CYBER STANDARDS DOCUMENT

Physical and Environmental Security Management Standard

ABSTRACT:
This Standard sets out the Physical and Environmental Security measures and considerations to be used within policing. This standard will outline key guidance and advice that should be acknowledged and referred to, and where practicably possible, implemented to safeguard Policing locations including the assets within them.

ISSUED	March 2024
PLANNED REVIEW DATE	January 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....3
Introduction....3
Owner....3
Purpose....4
Audience....4
Scope....4
Requirements....5
Communication approach....17
Review Cycle....17
Document Compliance Requirements....17
Equality Impact Assessment....17
Appendix A – Security Roles and Responsibilities....18
Appendix B – NPSA PSRM process....19
Appendix C – NPSA STaMP Methodology....20
Appendix D – Terms and Abbreviations....22
Document Information....32
Document Location....32
Revision History....32
Approvals....32
Document References....33

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 associated with Physical and Environmental Security.

Introduction

This Standard is intended to provide a baseline for best practices and guidance towards Physical and Environmental Security. This pillar of security is a specialism in its own field and requires those with the remit and responsibility of securing assets within, or the structure itself, to ensure they have considered all aspects associated with safeguarding that asset, and liaised with all associated Stakeholders.

Whilst this is a National Policing Standard it should be noted that specialised advice and guidance is collated and often referenced to specialist UK Technical Authorities including the National Protective Security Authority (NPSA – formerly CPNI), National Cyber Security Centre (NCSC), National Authority for Counter Eavesdropping (NACE) and the official Police security initiative, Secured by Design (SBD).

This Standard will highlight risk management techniques and methodologies that should be used in the physical assessment of any asset, or structure that contains an asset, to identify the threat and risks and commensurate mitigations.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this Standard is to:

- Empower policing colleagues and partners to be confident in assessing the physical security of their sites/assets.
- Provide an understanding of the risk methodologies and processes that should be used to ensure that a thorough physical assessment of assets (in conjunction with other pillars of security) is conducted.
- Understand physical security considerations and measures to undertake where required.
- Align with UK Technical Authority guidance and best practices.
- Adherence to recognised Standards such as ISO 27001/2.

Audience

The Standard is aimed at:

- Information Security and Assurance Professionals who have a remit to manage and assess UK Policing locations and assets.
- UK police force end-users, and in particular local Information Security and Assurance teams, who have a remit to manage and assess UK policing locations and assets.
- The user community, including suppliers, with remit of storing and/or processing UK policing data.

Scope

1. This standard is applicable when required to assess the physical security measures associated with a location and/or the containment of any asset.
2. This standard should be used to help understand the threats and risks associated to an asset and/or physical location housing that asset.
3. This standard should be considered as the baseline for Physical and Environmental security and may be supported by other assessments and/or compliance obligations already in operation.
4. The application of this standards requirements should be done so with consultation of Force-specific teams such as Design Out Crime Officers (DOCOs), Counter Terrorism Security Advisors (CTSAs), and Regional Organised Crime Unit (ROCU) Operational Security Advisors (OpSys).

Requirements

This Section details the requirements that this standard aims to deliver regarding the protection of policing assets from a Physical and Environmental Security standpoint. The minimum requirements outlined below are a baseline which should be adopted and put in place; where commensurate and viable these should be extended upon to enhance the physical security of your estate.

