



Australian Government
Australian Signals Directorate

cyber.gov.au

Assessment evidence guide for enterprise IT



Essentials

Contents

Purpose	3
How to use this document	3
Indicators of Good Practice	3
Potential evidence sources	3
GOV-01 - Executive cyber security accountability	5
GOV-08 - Executive artificial intelligence accountability	6
GOV-04 - Cyber security resourcing	7
GOV-03 - Security risk management assurance	9
Identify principles	13
IDE-01 - Asset Identification	13
IDE-04 - Security risk identification	15
Protect principles	16
PRO-01 - Secure system lifecycle	16
PRO-12 - Least privilege access	26
PRO-05 - Secure administration	28
PRO-04 - Secure configuration management	32
PRO-06 - Vulnerability management	35
PRO-07 - Trustworthy software	38
PRO-10 - Regular and proven backups	39
PRO-18 - Network segmentation and segregation	43
PRO-09 - Content filtering	45
PRO-14 - Cyber security awareness training	48
Detect principles	50
DET-01 - Centralised event logging	50
DET-02 - Cyber security event detection	54
DET-03 - Cyber security incident identification	56
DET-05 - Detection capability efficacy	58
Respond principles	59
RES-05 - Cyber security incident coordination	59
RES-03 - Cyber security incident response	60
RES-04 - Cyber security incident insights	61
Annex A - Domains	63

Purpose

This document is intended to provide assessors with a series of supporting statements that can be used, alongside expert judgement, to determine how effectively an organisation is addressing the intent of the actions and overarching principles outlined in the Essentials for enterprise IT framework.

How to use this document

Indicators of Good Practice

Indicators of Good Practice (IGP) statements are included for each of the Essentials for enterprise IT actions. The IGP statements are optional indicators intended to aid assessors to evaluate the Action outcomes for an applicable Domain. The IGPs do not replace expert judgement, nor are they intended to serve as a checklist.

Each action is presented with three columns of statements, and each column includes a series of statements to consider when assessing the effectiveness of an action. An assessor can use the statements to assist in determining the observed implementation state for the assets in scope. Assessors rate the effectiveness of an action on the lowest level reached:

- If any not effective statement is true, the action is rated **not effective**.
- If all applicable fully effective statements are true, and no partially effective or not effective statement is true, the action is rated **fully effective**.
- In all other cases, including where some fully effective statements are true and others are not, the action is rated **partially effective**.

The **not assessed** status is not represented by IGP statements. It is applied where the action has not yet been assessed, or where there was insufficient visibility to determine whether risk was meaningfully reduced.

Each action is allocated a unique identifier, and each distinct statement for an action is identified to assist with record keeping purposes (for example IT.GOV-01.1.FE-1 can be used to reference the first fully effective statement for the first Govern principle).

Potential evidence sources

Organisations may choose to leverage controls from a variety of sources when addressing the Essentials principles. The effectiveness of a mitigation must also be considered in context of each individual domain, rather than organisation wide; a set of controls that may be effective for one domain does not automatically guarantee effectiveness for another domain.

References to independent cyber security frameworks have been included for each action, which indicate where supporting evidence of that action's effectiveness may exist (if an organisation has adopted that framework already). The list is not intended to define the controls required to meet the intent of the actions.

The frameworks referenced include:

Framework	Full name	Reference documents
ISM (excl. E8)	ASD's Information Security Manual v2026.09.4	PDF OSCAL XML OSCAL JSON OSCAL YAML
E8	ASD's Essential Eight 02 Oct 2024	PDF OSCAL XML OSCAL JSON OSCAL YAML
CSF	NIST Cyber security Framework 2.0	PDF OSCAL XML OSCAL JSON OSCAL YAML
800-171r3	NIST SP 800-171 r3 publication, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"	PDF OSCAL XML OSCAL JSON OSCAL YAML
AESCSF	AEMO's Australian Energy Sector Cyber Security Framework v2	XLSX

Govern principles

GOV-01 - Executive cyber security accountability

Principle: The board of directors or executive committee is accountable for cyber security.

IT.GOV-01.1

Action: Formally define and establish executive and board-level accountabilities for cyber security, including setting, monitoring and adjusting organisational risk appetite, and review these accountabilities at a defined cadence.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No named executive or board member is accountable for cyber security.	PE-1: A named executive or board member is accountable for cyber security, but reporting obligations are not formally defined.	FE-1: A named executive or board member has documented accountability for cyber security with defined reporting obligations.
NE-2: Cyber security accountability exists only informally, or is assumed rather than documented.	PE-2: Board-level reporting on cyber security occurs but is ad hoc rather than on a defined schedule.	FE-2: Regular reporting to the board or executives occurs on a defined cadence with evidence of reporting artefacts.
NE-3: No evidence of cyber security reporting to the executive board.	PE-3: Accountability is documented but has not been reviewed within the organisationally defined cadence or following relevant organisational restructuring or leadership changes.	FE-3: Accountability arrangements are reviewed when organisational structures or leadership changes occur.
NE-4: Organisational risk appetite is not set.	PE-4: Organisational risk appetite is set but is not monitored or adjusted over time.	FE-4: Organisational risk appetite is set and is monitored and adjusted over time as required.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1997, ISM-1998, ISM-1999, ISM-2000, ISM-2005
E8	N/A
CSF	GV.OC-01, GV.RR-01, GV.RR-02, GV.RM-01, GV.RM-02
800-171r3	03.15.01, 03.11.01, 03.11.04
AESCSF	PROGRAM-2a, PROGRAM-2c, RISK-1e, RISK-1f, PROGRAM-1d

GOV-08 - Executive artificial intelligence accountability

Principle: The board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner.

IT.GOV-08.1

Action: Establish and maintain executive accountability for the use, governance and risk management of artificial intelligence within the organisation.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No named executive is accountable for the use, governance or risk management of artificial intelligence.	PE-1: A named executive is accountable for artificial intelligence but the governance process is informal or undocumented.	FE-1: A named executive has accountability for artificial intelligence, supported by an approved governance process that has evidence of being followed.
NE-2: Artificial intelligence is used within the organisation with no approval, risk assessment or oversight.	PE-2: Approval and risk assessment occur for some artificial intelligence use cases but coverage is inconsistent across internally developed, third-party and embedded artificial intelligence.	FE-2: The governance process addresses approval, risk assessment and oversight for internally developed, third-party and embedded artificial intelligence use cases.
NE-3: Artificial intelligence related risks are not reflected in the organisation's risk register.	PE-3: Some artificial intelligence-related risks are recorded but the organisation's risk register does not capture all known artificial intelligence use cases.	FE-3: Artificial intelligence-related risks are reflected in the organisation's risk register and reported through standard governance channels.
NE-4: Artificial intelligence use and governance arrangements have not been reviewed within the schedule defined by the organisation.	PE-4: Reviews occur within the schedule defined by the organisation, but do not consistently address changes in artificial intelligence capability, threat environment or organisational use.	FE-4: Reviews of artificial intelligence use and governance arrangements are conducted on a schedule defined by the organisation and consistently address changes in artificial intelligence capability, threat environment or organisational use.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1998, ISM-2074, ISM-2002
E8	N/A
CSF	GV.OC-01, GV.RR-01, GV.RR-02, GV.RM-06
800-171r3	03.15.01, 03.11.01, 03.04.08
AESCSF	PROGRAM-2a, PROGRAM-2c, RISK-1c, RISK-2a

GOV-04 - Cyber security resourcing

Principle: Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.

IT.GOV-04.1

Action: Assign sufficient cyber security personnel and resources with the required skills to operate, monitor, maintain and manage the lifecycle of security controls and define cyber security responsibilities within role descriptions.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Cyber security functions are staffed on an ad hoc basis without reference to required skills or capacity.	PE-1: Some critical roles are filled but identified skills gaps have no plan for remediation.	FE-1: Sufficient cyber security personnel are assigned to operate, monitor, maintain and manage the lifecycle of controls across the organisation.
NE-2: Critical cyber security roles are unfilled with no approved recruitment plan.	PE-2: While assigned personnel provide some capability, there are gaps in capacity, resources, or expertise that hinder the operation, monitoring, maintenance, and lifecycle management of controls.	FE-2: Skills gaps are identified and addressed through recruitment, training or contracted services.
NE-3: No resourcing plan for cyber security personnel exists.	PE-3: A resourcing plan exists but does not cover all required cyber security functions.	FE-3: A resourcing plan identifies all required cyber security personnel, roles, skills, resources and capacity.
	PE-4: Outstanding cyber security positions are being actively recruited, but capacity or skills gaps remain.	FE-4: Cyber security responsibilities are defined within applicable role descriptions.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0717, ISM-2020, ISM-0732, ISM-2004
E8	N/A
CSF	GV.RR-02, GV.RR-03, GV.RR-04
800-171r3	03.02.02, 03.15.01
AESCSF	WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4b, PROGRAM-2e

IT.GOV-04.2

Action: Periodically review cyber security resourcing against cyber threat trends, cyber security incident outcomes and organisational changes.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No review of cyber security resourcing has been conducted. NE-2: Resourcing has not been reassessed following significant organisational or threat landscape changes.	PE-1: A review has been conducted but did not reference current threat trends, cyber security incident outcomes, or organisational changes. PE-2: Review outcomes have identified required adjustments, but those adjustments have not been made.	FE-1: A resourcing review has been completed within the review period defined by the organisation. FE-2: The review references current threat trends, cyber security incident outcomes and organisational changes. FE-3: Documented review outcomes include resourcing adjustments that are implemented within timeframes defined by the organisation, or formally risk accepted by an appropriate authority.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1617, ISM-2020, ISM-0724, ISM-2003
E8	N/A
CSF	GV.RR-03, GV.OV-03, GV.OC-05
800-171r3	03.11.01, 03.12.03, 03.14.03
AESCSF	WORKFORCE-3e, WORKFORCE-4c, PROGRAM-2g, RISK-2g

GOV-03 - Security risk management assurance

Principle: Security risk management activities for an organisation and their systems (infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks and subject to ongoing monitoring and assurance activities by the board of directors or executive committee.

