CYBER STANDARDS DOCUMENT

Technical Security Management

ABSTRACT:

This Standard specifies the minimum requirements regarding technical security management. It describes the requirements to enable members of the community of trust to build and operate an effective technical security infrastructure, applying security architecture principles and integrating technical security solutions, such as malware protection, intrusion detection and cryptography.

APPENDIX A: Terms and Abbreviations

ISSUED	December 2025
PLANNED REVIEW DATE	November 2026
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 the design, building and managing sound technical security infrastructures protecting policing systems and data.

Introduction

In today's dynamic and interconnected digital policing landscape, establishing a robust technical security infrastructure is critical to safeguarding sensitive information and ensuring the confidentiality, integrity and availability of policing information assets.

This document provides the requirements to design, implement and maintain a sound technical security framework, incorporating security architecture principles and integrated solutions such as malware protection, intrusion detection, and approved cryptographic solutions, including Public Key Infrastructure (PKI).

It should be read in conjunction with the suite of the National Community Security Policy (NCSP) standards, guidelines and blueprints. Application of this standard should be considered in the context of local and national policing risk appetites.

Owner

National Chief Information Security Officer (NCISO).

Purpose

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

This standard helps organisations demonstrate compliance with the following NPCSP statements:

Technical Security Management

- Build a resilient technical security infrastructure, applying security architecture principles and integrating technical security solutions, which include malware protection and intrusion detection.

- Deploy approved cryptographic solutions (e.g. using encryption, public key infrastructure and digital signatures) in a consistent manner across the organisation to help protect the confidentiality of information; determine if critical information has been altered; provide strong authentication; and support non-repudiation.

The requirements stated in this standard are mapped across from the following industry standards:

- International Security Forum Standard of Good Practice (ISF SoGP) 2024
- ISO 27002:2022
- CIS Controls
- NIST Cyber Security Framework v2.0

Audience

Members of the Policing Community of Trust.

More specifically the standard is targeted at, architects, developers, and security experts tasked with designing and building solutions, applications and services that will process or store policing information assets.

The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of the use of technology within policing:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Auditors providing assurance services to policing or PDS.

Finally, Policing's reliance on third parties means that suppliers acting as service providers or developing products or services for policing, should also be made aware of and comply with the content of this standard, in relation to their work on Policing systems and data.

Scope

1. This standard applies to all networks, cloud environments, applications and systems that process, store or access policing data or information assets. This includes but is not limited to servers, desktops, laptops & mobiles.
2. In addition, devices or systems that are not owned by members are expected to have the required technical controls in place wherever the systems are connected to national policing systems.
3. This standard applies to all production and non-production environments, including network, cloud and application environments.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1.0	**Build a sound technical security infrastructure** **Linked Documents** - Cyber Security Architecture Principles		
1.1	When designing or improving security infrastructure, ensure that the National Policing's Cyber Security Architecture Principles are applied.	National Policing Cyber Security Architectural Principles **NIST CSF v2.0** ID.AM-08 **NIST CSF v2.0** PR.PS-06 **CIS v8.1** 16.1 **ISO 27002:2022** 8.27 **ISF SOGP 2024** SD1.1, SD 1.2, TI2.1	Project governance and design documents detailing alignment to the principles. Decisions and exceptions follow a process which has been approved by a relevant governance body and are documented.
1.2	Ensure designs and documentation are clear and easy to follow. Any decisions should be supported with a rationale. This ensures any later decisions can be made with full understanding of the facts, allowing for correct implementation of technical security controls.	**NIST CSF v2.0** ID.AM-08 **NIST CSF v2.0** PR.PS-06 **CIS v8.1** 16.1 **ISO 27001:2022** 8.27 **ISF SOGP 2024** SD1.1, SD 1.2, TI2.1	High-level design. Low-level design. Supporting design artefacts. Design review processes.
1.3	Ensure that the implemented security controls support the risk profile of the organisation(s) that is deploying the solution, and supports the National Information Security Risk Management Framework.	National Information Security Risk Management Framework (NISRMF)	Business Impact Assessments. Risk assessments. Application of the NISRMF.

Reference	Minimum requirement	Control reference	Compliance Metric
2.0	**Malware protection** **Linked Documents** • Privileged Access Management Standard (2.4) • Physical Asset Management (2.8) • NEP Blueprints Volume 11 (Windows Modern Management) • NMC Blueprints Volume 2 (Sentinel)		
2.1	Malware protection must be in place on relevant components within technical designs. These may be standard anti-virus tools, or newer technologies like Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR).	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2 IAM & PS LLD Vol 10 IAM & PS LLD Vol 11	Malware protection must be evidenced within designs. A comprehensive incident response plan to demonstrate actions taken in the event of a malware attack. Evidence of regular penetration tests/ITHCs, scoped to include testing the performance and reporting capabilities.
2.2	Malware protection must be managed and monitored to ensure updates are applied and that any detections are reported to administrators.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.7	Evidence of logging and monitoring of malware protection products.