Reference	Minimum Requirement	Control Reference	Compliance Metric
1	**Security Governance**		
1.1	Roles and responsibilities must be distinguished and outlined to ensure that a clear definition and ownership of information security duties and responsibilities can be understood. This should include Senior Officers and Executives from whom must own the overall risk position, to the individuals or teams performing the activities. Please see Appendix A – Security Roles and Responsibilities for a prospective structure of local Force roles.	**ISO 27001 ref:** Annex 5.2 Annex 5.4 **ISF SOGP ref:** SG1.1 SG1.2 SG1.3 **NIST CSF ref:** ID.GV-1 ID.GV-2 ID.GV-4	Information Security Policy, formal governance structure with RACI of defined roles.
1.2	Ensure security threats and risks are regularly reviewed and recorded in a formal setting. This will enable those accountable for security risk to make informed decisions and ensure corporate memory.		Board minutes, risk registers, audit reports.
2	**Physical Security Assessment**		
2.1	An appropriate risk assessment methodology should be chosen to assess and record the physical security of sites and assets.	**ISO 27001 ref:** Annex 5.2 **ISF SOGP ref:** IR1.1 IR1.2 IR1.3	Information Security Policy, Risk Management Strategy, previous risk assessments.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	This will allow consistency in risk assessment activities and provides a benchmark for future assessments. Example risk methodologies: • ISO 27005 • NPSAs PSRM [Appendix B] • NPSAs STaMP [Appendix C] • NCSC Risk Management • C-MAT • STRIDE	IR2.1 IR2.5 **NIST CSF ref:** ID.GV-4 ID.RA-5 ID.RA-6 ID.RM-1 ID.RM-2	
2.2	An accurate and up-to-date asset inventory must be in place detailing organisational assets and information systems, including physical buildings and offices, and data processed at those sites. This should be managed, maintained, and reviewed appropriately with a minimum target of annually. The NPSAs Asset Identification Guide is a valuable guidance document to consider when producing an asset inventory.	**ISO 27001 ref:** Annex 5.9 Annex 5.12 **ISF SOGP ref:** PE2.1 PE2.2 PE2.3 **NIST CSF ref:** ID.GV-4 ID.RM-1	Asset inventory, site assessment reports, Business Continuity and Disaster Recovery Plans, SOC 1 and SOC 2 reports (where applicable).
2.3	The criticality of each site and the assets they contain should be categorized in priority order and their purpose must be fully understood. By knowing what data is processed within the site or asset will help determine the importance and value it	**ISO 27001 ref:** Annex 5.9 Annex 5.12 **ISF SOGP ref:** IR2.2 PE1.1 PE1.2 PE1.3	Asset inventory, site assessment reports, past BIAs, Business Continuity and Disaster Recovery Plans.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	may have to your organisation, and to a threat actor. This can be achieved by conducting a Business Impact Assessment (BIA) on these locations / assets to understand impact to the organisation in the event of compromise or disruption.	PE1.4 **NIST CSF ref:** ID.RA-4 ID.BE-2	
2.4	A threat assessment should be undertaken to establish what threats to UK Policing and Government exist.	**ISO 27001 ref:** Annex 5.7 **ISF SOGP ref:** IR2.3 IR2.4 PM1.5 **NIST CSF ref:** ID.RA-2 ID.RA-3 **CIS v8 ref:** 16.1	NMC threat intel reports, NPSA quarterly threat reports, NCSC threat reports
2.5	Consideration of different attack types should be made. Whilst the threat and risk of physical attacks still remain, trends have identified that the most likely attack vector will be a surreptitious one i.e. attempt(s) to gain access to assets without alerting the owner, custodians or users. For specialised guidance on National Security Threats it is recommend to visit the NPSA website or contact your	-	Performance of NPSA PSRM and/or STaMP assessment.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	liaison officer. In addition – please refer to Appendix C: NPSA STaMP Methodology for further information on assessing against surreptitious threats.		
2.6	The inherent risk position produced as part of any physical security assessment should be recorded and reported in-line with your Force governance streams. The respective risk owners i.e. IAO and/or SIRO, should be briefed of any risks identified and the potential impact they would have on Force assets and any operations if those risks were realised.	**ISO 27001 ref:** Annex 5.2 Annex 5.4 **ISF SOGP ref:** SG1.1 SG1.2 SG1.3 **NIST CSF ref:** ID.GV-1 ID.GV-2 ID.GV-4	Information Security Policy, Board minutes, risk registers, audit reports.
3	**Physical Security Mitigations and Processes**		
3.1	Commensurate mitigations should be considered when reviewing the output of a physical security assessment in conjunction with the NPSA Catalogue of Security Equipment (CSE). When selecting mitigation measures, it is important that a defence in depth approach is taken. For surreptitious threats these layers would be from the inside out and for physical threats from the outside in. It is important to understand that multiple layers of the same controls does not offer the same level of	**ISO 27001 ref:** Annex 7.1 Annex 7.2 Annex 7.3 Annex 7.4 Annex 7.5	Information Security Policy, Force risk register, risk assessment artefacts incl control mapping documents to a specific risk framework.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	surreptitious protection as multiple layers of differing controls. The more diverse the security mitigations are throughout the layers, the greater the assurance they provide, due to the diversity of skills needed by the attacker to successfully surreptitiously attack an asset. Please refer to Appendix C: NPSA STaMP Methodology and NPSA asset protection guidance for further information on asset mitigation layering.	Annex 7.6 Annex 7.7 Annex 7.8 Annex 7.9 Annex 7.10 Annex 7.11 Annex 7.12 Annex 7.13 Annex 7.14 **ISF SOGP ref:** IR2.6 PE1.1 PE1.2 PE1.3 PE1.4 PE2.1 PE2.2 PE2.3 **NIST CSF ref:** DE.CM-2 DE.CM-7 PR.AC-2 PR.PT-5	
3.2	Any technology to be introduced to support your physical security or controls must be subject to a cyber risk assessment, including assessment of the Vendor providing the solution. It is recommended to review the National Policing TPAP Standard and NPSAs Supply Chain guidance for detail on Supply Chain management and assurance. Early communication with your Information Security team(s) is vital in ensuring a unified approach, and the avoidance of delays in mitigation installations. The NPSA's CSE physical / surreptitious products and Cyber Assurance of Physical Security Systems (CAPSS) Standard can be used with confidence that any physical, software and hardware security solutions that are in		Information Security Policy, Risk Management Strategy Force risk register, risk assessment artefacts, CAPSS products on CSE.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	place, or are considering, have strong and effective physical and cyber mitigations at the core of their development and operation.		
3.3	Commensurate and layered physical security defences should be in place across the various locations within your estate to mitigate unauthorised physical and surreptitious access to Policing information or equipment. Mitigation measures which support this requirement include (but not limited to): • Mechanisms for managing entry to locations i.e. security trained staffed receptions, Automatic Access Control Systems (AACS). • Installation of physical barriers to control authorised and public pedestrian and vehicle traffic, with consideration to the installation of Hostile Vehicle Mitigations (HVMs) if appropriate. • Comprehensive CCTV coverage with robust reviewing process especially for those helping to secure sensitive or critical assets. • Segregated network for security operations and data, passed to a centralise monitoring centre i.e. guard house.	**ISO 27001 ref:** Annex 7.1 Annex 7.2 Annex 7.3 **ISF SOGP ref:** PE1.1 PE1.2 PE1.3 PE1.4 PE2.3 **NIST CSF ref:** DE.CM-2 PR.AC-2	External audit report, physical penetration test (internal or external), access and visitor records.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Intruder Detection Systems (IDS) for sensitive and/or non-staffed areas. • Physical segregation of sensitive assets from publicly populated areas.		
3.4	A monitoring and alerting system should be in place to continuously monitor access to restricted areas that store sensitive information or critical assets. Any monitoring system in place should be regularly checked to ensure full functionality and no unauthorised access, so if required it can be used for investigatory purposes. The monitoring system should be protected from remote disabling attacks, and any console or control panel should be located in an environment which has either 24/7 staffing or IDS. Where appropriate it is recommended that tamper-proof seals (or equivalent) are utilised.	**ISO 27001 ref:** Annex 7.4 **ISF SOGP ref:** PE1.2 PE1.3 PE1.4 PE2.3 **NIST CSF ref:** DE.CM-2 DE.CM-7 PR.AC-2 PR.PT-5	External audit report, physical penetration test (internal or external).
3.5	Processes, procedures and training for all staff that work within secure areas must be in place. These will define what can, and cannot, be conducted or taken into those areas. A register should be maintained of any documents brought in or out of the secured area; this is extended to the reproduction of said documents.	**ISO 27001 ref:** Annex 7.6 Annex 7.7 **ISF SOGP ref:** PE1.1 PE1.2 PE1.3 PE1.4 PE2.1 PE2.3	Information Security Policy, Working in Secure Areas Policy, access register, visitor records.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	The threats, risks and/or classification of the secure area will define what (if any) corporate and/or personal devices are to be allowed within that area(s). Contingencies may be required for the secure storage of devices externally to the secure area and in a way that devices cannot provide unauthorised monitoring of the secure area e.g. STRAP conditions may be applied.	**NIST CSF ref:** DE.CM-2 DE.CM-7 PR.AC-2 PR.PT-5	
3.6	Supporting utilities, cabling and equipment involved in the operation and maintenance of information assets must be afforded the same level of physical protection as the assets, as well as mitigation from disruption or unexpected outages. Protective measures that should be taken (but not limited to) are: • Identification of key utilities and equipment. • Cabling should be armoured to prevent malicious or accidental cuts. • Regular maintenance and audit of utilities and equipment. • Regular cable inspections and technical sweeps should be conducted to ensure no unauthorised devices are connected to the cables. • Separate management network for utilities control, with isolation from internet or corporate networks.	**ISO 27001 ref:** Annex 7.11 Annex 7.12 Annex 7.13 **ISF SOGP ref:** PE1.1 PE1.2 PE1.3 PE1.4 PE2.3 **NIST CSF ref:** PR.AC-2 PR.PT-5	Business Continuity and Disaster Recovery Plans, emergency response plans, test drills, regular maintenance reports, external audit report, physical penetration test (internal or external).