IT.GOV-03.1

Action: Establish and maintain an approved risk management methodology and plan that is used to assess and treat cyber security risks.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No risk management methodology approved by the organisation is in place.	PE-1: An approved risk management methodology exists but risk assessments have not been conducted within the defined cycle.	FE-1: An approved risk management methodology and plan are in place and used to assess and treat security risks.
NE-2: No current organisational risk register exists, or the register has not been reviewed within the cycle defined by the organisation.	PE-2: A risk register exists but treatment plans are incomplete or have not been actioned.	FE-2: A current risk register exists with documented and implemented treatment plans for all identified risks.
NE-3: Risk treatment decisions are not documented.	PE-3: Risk assessments have been conducted but do not cover all in-scope assets.	FE-3: Risk assessments have been conducted or reviewed within the assessment cycle defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1203, ISM-1634, ISM-0009, ISM-1526
E8	N/A
CSF	GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-06, GV.RM-07
800-171r3	03.11.01, 03.11.04, 03.15.01, 03.12.02
AESCSF	RISK-1a, RISK-1b, RISK-2b, RISK-2e

GOV-11 - Supplier cyber security assurance

Principle: Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers whose cyber security practices are regularly verified or otherwise risk-assessed.

IT.GOV-11.1

Action: Select and engage suppliers of software, hardware and services on the basis of a cyber supply chain risk assessment proportionate to the risk the supplier introduces, and retain appropriate assurance evidence to support the decision.

Domains: Governance and culture; **Mitigated Techniques:** [Supply Chain Compromise](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No documented or approved governance process exists for evaluating the cyber security trustworthiness of suppliers.	PE-1: An evaluation process exists but is not consistently applied to all suppliers within scope.	FE-1: A documented and approved governance process is in place and consistently applied.
NE-2: No cyber security evaluation is performed before suppliers are onboarded.	PE-2: Evaluation is performed for some suppliers, but criteria are not documented or are inconsistently applied.	FE-2: Cyber security trustworthiness evaluations are performed for all suppliers within scope prior to onboarding.
NE-3: Evaluation outcomes are not documented.	PE-3: Outcomes are documented but contractual arrangements do not reflect identified risks or required controls.	FE-3: Evaluation criteria are documented, approved and proportionate to the criticality of what the supplier delivers.
NE-4: Findings from supplier evaluation outcomes are not used to inform supplier approval, contractual requirements or risk treatment decisions where concerns are identified.		FE-4: Evaluation outcomes are documented, reflected in contractual arrangements and recorded in the organisation's risk register where residual risk remains.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1631, ISM-1452, ISM-1568, ISM-1632, ISM-1787
E8	N/A
CSF	GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-06
800-171r3	03.17.01, 03.17.02, 03.17.03, 03.16.03
AESCSF	THIRD-PARTIES-2a, THIRD-PARTIES-2b, THIRD-PARTIES-2d, THIRD-PARTIES-2j

IT.GOV-11.2

Action: Maintain current assurance that suppliers continue to meet their cyber security commitments, and act when that assurance lapses or the supplier's risk changes.

Domains: Governance and culture; **Mitigated Techniques:** [Supply Chain Compromise](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No process exists to obtain and risk-assess current supplier assurance evidence proportionate to supplier criticality and risk.	PE-1: Supplier assurance evidence is obtained for some suppliers, but coverage is incomplete or the evidence is not reviewed and actioned.	FE-1: Current assurance evidence is obtained from suppliers in proportion to their criticality and risk, and is reviewed for findings that affect the organisation.
NE-2: No documented and approved governance process exists for maintaining assurance that suppliers meet their cyber security commitments.	PE-2: Some findings are actioned but the response process is informal or inconsistent.	FE-2: Material concerns are addressed through contractual remediation, compensating controls or supplier substitution within defined timeframes.
NE-3: No actions are taken when supplier cyber security assurance lapses or supplier risk changes.	PE-3: A process exists but acceptable forms and currency of assurance evidence are not defined or applied consistently.	FE-3: A documented and approved governance process specifies the acceptable forms, scope and currency of supplier assurance evidence.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1567, ISM-1882, ISM-1785
E8	N/A
CSF	GV.SC-07, GV.SC-09
800-171r3	03.17.03, 03.16.03
AESCSF	THIRD-PARTIES-2f, THIRD-PARTIES-2g

GOV-14 - Legacy system management

Principle: Systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating security controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or replaced.

IT.GOV-14.1

Action: Establish and maintain a process for identifying, assessing and treating cyber security risks associated with legacy systems and unsupported technologies through compensating controls, enhanced monitoring and assurance until the systems can be removed or replaced.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No documented or approved governance process exists for identifying or managing legacy systems.	PE-1: A process exists but the criteria for classifying a system as legacy are not documented or are inconsistently applied.	FE-1: A documented and approved governance process exists with clear criteria for classifying systems as legacy.
NE-2: Legacy systems are not formally identified within the environment.	PE-2: Some legacy systems are identified but the inventory is incomplete or is not maintained.	FE-2: Legacy systems are formally identified, inventoried and reviewed on a cycle defined by the organisation.
NE-3: Cyber security risks associated with legacy systems are not assessed or are assessed informally.	PE-3: Risks assessments are conducted for some legacy systems but treatment decisions are not documented or approved.	FE-3: Cyber security risks associated with legacy systems are assessed, treated and approved by an appropriate authority.
NE-4: There are no interim compensating controls to manage identified cyber security risks associated with legacy systems.	PE-4: Some compensating controls are in place to address risks associated with legacy systems, but coverage is not complete.	FE-4: Compensating controls are applied to manage cyber security risks for legacy systems while decommissioning or migration efforts are in progress.
NE-5: Legacy systems remain in operation indefinitely with no documented decommissioning, replacement or migration path.	PE-5: A path exists for some legacy systems but is not tracked to completion.	FE-5: A documented decommissioning, replacement or migration path exists for retained legacy systems and is tracked to completion.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1809, ISM-1526, ISM-1203
E8	ISM-1501
CSF	GV.RM-06, ID.AM-08, ID.RA-01
800-171r3	03.16.02, 03.11.01, 03.11.04, 03.12.02
AESCSF	THIRD-PARTIES-2i, RISK-2a, ASSET-1h, ARCHITECTURE-3i

Identify principles

IDE-01 - Asset Identification

Principle: Systems (infrastructure, operating systems, applications, identities, credentials and data) are continually and centrally identified and documented.

IT.IDE-01.1

Action: Use an approved asset inventory mechanism that supports automated discovery to detect new and changed physical and non-physical assets

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No approved asset inventory mechanism is in place. NE-2: Asset inventory records are maintained manually with no automated discovery capability.	PE-1: An approved asset inventory mechanism is deployed but does not cover all network segments or asset types. PE-2: Automated discovery scans to detect new and changed physical and non-physical assets occur on a schedule but reconciliation with the approved inventory is manual or inconsistent.	FE-1: An approved asset inventory mechanism which supports automated discovery is deployed to cover all applicable assets and network segments. FE-2: Discovery runs on a regular schedule defined by the organisation and new or changed physical or non-physical assets that are detected are reconciled with the approved inventory.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1493, ISM-1643, ISM-1966
E8	ISM-1807
CSF	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-08
800-171r3	03.04.10, 03.04.11
AESCSF	ASSET-1a, ASSET-1f, ASSET-1g, ASSET-2a

IT.IDE-01.2

Action: Maintain current records of infrastructure, operating systems, applications, identities, credentials and data assets.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: A maintained record of infrastructure, operating systems, applications, identities, credentials and data assets has not been established. NE-2: There is no defined process for identifying, recording, reviewing and updating asset records.	PE-1: Asset records are maintained, but identified omissions, inaccuracies or newly discovered assets are not triaged and addressed within the timeframes or tolerances defined by the organisation. PE-2: A process to update the asset inventory runs on a schedule but the results are not reconciled or updated within a period defined by the organisation.	FE-1: At each scheduled review or update, records of infrastructure, operating systems, applications, identities, credentials and data assets are complete and accurate within the tolerances defined by the organisation. FE-2: A defined process identifies changes and newly discovered assets between scheduled reviews, and ensures that records are reviewed, reconciled and updated within timeframes commensurate with the associated cyber security risk.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1493, ISM-1643, ISM-1966, ISM-1633
E8	N/A
CSF	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-07, ID.AM-08
800-171r3	03.04.10, 03.04.11
AESCSF	ASSET-1a, ASSET-1e, ASSET-2a

IDE-04 - Security risk identification

Principle: Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.

IT.IDE-04.1

Action: Identify relevant weaknesses, malicious actor techniques and cyber threat behaviours when undertaking risk assessments and review these inputs on a continuous basis.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Risk assessments do not reference relevant weaknesses, malicious actor techniques and cyber threat behaviours.	PE-1: Risk assessments reference threat intelligence but coverage is limited to well-known or generic threats.	FE-1: Risk assessments incorporate and reference relevant weaknesses, malicious actor techniques relevant to the sector, and cyber threat behaviours.
NE-2: No process exists to incorporate threat information into risk assessment activities.	PE-2: Threat information is considered but not systematically mapped to organisational assets or detection gaps.	FE-2: Relevant weaknesses, malicious actor techniques and cyber threat behaviours are systematically related to applicable assets and used to inform risk treatment decisions.
NE-3: Current weaknesses, malicious actor techniques and cyber threat behaviours that are relevant to the organisation are not reviewed or updated.	PE-3: Current weaknesses, malicious actor techniques and cyber threat behaviours that are relevant to the organisation are reviewed or updated, but are not used to inform risk assessments or are reviewed only on an ad hoc basis.	FE-3: Current weaknesses, malicious actor techniques and cyber threat behaviours relevant to the organisation are reviewed or updated on a continuous basis at a frequency that enables noted changes to inform risk assessments.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1203, ISM-1526, ISM-2116, ISM-1921
E8	N/A
CSF	ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-05
800-171r3	03.11.01, 03.11.02, 03.14.03, 03.12.03
AESCSF	THREAT-2a, THREAT-2b, THREAT-1a, RISK-2a

Protect principles

PRO-01 - Secure system lifecycle

Principle: Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality ratings and security and resilience requirements using Secure by Design and Secure by Default principles and practices.