Reference	Minimum requirement	Control reference	Compliance Metric
		IAM & PS LLD Vol 10 IAM & PS LLD Vol 11	
2.3	Malware protection should be configured to alert when threats are found, and when failures occur.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.7	A comprehensive incident response plan to demonstrate action in the event of a malware attack.
2.4	Access to the malware protection tool's management console should be restricted to privileged users.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7	Design documentation showing role-based access control processes for malware protection tooling.
2.5	Any changes to malware protection tool configurations must be undertaken in line with change management processes.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.8, TP1.2.9	Documentation showing change management processes. ITSM knowledge base articles on the processes to follow.
2.6	Any malware alerts must trigger a documented process resulting in the asset being promptly contained and analysed.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.7	Real-time alerting and reporting of detections and quarantined files, identifying regular patterns of Indicators of Compromise (IoC).

Reference	Minimum requirement	Control reference	Compliance Metric
2.7	Malware protection tools should have their signature database regularly updated, in line with the vendor's recommendations. Failures to update should be alerted to administrators.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.5	Regular reviews of AV consoles to identify updates, with processes in place to identify failure of updates.
2.8	Processes must be developed to cater for instances where malware protection is not possible, or ineffective. For example, industrial control units, encrypted files which cannot be scanned via traditional means, etc.	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.3	Records against assets where malware protection not in place with risk balance case or equivalent.
2.9	Malware protection should be configured to scan at least the following areas: • Firmware • Master Boot Records/GUID Partition Tables • Local files, including program executables • Removeable media • Network traffic • File shares	**NIST CSF v2.0** DE.CM-01 **NIST CSF v2.0** DE.CM-09 **CIS v8.1** 10.1, 10.2, 10.4, 10.5, 10.6, 10.7 **ISO27001:2022** 8.7 **ISF SOGP 2024** TP1.2.6	Malware tool configuration settings.

Reference	Minimum requirement	Control reference	Compliance Metric
3.0	**Protective monitoring & intrusion detection** **Linked Documents** • Incident Management Standard (3.2) • Logging and Monitoring Standard (3.4, 3.5)		
3.1	Establish a baseline of network operations and expected data flows for systems and users. This can be used to support further analysis and threat modelling for the solution.	**NIST-CSF v2.0** ID.AM-03 **NIST-CSF v2.0** ID.AM-07	Documented baselines within information asset registers. Data flow diagrams and technical designs/documentation.
3.2	Apply 24/7 protective monitoring solutions for on-premises and cloud environments with a defined timescale to respond to suspected and confirmed attacks.	**NIST CSF v2.0** DE.AE-02 **NIST CSF v2.0** DE.AE-04 **NIST CSF v2.0** DE.CM-01 **NIST-CSF v2.0** DE.CM-03 **NIST-CSF v2.0** DE.CM-06 **NIST-CSF v2.0** DE.CM-09 **NIST-CSF v2.0** PR.PS-05 **CIS v8.1** 13.2, 13.3, 13.7, 13.8 **ISO27001:2022** 8.16 **ISF SOGP 2024** SE1.2, TP1.3	Regular reporting and reviews of threats. Documented roles and responsibilities showing who is to identify and investigate threats. Regular reviews of functionality and assets covered by protective monitoring capabilities, including review of use cases. Regular reviews of incident response plans, ensuring they align with protective monitoring. Review log ingestion and retention to identify gaps.

Reference	Minimum requirement	Control reference	Compliance Metric
3.3	Protective monitoring use cases must be defined and tuned to the environment. Example of use cases include: • detecting compromised accounts, • monitoring system changes, • compliance with security policies, • threat hunting cloud applications, • detecting unusual behaviour on privileged accounts.	**NIST-CSF v2.0** ID.IM **NIST-CSF v2.0** ID.IM-03 **CIS v8.1** 13.11 **ISO27001:2022** 8.16 **ISF SOGP 2024** SE1.2	Regular reviews of incident response plans, ensuring they align with protective monitoring. Documented use-cases for Protective Monitoring.
3.4	Reporting and alerting should be provided to enable real time event management.	**NIST-CSF v2.0** DE.CM-03 **CIS v8.1** 8.11 **ISO27001:2022** 8.15 **ISF SOGP 2024** SE1.1.6	Tracking of reporting and alerting against SLAs.
3.5	Protective monitoring logs should be retained in line with current guidance. Additionally, protective monitoring logs need to be protected aligned to their sensitivity e.g. may need to be subject to: i) access restrictions ii) encryption iii) integrity protection against potential tampering	**CIS v8.1** 8.1 **ISO27001:2022** 8.15 **ISF SOGP 2024** SE1.1.6	Documented design showing log retention policies. Confirmation of protective measures based upon sensitivity.