Reference	Minimum Requirement	Control Reference	Compliance Metric
	• Backup generators/power to support any outage. Please refer to the National Policing Business Continuity Standard for more information.		
3.7	A building decommissioning process should be established for the scenario of a working area being taken out of operation and/or removed from your estate. It is recommended that a suitable search exercise is undertaken in-line with any decommissioning process. This may be undertaken by specialists within, or attached to, Force such PoISA operatives CTSAs or OpSys. Physical security controls must be removed when no longer required, and/or when closing down a premise. Keeping sensitive controls in place after you have vacated the premises may allow unauthorised personnel insight into knowing the gradings of equipment used to protect Policing assets. Please refer to the *National Policing Physical Asset Management Standard* and NPSA guidance for more information on secure disposal, destruction, and decommissioning.	**ISO 27001 ref:** Annex 7.14 **ISF SOGP ref:** PE1.2 PE1.3 PE2.3 **NIST CSF ref:** PR.AC-2 PR.PT-5 PR.DS-3 PR.DS-5 PR.IP-6	NIST 800-88, NPSA Secure Destruction Policy, asset inventory, security assessments, external audit reports, destruction certificate evidencing compliance legal and regulatory requirements.
3.8	All introduced security mitigations must be certified to the relevant		Internal and External audits,