IT.PRO-01.1

Action: Design systems securely to provide visibility, enforce authorised access, protect data, minimise required and default privileges, limit exposed services and remove unnecessary functionality.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Exploit Public-Facing Application](#), [Valid Accounts](#), [Remote Services](#), [Exploitation for Privilege Escalation](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Systems are deployed with default configurations and no evidence of security design considerations.	PE-1: Security is considered during system design but not consistently applied across all assets.	FE-1: Systems are designed and deployed with exposed services limited, required and default permissions minimised, data protections in place, authorised access enforced, and only required functionality enabled.
NE-2: Unnecessary services, protocols or functionality remain enabled with no documented rationale.	PE-2: Some unnecessary services have been disabled but a systematic review has not been completed.	FE-2: Security telemetry is enabled by default.
NE-3: Security telemetry is not enabled or is not considered as part of system design.	PE-3: Security telemetry is partially enabled but gaps in coverage exist.	FE-3: Evidence exists that security design decisions are recorded and reviewed during system changes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0041, ISM-1409, ISM-0380, ISM-2021
E8	ISM-1508
CSF	PR.AA-05, PR.DS-01, PR.DS-02, PR.PS-01, PR.IR-01
800-171r3	03.16.01, 03.01.05, 03.04.06, 03.13.01, 03.13.08
AESCSF	ARCHITECTURE-1c, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-1g

IT.PRO-01.2

Action: Secure build and deployment processes to enforce controls consistently across systems.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No controlled build or deployment process exists for applicable assets.	PE-1: A controlled deployment process exists but is not consistently followed for all changes.	FE-1: A controlled build and deployment process is in place and consistently followed.
NE-2: Changes to systems are applied ad hoc, without any version control, testing or approval.	PE-2: Version control is in place but pre-deployment security verification is not performed.	FE-2: Configuration changes are subject to version control, testing and approval before deployment.
		FE-3: Security controls are confirmed to be implemented consistently across systems following deployment processes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1914, ISM-1635, ISM-1211, ISM-1409
E8	N/A
CSF	PR.PS-01, PR.PS-02, PR.PS-03, DE.CM-09
800-171r3	03.04.01, 03.04.02, 03.04.03, 03.16.01
AESCSF	ASSET-3b, ASSET-3c, ARCHITECTURE-3e, ASSET-4e

PRO-16 - Cyber supply chain security

Principle: Cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response.

IT.PRO-16.1

Action: Assess the integrity and authenticity of software, components and updates before use, and verify provenance where suitable supplier evidence is available.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Supply Chain Compromise](#), [Server Software Component](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No verification of software, component or update integrity or authenticity is performed before introduction into systems. NE-2: Verification outcomes are not recorded or available for review. NE-3: Where verification cannot be performed, no compensating control or remediation paths are documented.	PE-1: Verification is performed for some categories of software but not consistently across operating systems, applications, firmware and dependencies. PE-2: Integrity or provenance checks are performed, but they do not provide sufficient assurance for all software, components or updates. PE-3: Verification outcomes are recorded for some software, components or updates prior to being introduced into systems, but not consistently. PE-4: Compensating controls exist for some unverifiable components but are not formally approved or time-bound.	FE-1: Verification of integrity and provenance is performed for software, components and updates across all relevant categories, and provenance is verified where suitable supplier evidence is available. FE-2: Verification uses one or more mechanisms appropriate to the software, component, update and source to provide reliable assurance of integrity and provenance. FE-3: Verification outcomes are recorded and available for review. FE-4: Where verification cannot be performed, compensating controls are applied, exceptions are time-bound and remediation paths are documented.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1791, ISM-1792, ISM-1790, ISM-2027, ISM-2055
E8	N/A
CSF	GV.SC-06, PR.PS-02
800-171r3	03.17.03, 03.04.08
AESCSF	ARCHITECTURE-4g, THIRD-PARTIES-2j, ARCHITECTURE-4e, ASSET-4e

IT.PRO-16.2

Action: Use vendor advisories and threat intelligence to maintain awareness of supplier, product and component exposure to compromise, and act within timeframes proportionate to the risk.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Supply Chain Compromise](#), [Server Software Component](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No monitoring is performed for indicators of supply chain compromise affecting software, components or services in use.	PE-1: Monitoring occurs but does not draw on relevant threat intelligence sources or does not cover all in-scope systems.	FE-1: Monitoring covers software, components and services in use, drawing on relevant threat intelligence sources.
NE-2: Vendor security notifications and threat advisories are not reviewed or actioned.	PE-2: Notifications and advisories are reviewed but exposure assessment and response are not conducted in a timely manner.	FE-2: Vendor security notifications and threat advisories are reviewed, exposure is assessed and response actions are initiated within defined timeframes.
NE-3: When supply chain compromise is identified, neither containment nor investigation is performed.	PE-3: Containment occurs but investigation for evidence of exploitation is not consistently undertaken.	FE-3: Identified supply chain compromises are responded to in timeframes defined by the organisation.
NE-4: Supply chain compromise events are integrated into neither incident response nor risk management.	PE-4: Some integration exists but findings are not reflected in the risk register or incident response procedures.	FE-4: Supply chain compromise events are integrated with incident response and reflected in the risk register.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-2116
E8	N/A
CSF	ID.RA-02, DE.CM-09, DE.CM-06
800-171r3	03.17.03
AESCSF	THIRD-PARTIES-2f

PRO-13 - Identity, credential and access management

Principle: Robust and secure identity, credential and access management is used to establish, maintain and control access to systems (infrastructure, operating systems, applications and data) and to support effective detection of identity and credential misuse.

IT.PRO-13.1

Action: Identify and disable or remove default and unused accounts regularly, permitting exceptions only where the account is documented, justified, hardened and monitored.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Valid Accounts](#), [Brute Force](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No review of default or unused accounts has been conducted within the review period defined by the organisation. NE-2: Default vendor accounts remain enabled on production systems without appropriate documentation, justification, hardening and monitoring in place for their use. NE-3: No process exists to identify accounts that have not authenticated within a defined period.	PE-1: A review has been conducted but does not cover all assets. PE-2: Default accounts have been identified but some remain enabled without documented justification. PE-3: Unused accounts are identified but remediation is incomplete or delayed beyond defined timeframes.	FE-1: A review of accounts has been completed within the defined review period covering all assets. FE-2: Default accounts are disabled or have approved justification for remaining active, with appropriate monitoring and compensating controls for their use in place. FE-3: Accounts that show no evidence of use, other than approved emergency access accounts, are identified and either disabled or removed in accordance with defined timeframes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0383, ISM-0380, ISM-1260
E8	ISM-1648, ISM-1647
CSF	PR.AA-01, PR.AA-05
800-171r3	03.01.01, 03.05.12
AEESCF	ACCESS-1c, ACCESS-1f, ACCESS-1j, ACCESS-1e

IT.PRO-13.2

Action: Store authentication keys, secrets and tokens in approved secure repositories with access controls, including MFA.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** [Unsecured Credentials](#), [Credentials from Password Stores](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Credentials are stored in plaintext, spreadsheets, shared drives or other unapproved locations as standard practice. NE-2: No approved secure repository is in use to store authentication keys, secrets and tokens. NE-3: Access to credential stores is neither controlled nor audited. NE-4: Access controls such as MFA are not enabled for authentication to secure repositories	PE-1: An approved secure repository is in use but does not cover all authentication keys, secrets and tokens within scope. PE-2: Access controls for secure repositories are in place but access logging is not enabled or not reviewed. PE-3: Access controls such as MFA are enabled for authentication to secure repositories, but are not enforced.	FE-1: All authentication keys, secrets and tokens within scope are stored in approved secure repositories. FE-2: Access to secure repositories is restricted using attribute or role-based access controls, multi-factor authentication is enforced for all applicable authentication pathways, and access is logged and reviewed.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1402, ISM-1957
E8	ISM-1505, ISM-1894
CSF	PR.AA-01, PR.AA-02, PR.DS-01, PR.DS-02
800-171r3	03.05.12, 03.13.10, 03.05.03, 03.13.08
AESCSF	ACCESS-1b, ARCHITECTURE-5e, ACCESS-1h, ARCHITECTURE-5a

IT.PRO-13.3

Action: Identify and remediate unsecured keys, secrets and credentials by regularly scanning codebases, configuration files, file shares and user collaboration platforms.

