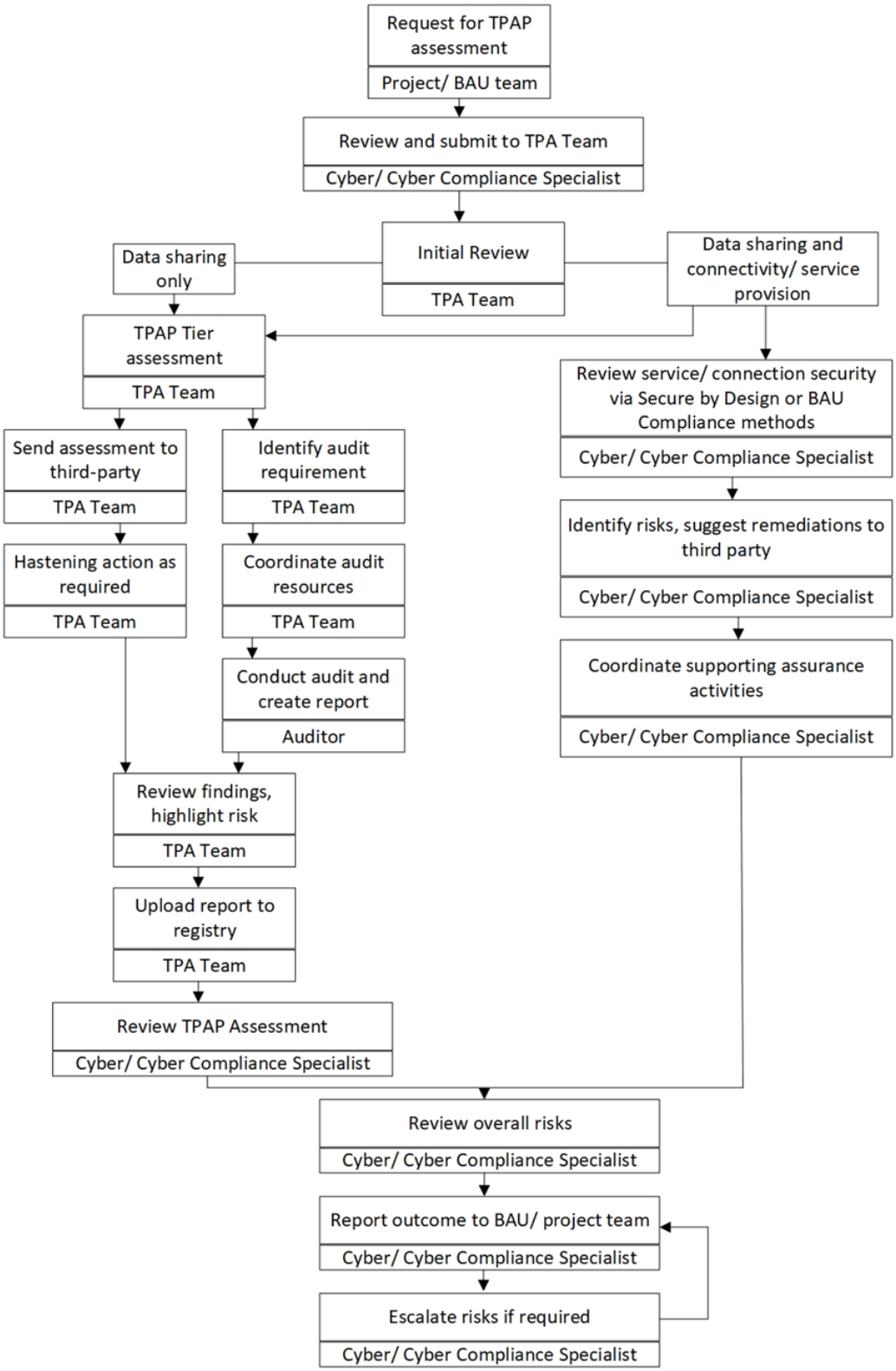
Review Cycle

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 policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

Equality Impact Assessment

Annex A – Example: PDS TPAP – Third Party Assurance Process



COPYRIGHT: Police Digital Service