Reference	Minimum Requirement	Control Reference	Compliance Metric
	grading for protecting assets of respective classification. Examples include: • PAS24:2022: external doors, windows, and associated entry mechanisms. • PAS68/PAS69: impact testing of vehicle security barriers. • BS EN 1063: bullet-resistant glass. • Products should be purchased from Secured by Design members, especially where applicable to "Police Preferred Specification". • Apex Templar series: sensitive material should be stored within rated cabinets. • BS EN 50131: wired and wire-free intruder alarm systems. The NPSA's Catalogue of Security Equipment (CSE) and Manual Forced Entry Standard (MFES) is available to help security practitioners to identify appropriate physical security equipment. Furthermore, it is recommended using the NPSA's Forced Entry Protection guidance in parallel with the MFES; this enables security practitioners to compare the most widely used Standards for forced entry protection based on the threat they are aiming to protect against i.e. EN 1627-2021,	-	physical security review, compliance reports conducted during site visits, control mapping documents to a specific risk framework.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	LPS1175 issue 8, LPS2081 issue 1, PAS 24 2022, MTAS.		
3.9	It is noted that whatever mitigations are put in place the risks identified within the physical security risk assessment cannot be removed in their entirety. It is therefore vital that a layered security approach is applied which delays physical or surreptitious threat actors to enable the security response. It is recommended to review Appendix C: NPSA STaMP Methodology and the NPSAs Marauding Terrorist Attack (MTA) guidance to get further information on delays a control i.e. barrier, can afford against specific attacks.	-	Risk assessment documentation, stress tests of controls, risk acceptance records and decision justifications.
4	**Continuous Improvement and Management**		
4.1	The outputs of all risk management activities should be recorded on the sites/corporate risk register and reported to Senior Management for review, insight, and where applicable, decisions.	**ISO 27001 ref:** Annex 5.2 Annex 5.4 **ISF SOGP ref:** SG1.1 SG1.2 SG1.3 **NIST CSF ref:** ID.GV-1 ID.GV-2 ID.GV-4	Risk reports including executive summary and risk treatment plans, briefing reports, Board minutes.
4.2	Review dates and cycles should be recorded on the sites/corporate risk register and agreed with Senior	-	Board minutes and decision reports.

Reference	Minimum Requirement	Control Reference	Compliance Metric
	Management, along with a commitment to achieve these.		
4.3	Any changes to threat and business practices, as well as major changes to locations assessed, or changes that may impact assets within, should result in a re-assessment, where viable, to ensure the risk position is still accurate.	**ISO 27001 ref:** Annex 5.2 Annex 5.4 **ISF SOGP ref:** BC1.4 **NIST CSF ref:** DE.CM-2	Change Advisory Board, risk assessment artefacts, Threat intel reports.
4.4	When considering the appropriateness of storing data at external locations, it is important to understand if those sites have been audited and/or assessed for processing Policing data. Engagement with PDS Compliance to understand any TPAP process undertaken or if that site has received a PASF (or equivalent) is vital. Please refer to the National Policing TPAP Standard for further information.	**ISO 27001 ref:** Annex 5.2 Annex 5.19 Annex 5.20 **ISF SOGP ref:** SC1.1 SC1.2 SC1.3 SC1.4 SC2.1 SC2.2 **NIST CSF ref:** ID.SC-3 PR.AT-3	PDS TPAP process, PASF register, Supplier certifications and accreditations, SOC 1 and SOC 2 reports (where applicable).

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.

For external use, this Standard should be distributed within associated teams e.g. Information Security and Assurance, Design Out Crime Units (DOCUs) etc, to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with Force SIROs / Security Management Forums and Boards. Consideration should also be given to raising awareness amongst Force personnel of the implementation of this Standard where it may affect them.

This Physical and Environmental Security Standard should be used in conjunction with any security assessments being undertaken on/for Policing locations and assets to ensure all Physical Security best practices are acknowledged and considered when assessing to understand their risk maturity or position.

Measurables generated by adopting this Standard can also form part of your internal Cyber Management and Physical Security reporting governance.

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.)