Domains: Visibility and response; **Mitigated Techniques:** [Valid Accounts](#), [Unsecured Credentials](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No secret scanning capability is deployed. NE-2: No process exists to identify credentials exposed in codebases, configuration files, file shares or user collaboration platforms. NE-3: Unsecured keys, secrets and credentials found exposed in codebases, configuration files, scripts, file shares or user collaboration platforms are left in place with no action taken.	PE-1: Secret scanning is deployed but does not cover all repositories, pipelines or user collaboration platforms. PE-2: Scanning runs but discovered credentials are not assessed in a timely manner. PE-3: Unsecured keys, secrets and credentials that are discovered are assessed, but are not rotated or revoked in a timely manner.	FE-1: Secret scanning tooling is deployed across codebases, configuration files, file shares and user collaboration platforms. FE-2: Scans to identify unsecured keys, secrets and credentials run on a regular schedule defined by the organisation. FE-3: Unsecured keys, secrets and credentials that are discovered are assessed, then rotated and/or revoked within timeframes defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1875, ISM-2030, ISM-1402
E8	N/A
CSF	PR.AA-01, ID.RA-01, DE.CM-09
800-171r3	03.05.12, 03.11.02, 03.05.07
AESCSF	ACCESS-1b, THREAT-1c, ARCHITECTURE-5a

IT.PRO-13.4

Action: Use phishing-resistant MFA for users authenticating to systems, including from untrusted, external or high-risk locations.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Valid Accounts](#), [Account Manipulation](#), [Brute Force](#), [Multi-Factor Authentication Request Generation](#), [Adversary-in-the-Middle](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Phishing-resistant MFA is not enforced for interactive user authentication to systems. NE-2: MFA is deployed but uses non-phishing-resistant methods, such as SMS, voice, or push-only authentication instead of phishing-resistant MFA. NE-3: No access policies differentiate between trusted and untrusted, external or high-risk locations. NE-4: Access from untrusted, external or high-risk locations is permitted without MFA, or with non-phishing-resistant MFA.	PE-1: Phishing-resistant MFA is deployed for some but not all systems within scope. PE-2: Access policies exist but do not cover all organisationally defined high-risk location categories. PE-3: Exceptions or alternative authentication pathways allow routine or recurring authentication without phishing-resistant MFA, or emergency access arrangements are not adequately restricted, monitored, tested or reviewed.	FE-1: Phishing-resistant MFA is enforced for all routine interactive user authentication to systems within scope. FE-2: Phishing-resistant MFA is enforced for routine authentication attempts from untrusted, external or high-risk locations. FE-3: Customer-facing services provide a phishing-resistant MFA option for authentication. FE-4: Emergency access arrangements are periodically tested and reviewed to confirm that they remain operational, appropriately protected and limited to their intended purpose. Credentials or authentication factors used for emergency access are securely managed and are not used for routine administration.

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-1504, ISM-1679, ISM-1680, ISM-1892, ISM-1893, ISM-1681, ISM-1401, ISM-1873, ISM-1173, ISM-0974, ISM-1872, ISM-1682, ISM-1505, ISM-1874, ISM-1894
CSF	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05
800-171r3	03.05.03, 03.05.04, 03.01.12
AESCSF	ACCESS-1h, ACCESS-1i, ACCESS-2g

IT.PRO-13.5

Action: Disable legacy authentication protocols or, where this is not feasible, restrict and monitor their use, apply compensating controls and establish a time-bound decommissioning plan.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Brute Force](#), [Valid Accounts](#), [Adversary-in-the-Middle](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Legacy authentication protocols that cannot enforce modern authentication controls remain enabled and in active use without restriction. NE-2: No assessment has been conducted to identify which legacy authentication protocols are in use within the environment. NE-3: Authentication mechanisms transmitting credentials in cleartext or using weak cryptographic primitives remain enabled and no action has been taken to disable them. NE-4: Where legacy protocols are retained, no compensating controls, no monitoring and no decommissioning timelines are in place.	PE-1: Legacy authentication protocols have been identified and are partially restricted but some remain enabled across systems within scope without justification. PE-2: An assessment has been conducted but does not cover all in-scope systems, or the inventory of legacy protocols in use is not maintained. PE-3: Some weak authentication mechanisms have been disabled but others remain enabled without documented justification or remediation plan. PE-4: Compensating controls exist for some retained legacy protocols but monitoring is inconsistent or decommissioning timelines are not defined.	FE-1: Legacy authentication protocols that cannot enforce modern authentication controls have been identified and disabled across systems within scope, excluding documented and risk-accepted exceptions. FE-2: An assessment of legacy authentication protocol use has been conducted across in-scope systems and the inventory is maintained. FE-3: Where retention is necessary, compensating controls are applied and decommissioning timelines are recorded and tracked. FE-4: Ongoing use of legacy authentication protocols is regularly risk reviewed, accepted and recorded in the organisations risk register.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1603, ISM-1055, ISM-0380
E8	N/A
CSF	PR.AA-03, PR.PS-01, PR.IR-01
800-171r3	03.05.04, 03.04.06
AESCSF	ARCHITECTURE-3d, ASSET-3a

IT.PRO-13.6

Action: Ensure that user, machine, system and service account credentials are unique per system or account, particularly in high-privilege contexts.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Brute Force](#), [Valid Accounts](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Local administrator credentials are shared across the device fleet, or service or privileged account credentials are routinely reused across systems. NE-2: Credential uniqueness is not enforced for applicable user, machine, system or service identities. NE-3: Credential uniqueness has not been addressed in high-privilege contexts, including domain administrations, cloud administration or automation platforms. NE-4: Where credential uniqueness cannot be enforced, neither compensating controls nor remediation paths are in place.	PE-1: Local administrator credential uniqueness has been implemented for some device populations but coverage is incomplete across the device fleet. PE-2: A technical mechanism is in place but applies to only a subset of credentials types or systems within scope. PE-3: Credential uniqueness has been addressed in some high-privilege contexts but gaps remain in others. PE-4: Compensating controls exist for some shared credentials but monitoring is inconsistent or remediation plans do not exist.	FE-1: Credentials for applicable local administrative accounts are unique to each system or account. FE-2: Credential uniqueness is consistently enforced for applicable user, machine, system and service identities. FE-3: Credential uniqueness is enforced consistently in high-privilege context, with managed identities or equivalent capabilities used in preference to shared static credentials wherever feasible. FE-4: Where uniqueness cannot be enforced, compensating controls are applied, the use of the shared credentials is monitored, and a remediation plan exists.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1596, ISM-1953, ISM-1227
E8	ISM-1685
CSF	PR.AA-01, PR.AA-03, PR.AA-05
800-171r3	03.05.01, 03.05.05, 03.05.12
AESCSF	ACCESS-1b, ACCESS-1g, ACCESS-1d

PRO-12 - Least privilege access

Principle: Users are granted the minimum access to systems (infrastructure, operating systems, applications and data) required to undertake their duties or functions.

IT.PRO-12.1

Action: Periodically review and update access privileges in alignment with current roles, duties and business requirements.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Account Manipulation](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Access privileges are not reviewed against current roles, duties and business requirements. NE-2: Access reviews do not identify privileges that are no longer required. NE-3: Access privileges are not updated when personnel roles, duties or business requirements change. NE-4: Access privileges are not mapped to roles, duties and business requirements.	PE-1: Access reviews are conducted for some accounts or systems, but coverage is incomplete. PE-2: Reviews identify excessive or obsolete privileges, but updates are incomplete or not completed within timeframes defined by the organisation. PE-3: A process to review access privileges exists but only occurs on an ad hoc basis. PE-4: Some access privileges are mapped to roles, duties and business requirements, but not all.	FE-1: Access privileges for all applicable accounts and systems are reviewed within a cycle defined by the organisation and aligned with current roles, duties and business requirements. FE-2: Privileges identified as excessive or obsolete are removed or updated within timeframes defined by the organisation. FE-3: Review outcomes and resulting access changes are documented and available as evidence. FE-4: Access privileges are mapped to current roles, duties and business requirements.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1852
E8	ISM-1507, ISM-1508, ISM-1647
CSF	PR.AA-05, PR.AA-01, GV.RM-02
800-171r3	03.01.05, 03.01.01, 03.01.04
AESCSF	ACCESS-2h, ACCESS-2f, ACCESS-1e

IT.PRO-12.2

Action: Grant only authorised administrative roles permissions to create, modify or delete accounts and roles, and access privileged functions or applications.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Create Account](#), [Account Manipulation](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Non-administrative users can create, modify or delete accounts or roles. NE-2: Delegated permissions are broad and have not been audited.	PE-1: Permissions are restricted to administrative roles but some delegated permissions are broader than required. PE-2: Approval workflows exist for some high-impact changes but not all.	FE-1: Only designated administrative roles can create, modify or delete accounts and roles. FE-2: Delegated permissions are audited and scoped to the minimum required. FE-3: Approval workflows are enforced for high-impact identity and access changes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1584
E8	ISM-1508, ISM-1507, ISM-1175
CSF	PR.AA-05, PR.AA-01, PR.AA-04
800-171r3	03.01.06, 03.01.07, 03.01.01, 03.04.05
AESCSF	ACCESS-2d, ACCESS-1g, ARCHITECTURE-3c

IT.PRO-12.3

Action: Provision user, administrative and non-person accounts with only the minimum access and privileges required to perform defined operational functions.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Create Account](#), [Account Manipulation](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Accounts are provisioned with broad default permissions that exceed operational requirements.	PE-1: Minimum privilege provisioning is defined but not consistently applied to all account types.	FE-1: All accounts are provisioned with documented minimum permissions aligned to defined operational functions.
NE-2: Administrative and day-to-day user functions share the same account, with no separate privileged accounts.	PE-2: Administrative accounts are separated from user accounts but some exceptions exist without documented justification.	FE-2: Separate accounts are allocated for privileged and day-to-day functions, and controls prevent privileged use from day-to-day context.
		FE-3: Non-person and service accounts are scoped to their specific integration requirements.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1852, ISM-1249, ISM-1619
E8	ISM-1508, ISM-1175, ISM-1883, ISM-0445
CSF	PR.AA-05, PR.AA-01, PR.AA-03
800-171r3	03.01.05, 03.01.06, 03.01.02, 03.01.01
AESCSF	ACCESS-2d, ACCESS-1g, ACCESS-2c

PRO-05 - Secure administration

Principle: Systems (infrastructure, operating systems, applications and data) are administered in a secure, accountable and auditable manner.