Reference	Minimum requirement	Control reference	Compliance Metric
3.6	Ensure that all systems and assets are synchronised to at least two trusted and accurate time sources.	**CIS v8.1** 8.4 **ISO27001:2022** 8.17 **ISF SOGP 2024** SE1.1.3	Architectural designs showing two time sources in use. Checks on assets and security monitoring systems showing synchronised timings.
4.0	**Cryptographic solutions** **Linked Documents** • Cryptography Standard (4.1)		
4.1	Cryptography must be used to encrypt sensitive content and to provide non-repudiation. Further, it should be used wherever possible to encrypt data in transit and data at rest.	**NIST-CSF v2.0** PR.DS-01 **NIST-CSF v2.0** PR.DS-01 **CIS v8.1** 3.6, 3.9, 3.10, 3.11 **ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.1	Documented designs showing cryptographic usage. Data flow diagrams showing protocols in use.
4.2	Public key infrastructures (PKI) must be protected with controls to ensure confidentiality, integrity and availability.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.3 Cryptography Standard	Protective monitoring reports on PKI components. Audit logs showing usage of PKI components, including any offline components.

Reference	Minimum requirement	Control reference	Compliance Metric
4.3	To provide confidentiality and integrity to cryptographic keys they must be stored securely in hardware security modules (HSM).	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.3 Cryptography Standard	Documentary evidence of secure key storage such as physical HSMs, or Azure Key Vault. Technical designs showing secure architectures for PKI. Auditable access requests to keys, linked to a change management process.
4.4	HSMs must have strong access controls, including multi-factor authentication, to protect against unauthorised disclosure, theft, loss and corruption, minimising the risk of an attack exposing critical or sensitive information.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.4 Cryptography Standard	Documentary evidence of strong access controls. Documentary evidence showing restricted access to keys.
4.5	Monitoring of access requests to key material must be in place and supported by a change management process.	**ISO27001:2022** 8.24 Cryptography Standard	Audit logs showing usage of PKI components, including any offline components. Documented change management processes.
4.6	All key ceremonies required for the operation of the PKI root must be conducted with at least 2 individuals.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.6, CP1.3.8 Cryptography Standard	Certificate Policy. Certificate Practice Statement. Audit logs showing key ceremonies, including those present.

Reference	Minimum requirement	Control reference	Compliance Metric
4.7	Access to key components of the PKI should be split so that no one person can assemble the components and carry out functions that would normally be done under dual control.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.8 Cryptography Standard	Access logs to safes, or other suitable storage areas, showing who is accessing key components.
4.8	Cryptographic keys must be generated using random number generators (RNG) with high levels of entropy.	**ISO27001:2022** 8.24 Cryptography Standard	Documentary evidence that keys are generated using a random number generator with high levels of entropy.
4.9	Availability of PKI is critical to ensure that encryption services are operational and cryptographic keys can always be recovered during an emergency.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.9	Ensure regular backups of keys are taken and stored in a secure location. Ensure there is monitoring of the PKI with alerting in place.
4.10	Regular backups of key components of the PKI, including cryptographic keys should be undertaken, including the testing of recovery processes.	**ISO27001:2022** 8.24 **ISF SOGP 2024** CP1.3.9	Backup logs showing backups taking place. Recovery test documentation showing recovery is possible.

Reference	Minimum requirement	Control reference	Compliance Metric
5.0	**End user education** **Linked Documents** • People Security Management Standard (5.1) • Incident Management Standard (5.1)		
5.1	Have a comprehensive end-user training programme in place to ensure users are aware of, and vigilant to, the variety of threats they will face. As part of an organisational cyber security education and awareness programme the following behavioural objectives should be met for all users of any IT service, system or application: • Aware of threats to IT systems. • Ability to identify potential or actual malicious activity. • The importance of adhering to acceptable use policies and standards of behaviour. • How to report suspected or actual incidents in accordance with the local security incident management procedures.	**NIST-CSF v2.0** PR.AT-01 **CIS v8.1** 14.1, 14.2, 14.6 **ISO27001:2022** 6.3 **ISF SOGP 2024** ST1.1, ST1.2, ST1.3	Acceptable Use Policies (AUP) in place for systems and services. Incident reporting and management procedures in place and tested. Training records for an all-personnel cyber education & awareness programme in place. Records of reported suspected or actual malware.