Appendices

Appendix A – Security Roles and Responsibilities

The following bodies and individuals (and local Force alternatives) will have key responsibilities in your local risk management structure:

- **Senior Information Risk Owner (SIRO):** The senior risk owner for your local Force's policing systems and data. The key duties and responsibilities of the NSIRO are outlined within the SIRO Handbook, published by the NPCC.
- **Strategic Information Management Board (SIMB):** This forum may differ per Force however it is traditionally a formal Board that provides a strategic overview of risk across Force and manages the local Force's Information Management (incl Security) Risk Register.
- **Information Asset Owner (IAO):** The risk owners responsible for local Force's individual systems and/or data sets. The key duties and responsibilities of IAOs are outlined within the IAO Handbook, published by the NPCC.
- **Information Security Officer (ISO):** The individual responsible for the security, governance, and compliance of information assets within Force. This individual will cover a range of duties but most notably undertake security assessment and risk management activities.
- **Operational Security Advisor (OpSy):** The individual, either within Force or as part of local ROCU, whose objective is to monitor and reduce operational security risk. They will be responsible for maintaining consistency in standards of security and practice in accordance with legislation, national guidelines, local security policy, and working in conjunction with operational partners (e.g. NCA).
- **Counter Terrorism Security Advisor (CTSA):** The individual, either within Force or as part of local CTU, whose primary role is to provide advice and guidance on all aspects of counter terrorism protective security to specified industry sectors. They are specialists in physical security assessments and responsible for the provision of protective security advice to publicly accessible locations, local authorities, and local businesses to identify and assess sites that may be vulnerable to terrorist attack.

Appendix B – NPSA PSRM process

The NPSA's Protective Security Risk Management (PSRM) methodology is an established and trusted risk framework used for the assessment for physical security, personnel and cyber security including surreptitious threats and Marauding Terrorist Attacks (MTAs). That said, this methodology does outline key principles which can be transferred for other security assessments including cyber and personnel.

The below diagram denotes the 8 steps associated with the PSRM process:

Whilst the PSRM is a holistic approach to risk assessment, it does emphasise the importance of ensuring you understand and label your assets to which you can then scope the assessment you wish to undertake. Often this is an area that is overlooked during the risk assessment process but with Steps 1 and 2 focused solely on assets, it enables a clear direction of your assessment from the very start.

Appendix C – NPSA STaMP Methodology

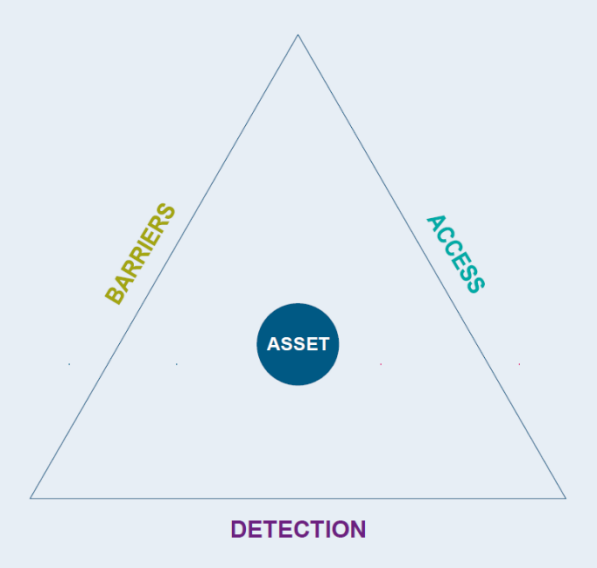
The NPSA's Surreptitious Threat Mitigation Process (STaMP) replaced the CPNI Classified Material Assessment Tool (CMAT), and was developed to support owners, custodians and users of classified material and holders of sensitive assets to determine whether their current or proposed physical security arrangements are adequate to protect, detect and effectively mitigate unauthorised access, from a range of surreptitious threat actors.

STaMP provides a structured method for benchmarking both existing and proposed physical protective security measures against the level of security deemed appropriate for the classification of material being held, under the prevailing threats.