IT.PRO-05.1

Action: Ensure administrative activities can only be performed from dedicated and hardened environments that are isolated from unprivileged user workloads.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Exploitation for Privilege Escalation](#), [OS Credential Dumping](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Administrative access to systems is routinely performed from standard user devices without additional controls to protect the administrative session. NE-2: No dedicated or hardened administrative environment exists. NE-3: Exceptions to the use of dedicated administrative environments are neither identified nor assessed.	PE-1: A dedicated administrative environment has been established, but administrative access is not consistently routed through it. PE-2: Administrative endpoints have been hardened, but unprivileged user workloads or unnecessary functions remain accessible. PE-3: Exceptions are documented, but their justification, risk acceptance, compensating controls or review arrangements are incomplete or inconsistently applied.	FE-1: Administrative sessions originate from dedicated and hardened administrative environments that are isolated from unprivileged user workloads. Where this cannot be technically enforced, exceptions are documented, risk-assessed, formally accepted and protected by compensating controls. FE-2: Administrative environments are hardened and restricted to the functions required for authorised administration. FE-3: Exceptions are limited to systems or services that cannot support administration through a dedicated environment, are periodically reviewed and are removed when the technical limitation no longer applies.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1385
E8	ISM-1898, ISM-1380, ISM-1688, ISM-1689, ISM-1387
CSF	PR.AA-05, PR.IR-01, PR.PS-01, PR.IR-02
800-171r3	03.01.06, 03.04.06, 03.13.01, 03.01.12
AESCSF	ARCHITECTURE-3c, ARCHITECTURE-2e, ARCHITECTURE-2d

IT.PRO-05.2

Action: Enforce explicit session establishment controls before privileged actions are permitted, including the use of time-bound privilege grants.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Use Alternate Authentication Material](#), [Steal or Forge Kerberos Tickets](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Privileged access is standing and does not require explicit activation or time-bound grants, excluding approved break-glass and emergency access accounts. NE-2: No re-authentication or step-up authentication is required before privileged sessions.	PE-1: Time-bound access is implemented for some privileged roles but standing access remains for others. PE-2: Session duration limits exist but are not consistently enforced or are set excessively long.	FE-1: Time-bound privilege grants are enforced for applicable privileged roles, with defined maximum session durations and approved emergency access arrangements. FE-2: Re-authentication or step-up authentication is required before privilege activation. FE-3: All privilege activations are logged with activating user, role and timeframes.

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-1649
CSF	PR.AA-03, PR.AA-04, PR.AA-05
800-171r3	03.01.12, 03.05.03, 03.01.11
AESCSF	ACCESS-1g, ACCESS-2g, ACCESS-1h

IT.PRO-05.3

Action: Record all administrative or management actions that modify systems, configurations or controls, including the details of the associated user, timestamp and target.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** [Disable or Modify Tools](#), [Modify Registry](#), [Create or Modify System Process](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Administrative or management actions that modify systems, configurations or controls are not logged. NE-2: Logs do not capture sufficient detail to identify who made a change, when and to what target.	PE-1: Logging is enabled and provides useful coverage, but does not cover all applicable administrative or management platforms. PE-2: Logs capture the administrator identity and action but lack detail on the target or change nature.	FE-1: Comprehensive audit logging to capture all administrative or management actions is enabled on all platforms in scope. FE-2: Logs capture administrator identity, timestamp, target object and nature of change.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1509, ISM-0585, ISM-1566
E8	ISM-1509, ISM-1650
CSF	PR.PS-04, DE.CM-03, DE.AE-03
800-171r3	03.01.07, 03.03.01, 03.03.02, 03.03.03
AESCSF	SITUATION-1a, ASSET-4i, ACCESS-2i

PRO-04 - Secure configuration management

Principle: Systems (infrastructure, operating systems and applications) are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced.

IT.PRO-04.1

Action: Define approved configuration baselines, informed by vendor and industry hardening guidance, that disable or remove unnecessary services, insecure settings, and unsupported or weak communication protocols.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Server Software Component](#), [Windows Management Instrumentation](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No documented configuration baseline exists for assets.	PE-1: A baseline exists but does not address all applicable asset types.	FE-1: A documented and approved baseline exists for all applicable asset types.
NE-2: Systems are deployed with vendor defaults and no documented hardening has been applied.	PE-2: The baseline is documented but has not been reviewed or updated within the cycle defined by the organisation. PE-3: The baseline exists but rationale for configuration decisions is not documented.	FE-2: The baseline disables or removes unnecessary services, insecure settings, and unsupported or weak communication protocols. FE-3: Configuration decisions are documented with rationale to support drift assessment. FE-4: The baseline is reviewed and updated on a cycle defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1914, ISM-0380, ISM-1409, ISM-1916, ISM-1603
E8	ISM-1654, ISM-1486, ISM-1485, ISM-1488, ISM-1585, ISM-1671, ISM-1667, ISM-1668, ISM-1669, ISM-1542, ISM-1859, ISM-1412, ISM-1670, ISM-1860, ISM-1673, ISM-1823, ISM-1824, ISM-1655, ISM-1621, ISM-1622, ISM-1675, ISM-1891, ISM-0304, ISM-1896, ISM-1861, ISM-1686, ISM-1897
CSF	PR.PS-01, PR.PS-02, PR.PS-03, PR.IR-01
800-171r3	03.04.02, 03.04.06, 03.04.01, 03.16.02
AESCSF	ASSET-3a, ARCHITECTURE-3d, ARCHITECTURE-3e, ASSET-3c

IT.PRO-04.2

Action: Deploy approved configuration baselines on systems, including infrastructure, operating systems and applications.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Exploit Public-Facing Application, External Remote Services, User Execution;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Approved baselines have not been applied to assets. NE-2: Baseline deployment has not been validated through technical assessment.	PE-1: Approved baselines have been implemented where available, but some relevant asset types are not covered by an approved baseline. PE-2: Deployment has occurred but validation through technical assessment is incomplete or not current. PE-3: Approved baselines have been deployed, but coverage for all applicable assets is inconsistent.	FE-1: Approved baselines have been applied to all applicable assets. FE-2: Deployment has been validated through technical assessment. FE-3: Coverage metrics are available demonstrating deployment completeness.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1914, ISM-1409, ISM-1246, ISM-1635
E8	ISM-1672, ISM-1489, ISM-1859, ISM-1412, ISM-1860, ISM-1622
CSF	PR.PS-01, PR.PS-02, PR.PS-05, DE.CM-09
800-171r3	03.04.01, 03.04.02, 03.04.03
AESCSF	ASSET-3b, ASSET-3c, ARCHITECTURE-3e

IT.PRO-04.3

Action: Detect and respond to configuration drift using scheduled technical assessments and, where supported, automated monitoring, based on system criticality and change rate.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Disable or Modify Tools, Modify Registry;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No mechanism exists to detect configuration drift from approved baselines.	PE-1: Drift detection is in place but does not cover all applicable assets.	FE-1: Automated configuration monitoring or regular technical assessments detect drift across the applicable assets, occurring at a frequency based on system criticality and change rate.
NE-2: Assessments to detect configuration drift have not been conducted within the review period defined by the organisation.	PE-2: Drift is detected but the remediation process is informal or response timeframes are not defined.	FE-2: A documented remediation process exists with defined response timeframes aligned to severity.
NE-3: Assessments do not systematically identify instances of configuration drift for assets.		FE-3: Drift events are tracked to closure with evidence of remediation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1211, ISM-1526
E8	ISM-1582
CSF	PR.PS-01, DE.CM-09, DE.AE-02
800-171r3	03.04.03, 03.04.04, 03.12.03, 03.14.06
AESCSF	ASSET-3e, ASSET-4i

PRO-06 - Vulnerability management

Principle: Vulnerabilities in systems (infrastructure, operating systems, applications and data) are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.

IT.PRO-06.1

Action: Identify known software and configuration weaknesses of assets through continuous and repeatable assessment activities, including vulnerability scanning activities.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Exploit Public-Facing Application](#), [Exploitation for Privilege Escalation](#), [Exploitation of Remote Services](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Vulnerability scanning activities are not undertaken.	PE-1: Vulnerability scanning is deployed but does not cover all applicable assets.	FE-1: All applicable assets are included in routine vulnerability scanning, and scanning frequency enables timely response.
NE-2: No routine vulnerability assessment activity has been conducted within a period defined by the organisation.	PE-2: Vulnerability scans are conducted but results are not reviewed and prioritised within timeframes defined by the organisation.	FE-2: Scanning covers both software vulnerabilities and configuration weaknesses.
NE-3: Advisories for relevant software and configuration weaknesses for organisational assets are not reviewed and assessed for impact.	PE-3: Vulnerability scans are conducted but frequency is not regular enough to enable timely response.	FE-3: Results are reviewed and prioritised within timeframes defined by the organisation.
	PE-4: Scanning covers software vulnerabilities but not configuration weaknesses.	FE-4: Advisories for relevant software and configuration weaknesses in all organisational assets are regularly reviewed and assessed for impact.
	PE-5: Advisories for relevant software and configuration weaknesses for organisational assets are reviewed on an ad hoc basis, or only for some assets.	