Reference	Minimum requirement	Control reference	Compliance Metric
5.2	Have role specific education programmes in place for high profile and highly privileged users.	**NIST-CSF v2.0** PR.AT-02 **CIS v8.1** 14.9 **ISO27001:2022** 6.3 **ISF SOGP 2024** ST1.1, ST1.2, ST1.3	Register of persons and roles who are considered high-profile and/or highly privileged. Training records for high-risk users' cyber education & awareness programme in place.
5.3	Train users to spot the signs of social engineering.	**NIST-CSF v2.0** PR.AT-01 **CIS v8.1** 14.2 **ISO27001:2022** 6.3 **ISF SOGP 2024** ST1.1, ST1.2, ST1.3	Training records for an all-personnel cyber education & awareness programme in place.
5.4	Train users in the risks and causes of accidental data exposure.	**NIST-CSF v2.0** PR.AT-01 **CIS v8.1** 14.4, 14.5 **ISO27001:2022** 6.3 **ISF SOGP 2024** ST1.1, ST1.2, ST1.3	Training records for an all-personnel cyber education & awareness programme in place.

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 representatives from participating forces and PDS.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to police forces, PDS and associated bodies.

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

This standard should be distributed within IT 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 force personnel of the implementation of this standard where it may affect them.

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
0.1	PDS Cyber	Initial version	07/07/23
0.2	PDS Cyber	Updated following internal peer reviews	13/12/23
1.0	NCPSB	Published	January 2024
1.1	PDS Cyber	Annual review	22/10/2024
1.2	PDS Cyber	Annual Review	27/10/2025

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	January 2024
1.1	NCPSB	National Cyber Policy & Standards Board	26/11/24
1.1	NCPSB	National Cyber Policy & Standards Board	27/11/25

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
ISO 27001:2022 - Information security, cybersecurity and privacy protection – Information security management controls – Requirements	v2022, Third Edition	10/2022
CIS Controls	v8.1	05/2021
NIST Cyber Security Framework	V2.0	02/2024

Appendix A – Terms and Abbreviations

Based upon National Institute of Standards & Technology (NIST) and National Cyber Security Centre

Term	Abbreviation	Brief explanation
Alert		A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.
Anomalies		Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.
Attack		Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Attacker		Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.
Anti-virus	AV	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
Data Loss Prevention	DLP	A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.
Distributed Denial of Service	DDOS	When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. Distributed uses numerous hosts to perform the attack.

Term	Abbreviation	Brief explanation
Endpoint Detection & Response	EDR	Endpoint Detection and Response (EDR) is an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response.
European Institute for Computer Anti-Virus Research	EICAR / WICAR	The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO) to test the response of computer antivirus (AV) programs.
Event		Any observable occurrence in a network or information system.
Exploit		May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.
Forensics		The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
(Cyber) Incident		A breach of the security rules for a system or service - most commonly; Attempts to gain unauthorised access to a system and/or to data. Unauthorised use of systems for the processing or storing of data. Changes to a systems firmware, software or hardware without the system owners consent. Malicious disruption and/or denial of service.
Hardware Security Module	HSM	A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs.

Term	Abbreviation	Brief explanation
Impact		The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Intelligence		Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.
IoC (Indicator of Compromise)		(IOCs) serve as forensic evidence of potential intrusions on a host system or network. These artifacts enable information security (InfoSec) professionals and system administrators to detect intrusion attempts or other malicious activities. Security researchers use IOCs to better analyse a particular malware's techniques and behaviours. IOCs also provides actionable threat intelligence that can be shared within the community to further improve an organization's incident response and remediation strategies.
Intrusion Detection System	IDS	A security service that monitors and analyses network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
Intrusion Prevention System	IPS	A system that monitors the events occurring in a computer system or network, analysing them for signs of possible incidents, and attempting to stop detected possible incidents.
Malware		Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Term	Abbreviation	Brief explanation
Multi Factor Authentication	MFA	An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.
MITRE Attack	MITRE ATT&CK	MITRE ATT&CK ® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Adversarial Tactics, Techniques, and Common Knowledge
Phishing		Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Public Key Infrastructure	PKI	Public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption , The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.
Roles Based Access Controls	**RBAC**	Role-based access control is a policy-neutral access control mechanism defined around roles and privileges.
Security information and event management	**SIEM**	Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

Term	Abbreviation	Brief explanation
Security orchestration, automation and response	**SOAR**	Security orchestration, automation and response (SOAR) is a group of cyber security technologies that allow organizations to respond to some incidents automatically. It collects inputs monitored by the SOC such as alerts from the SIEM system and supports with incident response activities.
Security Operation centre	**SOC**	Security Operation centre is a team of security analysts that monitor and detect any malicious activity within systems over a 24/7 period, if any malicious activity is detected action is taken to eliminate the threat and report accordingly.
Threat		Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Hunting		Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find any malicious actors in your environment that may have slipped past your initial endpoint security defences.
Trusted Platform Module	TPM	A dedicated microcontroller designed to secure hardware through integrated cryptographic keys. The term can also refer to a chip conforming to the standard ISO/IEC 11889.
Vulnerability		A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.