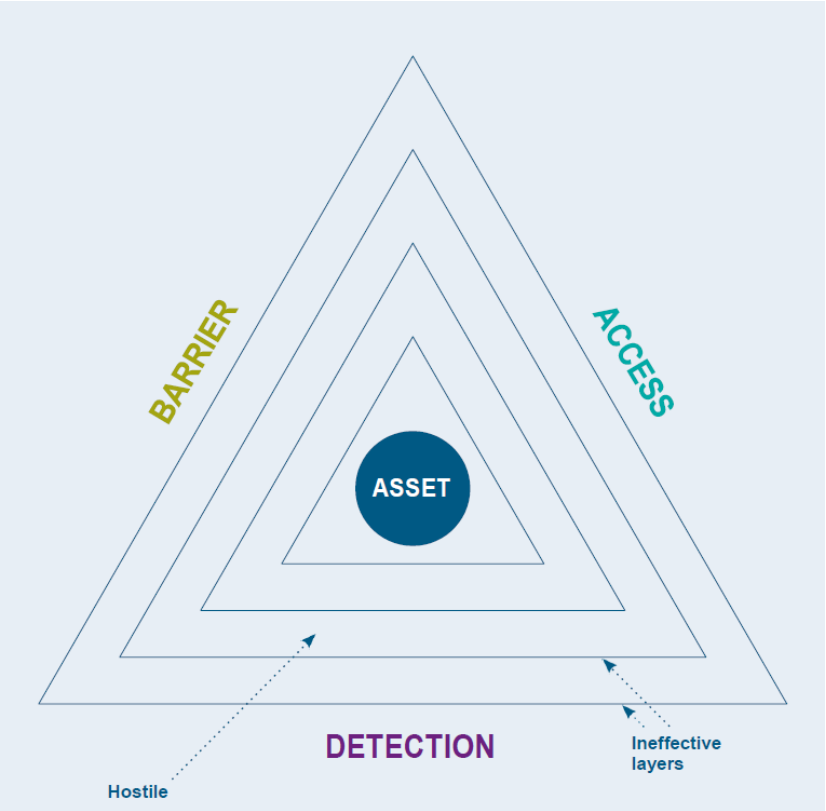
STaMP is a methodology that uses a layered, defence in depth approach to risk assessing threat vectors of a surreptitious nature. To do this it applies a concept that an effective control layer is based off three distinct elements:

1. Implementing effective Barriers
2. Controlling Access
3. Detection of attacks

The unison of these three elements will then form an effective protective security layer; any missing element or a weakness to one of them, the layer is compromised and thus deemed ineffective. The below diagram outlines the layer approach:



A key aspect to STaMP is that it applies the first protective layer as close to the asset you seek to protect and then works outward; the rationale for this being **1)** the closer the protective layer to the asset gives you greater control over *access* and a greater certainty when looking to *detect* attacks, and **2)** is to assume the threat actor(s) has an element of access within your organisation already thus any control layers further from the asset are deemed to be ineffective [denoted below]:



Appendix D – Terms and Abbreviations

Term	Abbreviation	Brief Explanation
Automatic Access Control Systems	AACS	This is the control panel, a form of decision maker. It is on this panel, or software, that the decision to allow entry is made. It is here that permissions are granted, where individuals are enrolled onto the system and given the rules of entry; for example, where they are allowed to enter and when.
Business Impact Assessment	BIA	A BIA is conducted, as part of an assurance process, to identify information assets and their value. It provides an essential snapshot of the direct impacts that any loss or breach of confidentiality, integrity or availability would have on the business and its ability to carry out core functions, prior to mitigating controls and processes being implemented. The likely and worst case impacts of compromise against each information asset should be considered and agreed.
British Standards Institute	BSI	The national standards body of the United Kingdom. BSI produces technical standards on a wide range of products and services and also supplies certification and standards-related services to businesses.
Cyber Assurance of Physical Security Systems	CAPSS	A programme within NPSA that covers both physical and cyber security. CAPSS is about gaining confidence in the 'cyber' elements of electronic security products which, while robust in the physical security domain, could potentially be compromised by a hacker. CAPSS has been jointly written by NCSC and NPSA leveraging the expertise of both technical authorities.

Term	Abbreviation	Brief Explanation
Closed-Circuit Television	CCTV	A system whereby which images are monitored and recorded for surveillance and security purposes. Has now been superseded in most cases by Video Surveillance Systems (VSS).
Center for Internet Security	CIS	The Center for Internet Security (USA) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. CIS has several program areas, including MS-ISAC, CIS Controls, and CIS Benchmarks. Through these program areas, CIS works with a wide range of entities to increase and improve security efficiency and effectiveness.
Centre for the Protection of National Infrastructure	CPNI	Predecessor to the National Protective Security Authority (NPSA).
Catalogue of Security Equipment	CSE	The CSE is available to help security practitioners to identify appropriate physical security equipment. The CSE provides a range of products that have been evaluated against specific NPSA security standards and the performance rating achieved.
Counter Terrorism Unit	CTU	CTUs work within the wider National Counter Terrorism (CT) network to ensure UK Policing is better equipped to prevent and respond to incidents of terrorism, and to investigate and prosecute those involved. CTUs have a wide range of expertise including detectives, financial investigators, community contact teams,