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-1808, ISM-1698, ISM-1699, ISM-1700, ISM-1701, ISM-1702, ISM-1703, ISM-1900, ISM-1807
CSF	ID.RA-01, ID.RA-05, DE.CM-09
800-171r3	03.11.02, 03.12.03, 03.14.01
AESCSF	THREAT-1c, THREAT-1f, THREAT-1b

IT.PRO-06.2

Action: Apply security patches or updates within defined risk-based timeframes or automatically where operational impact is low.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Exploit Public-Facing Application](#), [Exploitation for Privilege Escalation](#), [Exploitation of Remote Services](#), [Exploitation for Client Execution](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No defined patching timeframes exist for applicable assets. NE-2: Patches are not applied or are applied on an ad hoc basis with no tracking.	PE-1: Expected patching timeframes are defined by the organisation but are not consistently met. PE-2: Patches are applied but compensating controls are not documented where operational constraints prevent timely patching. PE-3: Patching coverage metrics exist but show significant gaps.	FE-1: Risk-based patching timeframes defined by the organisation are in place and consistently met. FE-2: Patching is prioritised based on vulnerability severity, exposure and exploit availability. FE-3: Where operational constraints prevent timely patching, compensating controls are documented and approved. FE-4: Patching coverage metrics account for all applicable assets, with any exclusions identified and formally risk-accepted. FE-5: Automatic patching of assets is applied where available and the organisation has determined operational impact is low.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0298, ISM-1143
E8	ISM-1691, ISM-1695, ISM-1876, ISM-1690, ISM-1877, ISM-1694, ISM-1693, ISM-1692, ISM-1901, ISM-1696, ISM-1902, ISM-1879, ISM-1697, ISM-1903, ISM-1904
CSF	ID.RA-01, PR.PS-02, PR.PS-03, RS.MA-04
800-171r3	03.14.01, 03.14.03, 03.04.03
AESCSF	THREAT-1d, THREAT-1h, ASSET-4e

IT.PRO-06.3

Action: Remediate or mitigate vulnerabilities exceeding defined risk thresholds within defined timeframes based on exploitation, exposure, criticality, impact and compensating controls, and verify treatment effectiveness.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** [Exploit Public-Facing Application](#), [Exploitation for Privilege Escalation](#), [Exploitation of Remote Services](#), [Exploitation for Client Execution](#);

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No risk thresholds are defined for vulnerability remediation. NE-2: Vulnerabilities exceeding acceptable risk levels are not tracked or remediated.	PE-1: Risk thresholds are defined but vulnerabilities exceeding them are not consistently remediated within defined timeframes. PE-2: Compensating controls are applied in some cases but are not formally documented or approved.	FE-1: Risk thresholds defined by the organisation exist, and vulnerabilities exceeding them are remediated or have approved compensating controls within organisationally defined timeframes. FE-2: Remediation and mitigation actions are tracked to closure with verification that actions reduced the risk as intended. FE-3: The process is sustained, with historical data demonstrating consistent performance across organisationally defined reporting periods.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1921, ISM-1809
E8	ISM-1691, ISM-1695, ISM-1876, ISM-1690, ISM-1877, ISM-1694, ISM-1693, ISM-1692, ISM-1901, ISM-1696, ISM-1902, ISM-1879, ISM-1697, ISM-1903, ISM-1904
CSF	ID.RA-01, ID.RA-05, GV.RM-06
800-171r3	03.11.02, 03.11.04, 03.14.01, 03.12.02
AESCSF	THREAT-1d, THREAT-1g, THREAT-1i, RISK-2i

PRO-07 - Trustworthy software

Principle: Systems (operating systems and applications) only permit the execution of software that is supported, verified and authorised.

IT.PRO-07.1

Action: Permit only supported, verified and organisation-authorised software to execute on systems, with exceptions minimised, formally risk accepted, time-bound, monitored and regularly reviewed.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Disable or Modify Tools, User Execution, Command and Scripting Interpreter, Windows Management Instrumentation, Process Injection, System Binary Proxy Execution;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Unsupported, unverified or unauthorised software can execute without restriction.	PE-1: Execution restriction controls are deployed but do not cover all applicable assets.	FE-1: Controls restrict execution to supported, organisation-authorised and integrity-verified software on all applicable assets.
NE-2: The list of approved software does not exist.	PE-2: The organisation maintains a list of approved software, but it has not been reviewed within timeframes defined by the organisation.	FE-2: The organisation maintains a list of approved software and reviews it within the timeframes defined by the organisation.
	PE-3: Execution restrictions are in place but integrity verification of approved software is not performed.	FE-3: Integrity of permitted software is verified using trusted mechanisms appropriate to the software and its source.
	PE-4: Exceptions to execution restrictions are granted without formal approval or time-bounding.	FE-4: Exceptions are formally approved, documented, time-bound and reviewed on a regular cycle defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-0843, ISM-1582, ISM-1870, ISM-1657, ISM-1488, ISM-1672, ISM-1490, ISM-1871, ISM-1544, ISM-1673, ISM-1656, ISM-1658, ISM-1659, ISM-1674, ISM-1890, ISM-1487, ISM-1675, ISM-1891
CSF	PR.PS-01, PR.PS-05, DE.CM-09
800-171r3	03.04.08, 03.04.06, 03.16.01, 03.14.02
AESCSF	ARCHITECTURE-3m, ARCHITECTURE-4g, ARCHITECTURE-3b

IT.PRO-07.2

Action: Restrict administrative and management tooling to approved software sets and executed from only authorised, known locations.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Disable or Modify Tools, User Execution, Command and Scripting Interpreter, Windows Management Instrumentation, Process Injection, System Binary Proxy Execution;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No approved administrative toolset is defined.	PE-1: An approved toolset is defined but not consistently enforced across all assets.	FE-1: A defined and enforced approved toolset exists for administrative and management activities, and execution is limited to authorised, known locations.
NE-2: No restrictions are placed on the location administrative tooling can be executed from.	PE-2: Administrative tooling is configured to execute from known locations, but privileged users can still run tooling from unapproved locations.	FE-2: Administrative and management tooling outside the approved set is blocked from execution, including from unauthorised locations.
NE-3: No controls prevent unapproved administrative tools, including tools commonly used in post-compromise activity, from executing on managed assets.	PE-3: Some unapproved administrative tools are blocked but enforcement gaps exist.	

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1392, ISM-0846
E8	ISM-1898, ISM-1657
CSF	PR.AA-05, PR.PS-01, PR.PS-05, DE.CM-09
800-171r3	03.04.08, 03.01.06, 03.07.04, 03.04.05
AESCSF	ARCHITECTURE-3m, ARCHITECTURE-3c, ACCESS-1g

PRO-10 - Regular and proven backups

Principle: Systems (infrastructure, operating systems, applications and data) are regularly backed up in a secure and proven manner, including through the validation of restoration capabilities.

IT.PRO-10.1

Action: Back up important data, applications and settings on a defined schedule to secure, resilient storage protected by encryption and immutable, offline, logically isolated or equivalent controls.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Data Encrypted for Impact, Inhibit System Recovery;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No managed backup process exists for important data, applications and settings. NE-2: Backup storage is neither encrypted nor protected by immutable, offline, logically isolated or equivalent controls.	PE-1: Important data, applications and settings are backed up, but backup schedules are not defined, do not cover all important assets, or are not consistently met. PE-2: Backups are encrypted but no immutable, offline, logically isolated or equivalent resilience controls are consistently applied. PE-3: Backups use immutable, offline, logically isolated or equivalent controls, but encryption is not consistently enforced.	FE-1: All important data, applications and settings are backed up according to schedules defined by the organisation and aligned with their recovery requirements. FE-2: Backups schedules are monitored, and missed or unsuccessful backups are identified, investigated and remediated within timeframes defined by the organisation. FE-3: Backup storage is encrypted and protected by immutable, offline, logically isolated or equivalent controls.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1547
E8	ISM-1511, ISM-1811, ISM-1810
CSF	PR.DS-01, PR.DS-11, RC.RP-03
800-171r3	03.08.09, 03.13.11
AESCSF	RESPONSE-4b, RESPONSE-4j, ARCHITECTURE-5b

IT.PRO-10.2

Action: Isolate backup repositories from general user environments and production workloads, ensuring they are separated from primary systems to prevent unauthorised access, modification or deletion.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Data Encrypted for Impact, Data from Local System, Inhibit System Recovery;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Backup repositories are accessible from the production environment or by production administrators.	PE-1: Backup repositories are logically separated but use credentials managed by the same identity platform as production.	FE-1: Backup repositories are isolated from production environments and general user access.
NE-2: Compromise of a system would provide a direct path to access, modify or delete its own backups.	PE-2: Isolation is implemented but has not been tested or validated.	FE-2: Access is controlled through credentials and administrative paths isolated from compromise of the primary identity environment.
		FE-3: Isolation has been validated to confirm that compromise of a system does not provide access to backups.

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-1811, ISM-1812, ISM-1814, ISM-1813, ISM-1706, ISM-1708
CSF	PR.DS-01, PR.DS-11, PR.IR-01, PR.AA-05
800-171r3	03.08.09, 03.08.02, 03.01.02
AESCSF	RESPONSE-4k, RESPONSE-4j, ARCHITECTURE-2d

IT.PRO-10.3

Action: Conduct regular testing of backup and restoration procedures to ensure that backups are reliable and capable of meeting defined recovery time objectives and recovery point objectives.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Data Encrypted for Impact, Inhibit System Recovery;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No restoration test has been conducted within the test cycle defined by the organisation.	PE-1: Restoration testing has been conducted but does not cover all important assets.	FE-1: Restoration testing covering important assets is conducted within the test cycle defined by the organisation.
NE-2: No backup or restoration procedures exist.	PE-2: Backup procedures exist but have never been tested.	FE-2: Testing validates that restoration meets the expected recovery time and recovery point objectives.
NE-3: Restoration testing demonstrates that backups cannot be restored, or consistently fail to meet defined recovery time or recovery point objectives.	PE-3: Testing has been conducted but coverage is incomplete or some tests did not meet the expected recovery time or recovery point objectives.	FE-3: Test results are documented and gaps identified during testing are remediated.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1548
E8	ISM-1515, ISM-1511
CSF	PR.DS-11, RC.RP-03, RC.RP-04, RC.RP-05
800-171r3	03.08.09, 03.06.03
AESCSF	RESPONSE-4b, RESPONSE-4f

PRO-18 - Network segmentation and segregation

Principle: Systems (infrastructure, operating systems and applications) are segmented into network zones based on business criticality and trust levels, with only authorised, controlled and monitored inbound and outbound communication paths between network zones permitted.