Term	Abbreviation	Brief Explanation
		intelligence analysts, forensic specialists and investigators.
Counter Terrorism Security Advisor	CTSA	The individual, either within Force or as part of local CTU, whose primary role is to provide advice and guidance on all aspects of counter terrorism protective security to specified industry sectors. They are specialists in physical security assessments and responsible for the provision of protective security advice to publicly accessible locations, local authorities, and local businesses to identify and assess sites that may be vulnerable to terrorist attack.
Design Out Crime Officer	DOCO	A Police Officer or civilian personnel who operate within a DOCU, providing specialist advice and guidance regarding the built environment at every stage of architectural design from pre-planning to the full development control process (to minimise crime, fear of crime, disorder and anti-social behaviour). They are often public-facing individuals and working with a range of organisations, suppliers, and Policing partners.
Design Out Crime Unit	DOCU	A specialised unit within a local Force whose members (DOCOs) provide specialist advice and guidance on various environments to minimise crime, disorder and anti-social behaviour.
Hostile Vehicle Mitigation	HVM	A protective security discipline focusing on reducing risks associated with vehicle borne threats posed by terrorists and criminals. HVM is the delivery of measures that are informed by the threat and how it manifests itself, the multiple

Term	Abbreviation	Brief Explanation
		consequences of an attack, the vulnerability of a given location and the needs of the enterprise requiring protection.
Information Assurance	IA	The practice of assuring information and managing risks related to the use, processing, storage, and transmission of information. Key pillars of IA are the confidentiality, integrity, and availability of data, as well as its authenticity and non-repudiation.
Information Asset Owner	IAO	The nominated risk owner and decision-maker for a particular system(s) and/or dataset(s).
Intrusion Detection Systems	IDS	An IDS monitors traffic on your network, analyses that traffic for signatures matching known attacks, and when something unusual or suspicious occurs, you're alerted. In the meantime, the traffic keeps flowing.
Intrusion Prevention Systems	IPS	An IPS monitors traffic but when something unusual or suspicious occurs, the traffic stops altogether until you investigate and decide to open the floodgates again.
Information Security Forum Standard of Good Practice	ISF SOGP	Published by the Information Security Forum (ISF), the SOFP is a business-focused, practical and comprehensive guide to identifying and managing information security risks in organisations and their supply chains.
International Organisation for Standardisation	ISO	An international standard development organisation composed of representatives from the national standards organizations of member countries.

Term	Abbreviation	Brief Explanation
		The ISO 27000 series is a notable international standard which is focused on the management of information security.
Information Security Officer	ISO	The individual responsible for the security, governance, and compliance of information assets within Force.
Manual Forced Entry Standard	MFES	Produced by NPSA to outline independent forced entry testing of physical barriers to classify their performance and approve their use for protecting UK government and national infrastructure. NPSA use the results of tests conducted in accordance with the MFES to determine the forced entry resistance classifications attributed to products listed within the CSE. Note: MFES replaced the Physical Barriers Attack Standard (PBAS).
Marauding Terrorist Attack	MTA	Fast-moving, violent incidents where assailants move through a location aiming to find and kill or injure as many people as possible.
Marauding Terrorist Attack Standard	MTAS	The MTAS provides a means for determining the delay (resistance time) of a physical barrier against a particular type of attack e.g. the use of bladed weapons to attack the physical barrier in order to achieve access through it. MTAS focusses on the delay a barrier can afford against attacks; it does not consider the ease with which barriers can be secured and unlocked to aid escape.
National Authority for Counter Eavesdropping	NACE	The UK Governments Technical Authority for the practice of protecting sensitive

Term	Abbreviation	Brief Explanation
		information and technology from close access acquisition by hostile threat actors, as well as from any other form of technical manipulation.
National Chief Information Security Officer	NCISO	Responsible for providing technical and strategic direction and guidance across UK Policing.
National Cyber Policy & Standards Board	NCPSB	The National Cyber Policy & Standards Board is made up of senior representatives from the policing regions and members of PDS. The NCPSB is the approving authority for National cyber standards and control objectives.
National Cyber Policy & Standards Working Group	NCPSWG	The NCPSWG is made up of a number of police force representatives from across the regions, members of PDS, NPCC, Home Office, the National Cyber Security Centre (NCSC) and the National Protective Security Authority (NPSA). This group reviews new requests and documents that are being authored.
National Cyber Security Centre	NCSC	The UK government's National Technical Authority for cyber threats and Information Assurance.
National Information Asset Owner	NIAO	A National IAO is responsible for approving risks which fall solely within their area of responsibility and which are within the risk levels specified above depending on the risk appetite for the system or data concerned. If a risk level exceeds the National IAO's remit (or involves a risk that spans the area of responsibility for multiple IAOs) then it is escalated to the National SIRO. A register of all National IAOs is held by PDS Cyber Services.