IT.PRO-18.1

Action: Isolate systems within network zones based on business criticality and trust level, and restrict and monitor inbound and outbound access to explicitly approved pathways and services.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Exploit Public-Facing Application, External Remote Services;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Systems are deployed on shared or flat network segments with no segregation between functions or trust levels.	PE-1: Network segmentation has been implemented but does not cover all in-scope systems, or segments are defined inconsistently.	FE-1: Systems within scope are deployed in network segments defined according to function, criticality and trust level, with segmentation applied consistently.
NE-2: No access controls restrict network access from external or general user networks to in-scope systems.	PE-2: Access controls exist between segments, but deny-by-default is not enforced, or some pathways are permitted without documented approval.	FE-2: Deny-by-default access controls are enforced between segments, with access from external and general user networks limited to documented and approved pathways.
NE-3: Segmentation is documented or administratively defined but not enforced by technical controls.	PE-3: Technical enforcement is in place for some segments but relies on a single mechanism that does not provide meaningful isolation.	FE-3: Segmentation is enforced through network-layer technical controls that provide meaningful isolation.
NE-4: Segmentation has not been validated through technical assessment.	PE-4: Validation has been performed for some segments but not consistently across in-scope systems, or validation is out of date.	FE-4: Segmentation has been validated through technical assessment with results documented and gaps remediated.
	PE-5: Pathways are reviewed but findings are not actioned, or the review cycle is not defined by the organisation.	FE-5: Approved pathways are reviewed on a regular cycle defined by the organisation, with unjustified pathways removed and changes reflected in the access control configuration.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1181, ISM-0520, ISM-1577, ISM-1385
E8	N/A
CSF	PR.IR-01, PR.AA-05, PR.PS-01
800-171r3	03.13.01, 03.13.06, 03.01.03
AESCSF	ARCHITECTURE-2b, ARCHITECTURE-2d, ARCHITECTURE-2h

IT.PRO-18.2

Action: Limit lateral movement between, and within, network segments to explicitly approved pathways and services, based on business requirements and trust levels.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Remote Services, Lateral Tool Transfer;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No controls limit lateral movement between or within network segments.	PE-1: Controls limit lateral movement between segments but no controls operate within segments.	FE-1: Controls limit lateral movement both between and within segments, with deny-by-default applied at each boundary.
NE-2: Lateral movement is permitted by default across the environment, with restrictions applied only on an exception basis.	PE-2: Restrictions are applied to some pathways, but the default position remains permissive in parts of the environment.	FE-2: Pathways and services are explicitly approved based on documented business requirements and trust levels, with all other lateral movement denied.
NE-3: Approved pathways are not documented.	PE-3: Approved pathways are documented but documentation is out of date or incomplete.	FE-3: Approved pathways are documented, reflect the current configuration and identify the business requirement and trust relationship justifying each.
NE-4: Lateral movement controls have not been validated through technical assessment.	PE-4: Validation has been performed but does not cover all in-scope segments, or is out of date.	FE-4: Lateral movement controls have been validated through technical assessment with results documented and gaps remediated
NE-5: Pathways and services are not reviewed after initial approval.	PE-5: Pathways are reviewed, but findings are not actioned, or the review cycle is not defined by the organisation.	FE-5: Pathways and services are reviewed on a regular cycle defined by the organisation, with unjustified pathways removed and the configuration updated to reflect approved changes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1182, ISM-1181, ISM-0520
E8	ISM-1380
CSF	PR.IR-01, PR.AA-05, DE.CM-01
800-171r3	03.13.06, 03.13.01, 03.01.03
AESCSF	ARCHITECTURE-2h, ARCHITECTURE-2i, ARCHITECTURE-2e

PRO-09 - Content filtering

Principle: Data communicated between different security domains for systems (infrastructure and applications) is controlled and subject to inspection and verification.

IT.PRO-09.1

Action: Inspect outbound content flows to detect unauthorised transfer of sensitive or high-value data.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems; **Mitigated Techniques:** Exfiltration Over C2 Channel, Exfiltration Over Alternative Protocol, Proxy;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No outbound content inspection is deployed.	PE-1: Outbound inspection is deployed but does not cover all applicable egress paths.	FE-1: Outbound content inspection is deployed covering all applicable egress paths.
NE-2: Sensitive data can leave the organisation through any egress path without detection or control.	PE-2: Rules are configured but do not cover all classified, regulated or high-value data types.	FE-2: Rules are configured to detect unauthorised transfer of classified, regulated and high-value data.
	PE-3: Alerts are generated but are not triaged or acted upon in a timely manner.	FE-3: Alerts are triaged and responded to within accepted risk timeframes defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1237, ISM-0659, ISM-0963
E8	N/A
CSF	PR.DS-02, DE.CM-01, DE.CM-06, PR.IR-01
800-171r3	03.01.03, 03.13.01, 03.14.06
AESCSF	ARCHITECTURE-5f, SITUATION-2d, ARCHITECTURE-5c

IT.PRO-09.2

Action: Block outbound network connections to known malicious or untrusted destinations.

Domains: Boundary services, Critical processes and services; **Mitigated Techniques:** Phishing, User Execution, Exfiltration Over C2 Channel, Exfiltration Over Alternative Protocol, Proxy;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No controls are deployed to prevent systems from establishing outbound connections to known malicious or untrusted destinations.	PE-1: Controls to prevent outbound connections being established are deployed but cover only a subset of in-scope systems or egress paths.	FE-1: Controls are deployed and applied across in-scope systems, egress paths, services, and network boundaries.
NE-2: Blocking decisions are not informed by current threat intelligence.	PE-2: Threat intelligence is used to inform block decisions for outbound connections, but updates are infrequent, manual or limited to a single source.	FE-2: Blocking decisions draw on current threat intelligence, with destination lists updated on a cycle defined by the organisation.
NE-3: Destination categorisation is not used.	PE-3: Categorisation is in place, but the categories blocked do not reflect the organisation's risk position.	FE-3: Destination reputation, category and age are considered alongside threat intelligence, with category-based blocking aligned to the organisation's risk position.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0958, ISM-1 236, ISM-1 171, ISM-0963
E8	N/A
CSF	PR.IR-01, DE.CM-01, PR.PS-01
800-171r3	03.13.01, 03.13.06, 03.01.03
AESCSF	ARCHITECTURE-2e, ARCHITECTURE-3m, SITUATION-2d

IT.PRO-09.3

Action: Inspect inbound content from external or untrusted sources to prevent delivery of malicious or unsafe content.

Domains: Boundary services, Critical processes and services; **Mitigated Techniques:** Phishing, Remote Services, Ingress Tool Transfer;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No inbound content inspection is deployed.	PE-1: Inbound inspection is deployed but does not cover all applicable content channels. PE-2: Inspection is in place but detection signatures or rules are not maintained or updated.	FE-1: Inbound content inspection covers all applicable content channels. FE-2: Detection signatures and rules are maintained and updated on a regular cycle defined by the organisation. FE-3: Blocked content is logged and available for review. FE-4: Current cyber threat intelligence is considered when implementing controls to prevent the delivery of malicious or unsafe content.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0659, ISM-0651, ISM-0652, ISM-1234, ISM-0963
E8	N/A
CSF	PR.IR-01, DE.CM-01, PR.DS-02
800-171r3	03.13.01, 03.14.02, 03.13.13
AESCSF	ARCHITECTURE-3b, ARCHITECTURE-2e, THREAT-2d

PRO-14 - Cyber security awareness training

Principle: Personnel are provided with ongoing cyber security awareness training, including operational security considerations, tailored to their duties, access levels and current cyber threats.

IT.PRO-14.1

Action: Ensure all personnel receive cyber security awareness training, that is tailored to how they will interact with systems, applications and data in their assigned roles, before being granted access to organisational systems and data.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** Phishing, Valid Accounts;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No requirement exists for personnel to complete cyber security awareness training before being granted access to critical, privileged or business systems. NE-2: No training completion records are maintained.	PE-1: A training program exists but is not tailored to the specific risks of the systems in-scope. PE-2: A requirement to complete training before access is granted exists but is not consistently enforced. PE-3: Completion records are maintained but show significant gaps in coverage.	FE-1: Role-tailored training programs address the specific risks, data handling obligations and incident reporting requirements relevant to in-scope systems. FE-2: All personnel complete role-tailored training before being granted access to organisational systems and data, with refresher training mandated within a cycle defined by the organisation. FE-3: Completion records are maintained and demonstrate full coverage.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0252, ISM-1565, ISM-0435, ISM-1865
E8	N/A
CSF	PR.AT-01, PR.AT-02, GV.RR-04
800-171r3	03.02.01, 03.02.02, 03.15.03
AESCSF	WORKFORCE-2a, WORKFORCE-2e, WORKFORCE-4d

IT.PRO-14.2

Action: Update and provide cyber security awareness training on a regular basis to reflect current threats and operational considerations.

Domains: Governance and culture; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No cyber security awareness training program exists. NE-2: Cyber security awareness training is not reviewed or updated after initial deployment. NE-3: Lessons learnt from cyber security incidents are not incorporated into training content. NE-4: The cadence of review is not defined.	PE-1: Training is reviewed but updates do not reflect current threat intelligence, sector relevant adversary techniques or organisational changes. PE-2: Some lessons are incorporated but the process is informal, or coverage is limited to a small number of incidents. PE-3: Some changes are reflected, but training is not updated to address recently introduced systems or significant changes to working arrangements. PE-4: A review cadence exists, but is not consistently met, or is not proportionate to the rate of change.	FE-1: Training content is reviewed and updated on a defined cycle, with updates reflecting current threat intelligence, adversary techniques relevant to the workforce and organisation's operating context. FE-2: Lessons learnt from cyber security incidents within the organisation or its sector are systematically incorporated into training content. FE-3: Training reflects the systems, platforms and working arrangements that personnel currently interact with, including newly introduced platforms and changes to ways of working. FE-4: The cadence of review is defined, proportionate to the rate of change in the threat environment, and consistently met.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-2022, ISM-1565
E8	N/A
CSF	PR.AT-01, GV.OC-03, ID.RA-02
800-171r3	03.02.01, 03.02.02
AESCSF	WORKFORCE-2d, WORKFORCE-2c, WORKFORCE-2g

Detect principles

DET-01 - Centralised event logging

Principle: Security-relevant event logs and configuration changes for systems (infrastructure, operating systems, applications and data) are centrally collected, protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation.