Term	Abbreviation	Brief Explanation
National Institute of Standards and Technology Cyber Security Framework	NIST CSF	A set of guidelines for mitigating organisational cybersecurity risks, published by the United States National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and best practices.
National Management Centre	NMC	The national centre of expertise dedicated to protecting police forces across the UK against cybercrime. The NMC provides a 24/7 nationally coordinated, locally delivered, cybersecurity service for police forces across the UK. Seven services are available to forces, all designed to protect, detect, and respond to cyber activity on policing infrastructures.
National Protective Security Authority	NPSA	The UK government's National Technical Authority for physical and personnel protective security. NPSA helps organisations understand the range of threats they and the UK face e.g. from terrorism, espionage, and state actors, and importantly what they can do to minimise their risk through how they operate day to day.
National Senior Information Risk Owner	NSIRO	The National SIRO is the ultimate risk owner for policing and provides a decision on the most serious of risks at a national level.
Operational Security Advisor	OpSy	An individual, either within Force or as part of local ROCU, whose objective is to monitor and reduce operational security risk. They will be responsible for maintaining consistency in standards of security and practice in accordance with legislation, national guidelines, local

Term	Abbreviation	Brief Explanation
		security policy, and working in conjunction with operational partners (e.g. NCA).
Publicly Available Specification	PAS	A standard, governed by BSI, set by an industry to ensure that all manufacturers in an industry are making and selling products that reach the industry benchmark for quality.
Police Assured Security Facility	PASF	A physical security assessment of a structure to determine the security maturity of that building/site in terms of physical security as well as personnel security, security awareness and education, and management and disposal of assets.
Police Digital Service	PDS	PDS is the UK organisation responsible for coordinating, developing, delivering, and managing digital services and solutions that enable UK policing to safely harness technology to improve public safety. Funded by policing and the Home Office, PDS works with law enforcement organisations, private industry, charities, public bodies, and government to deliver digital services and solutions with policing, for policing.
Police Search Advisor	PolSA	Specialised operative on search-related matters, planning searches and controlling search teams on low risk and other police search operations, and supporting and developing search team and force search training.
Protective Security Risk Management	PSRM	The NPSA's Protective Security Risk Management (PSRM) methodology is an established and trusted risk framework used for the assessment for physical security, personnel and cyber security

Term	Abbreviation	Brief Explanation
		including surreptitious threats and Marauding Terrorist Attacks (MTAs).
Regional Organised Crime Unit	ROCU	A unit, usually made up of various local Forces, that have a range of specialist policing capabilities including a dedicated cyber security team that works with businesses, organisations, and communities to promote the steps that will reduce the chances of becoming a victim of cybercrime. ROCUs, and their counterparts in Scotland and Northern Ireland, regularly work with SMEs, charities, and other organisations in response to specific threats and can provide support in the event of a cyber incident, irrespective of whether a formal police investigation exists.
Secured by Design	SBD	The official Police security initiative that provides guidance and support on physical security best practices across various industries.
Secure by Design	SbD	A risk assessment framework used for the assurance of National Policing systems, and widely adopted across UK Government.
Senior Information Risk Owner	SIRO	The nominated senior risk owner and decision-maker for your organisations systems and data.
Surreptitious Threat Mitigation Process	STaMP	STaMP provides a structured framework for benchmarking both existing and proposed physical protective security measures against a surreptitious threat.
Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege	STRIDE	A risk model used for identifying and assessing cyber security threats against a defined scope.
Third Party Assurance for Policing	TPAP	Policing's third party security assurance framework to embed information security

Term	Abbreviation	Brief Explanation
		requirements into both the procurement process and formal third party contracts.
Video Surveillance Systems	VSS	Digital video surveillance systems that operate over TCP/IP networks, opposed to previous capabilities operating on hard-wired analogue cabling i.e. CCTV.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Scott Patterson	Initial version	11/10/23
0.2	Scott Patterson	Amendments following peer review	18/01/24

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	21/03/24

Document References

Ref	Title	Source	Date
1	National Police Information Security Risk Management Framework	PDS	05/23
2	National Police Information Security Risk Assessment Guidance	PDS	05/23
3	Standard of Good Practice (for Information Security)	ISF	07/22
4	ISO 27002:2022	ISO	02/22
5	CIS Controls [v8]	CIS	05/21
6	10 Steps to Cyber Security	NCSC	05/21
7	CSA Cloud Controls Matrix	CSA	01/21
8	NIST Cyber Security Framework	NIST	04/18
9	NPSA Protective Security Risk Management (PSRM)	NPSA	01/23
10	Passport to Good Security	NPSA	01/23
11	STaMP Methodology Guidance	NPSA	2021
12	Secured by Design (SBD) Development Guides	SBD	2023
13	Secured by Design (SBD) Technical Guides	SBD	2019
14	Third Party Assurance for Policing (TPAP) Standard	PDS	05/23
15	Marauding Terrorist Attack Standard (MTAS)	NPSA	04/21
16	Cyber Assurance of Physical Security Systems (CAPSS)	NPSA	05/23
17	Catalogue of Security Equipment (CSE)	NPSA	-
18	Secure Destruction of Sensitive Items	NPSA	04/14