IT.DET-01.1

Action: Protect event logs from unauthorised access, modification or deletion, including by encrypting them during transit and at rest and securing the systems and accounts used to store, manage and analyse them.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Indicator Removal, Disable or Modify Tools;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Logs generated by applicable assets are not protected from modification or deletion.	PE-1: Logs are forwarded but integrity protections are not in place at the source.	FE-1: Logs are protected against modification or deletion.
NE-2: Log access is not restricted to authorised roles with a business need.	PE-2: Log access is restricted but some roles retain the ability to modify or delete logs.	FE-2: Logs are encrypted in transit and at rest.
NE-3: Logs are neither encrypted during transit nor at rest.	PE-3: Logs are encrypted during transit but are not protected with encryption at rest (or vice versa).	FE-3: Access to logs is restricted to authorised roles with a business need.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1985, ISM-1984
E8	ISM-1815
CSF	PR.DS-01, PR.DS-02
800-171r3	03.03.08, 03.13.08
AESCSF	ARCHITECTURE-5b, ACCESS-2d

IT.DET-01.2

Action: Forward high-value, security-relevant event logs and configuration changes from infrastructure, operating systems and applications to a central log storage capability.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** Indicator Removal, Disable or Modify Tools;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Security-relevant logs from assets are not forwarded to a central logging capability. NE-2: High-value, security relevant event logs or configuration changes from infrastructure, operating systems or applications are not forwarded.	PE-1: High-value, security-relevant event logs are forwarded, but coverage gaps are identified or completeness has not been validated. PE-2: Configuration change logs are forwarded inconsistently. PE-3: The utility of security log sources is reviewed, but on an ad hoc basis rather than according to a defined schedule. PE-4: Log forwarding is in place but latency is excessive for effective detection.	FE-1: High-value security-relevant event logs and configuration changes from all relevant infrastructure, operating systems and application sources are forwarded to the central logging capability. FE-2: Security log sources are reviewed at regular intervals to ensure their continued utility in detecting and responding to changing adversary techniques. FE-3: Log completeness has been validated against the expected log sources. FE-4: Logs are forwarded at a frequency that enables timely detection.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1405, ISM-1983, ISM-0585
E8	ISM-1509, ISM-1650, ISM-1660, ISM-1889, ISM-1623, ISM-1683
CSF	PR.PS-04, DE.CM-03, DE.AE-03, DE.CM-09
800-171r3	03.03.01, 03.03.03, 03.03.05, 03.01.07
AESCSF	SITUATION-1a, SITUATION-1c, SITUATION-1e

IT.DET-01.3

Action: Establish a centralised event log storage capability that protects logs from unauthorised access or modification.

Domains: Visibility and response; **Mitigated Techniques:** Indicator Removal, Disable or Modify Tools;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No centralised capability exists for storing event logs collected from systems across the environment.	PE-1: A centralised capability exists but does not receive logs from in-scope systems, or coverage is inconsistent.	FE-1: A centralised event log storage capability is in place for logs collected from in-scope systems.
NE-2: Stored logs have no protection against modification or deletion by administrators of the systems generating them.	PE-2: Stored logs are protected from modification, but the controls do not consistently prevent deletion, or controls are not applied to all log types.	FE-2: Stored logs are protected against unauthorised access, modification and deletion through technical controls including access restrictions, encryption at rest and integrity protection.
NE-3: Access to the centralised capability is not restricted, or access is granted to roles without a documented need.	PE-3: Access is restricted to a defined set of roles but access is not logged or monitored.	FE-3: Access to the centralised capability is restricted to security operations personnel and other roles with a documented need, with access logged and monitored.
NE-4: Log retention requirements are not defined.	PE-4: A retention period is defined but is inconsistently applied, or some log types are retained for shorter periods than required.	FE-4: Log retention requirements are defined and aligned to investigative, regulatory and contractual obligation, with retention applied consistently across log types.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1405, ISM-1985, ISM-1988
E8	ISM-1815
CSF	PR.PS-04, PR.DS-01, PR.AA-05
800-171r3	03.03.06, 03.03.08, 03.03.03
AESCSF	SITUATION-1e, SITUATION-1a, ACCESS-2d

DET-04 - Baseline high-risk access activities

Principle: Baseline patterns of identity and credential access activities, privileged access activities, and remote access activities are established and maintained for systems (infrastructure, operating systems, applications and data) to enable the detection of anomalous or unexpected behaviour.

IT.DET-04.1

Action: Continuously monitor and analyse software execution behaviour on systems to detect where legitimate tools and utilities are being used for malicious purposes.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments; **Mitigated Techniques:** Valid Accounts, System Binary Proxy Execution, Command and Scripting Interpreter;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No monitoring or equivalent analysis is used to identify anomalous or unexpected use of legitimate tools and utilities on applicable systems. NE-2: Existing controls do not provide a reasonable capability to detect security-relevant patterns of legitimate software being used for malicious purposes.	PE-1: Monitoring or equivalent analysis covers some priority tools, execution behaviours or applicable systems, but risk-significant coverage gaps exist. PE-2: Security-relevant execution telemetry is collected, but detection rules, behavioural analytics or equivalent analysis are incomplete or not consistently operational. PE-3: Alerts relating to anomalous or unexpected software execution are generated, but they are not consistently triaged and investigated within organisationally defined timeframes.	FE-1: The organisation identifies the legitimate tools, utilities and execution behaviours that present heightened risk of malicious use within applicable systems. FE-2: Security-relevant telemetry and contextual information are analysed using detection rules, behavioural analytics or equivalent methods to identify anomalous or unexpected use of priority tools and utilities. FE-3: Detection coverage is periodically reviewed and adjusted in response to changes in applicable systems, threat intelligence, observed activity and the organisation's risk profile. FE-4: Alerts are prioritised, triaged and investigated within timeframes defined according to their assessed security risk.

Potential evidence sources

Framework	References
ISM (excl. E8)	See E8 references
E8	ISM-1623, ISM-1660, ISM-1228, ISM-1907

Framework	References
CSF	DE.CM-03, DE.CM-09, DE.AE-02
800-171r3	03.14.06, 03.03.05
AESCSF	SITUATION-2d, SITUATION-2e

DET-02 - Cyber security event detection

Principle: Anomalous or unexpected events and behaviours for systems (infrastructure, operating systems, applications and data) are analysed in a timely manner to detect cyber security events.

IT.DET-02.1

Action: Ensure event logs are normalised, time-synchronised and enriched to support correlation across systems and environments.

Domains: Boundary services, Identity services, Critical processes and services, Privileged environments, Business systems, User devices; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Logs are not time-synchronised to an authoritative source. NE-2: Logs are ingested in raw format and are neither normalised nor enriched.	PE-1: Logs are time-synchronised but are not normalised to a common schema. PE-2: Some enrichment is applied but critical contextual data such as asset classification or account type is missing.	FE-1: Logs are time-synchronised to the authoritative time source. FE-2: Logs are normalised into the common log schema and enriched with contextual metadata. FE-3: Enriched logs support correlation across relevant systems, environments and data sources in the central logging platform.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1959, ISM-0988, ISM-0585, ISM-1405
E8	N/A
CSF	DE.AE-03, DE.AE-06, DE.CM-03, PR.PS-04
800-171r3	03.03.02, 03.03.07, 03.03.05, 03.03.06
AESCSF	SITUATION-1e, SITUATION-3f, RESPONSE-1d

IT.DET-02.2

Action: Ensure detection logic identifies unauthorised changes, anomalous authentication activity and suspicious software execution.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No detection logic is deployed to identify unauthorised changes, anomalous authentication activity or suspicious software execution events originating from assets.	PE-1: Detection logic exists but does not cover all three categories (unauthorised changes, anomalous authentication, suspicious execution).	FE-1: Detection logic is deployed, and unauthorised configuration changes, anomalous authentication patterns and suspicious process execution events are captured and produce alerts.
NE-2: Detection relies entirely on manual log review with no automated rules or alerting.	PE-2: Rules are deployed but are not tested or tuned on a regular cycle defined by the organisation.	FE-2: Detection logic is tested and tuned on a regular cycle defined by the organisation to maintain effectiveness.
		FE-3: Detection coverage is reviewed following cyber security incidents or significant environmental changes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1986, ISM-2116
E8	ISM-0109, ISM-1683, ISM-1660
CSF	DE.CM-01, DE.CM-03, DE.CM-09, DE.AE-02, DE.AE-07
800-171r3	03.14.06, 03.03.05, 03.01.07
AESCSF	SITUATION-2d, ACCESS-2i, SITUATION-2e

DET-03 - Cyber security incident identification

Principle: Cyber security events are analysed in a timely manner to identify cyber security incidents.

IT.DET-03.1

Action: Triage alerts and events in a timely manner to determine whether cyber security incident thresholds have been met.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No documented triage process exists.	PE-1: A triage process exists but response times are not defined or consistently met.	FE-1: A documented triage process with defined severity thresholds and response timeframes is in place.
NE-2: Alerts are routinely ignored or left unreviewed.	PE-2: Severity thresholds are defined but escalation procedures are informal.	FE-2: Alerts are triaged within the timeframes defined by the organisation and escalated where cyber security incident thresholds are met.
NE-3: No incident severity thresholds are defined.		FE-3: Triage performance is tracked and reported.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0125, ISM-0120
E8	ISM-1906, ISM-1907, ISM-0109, ISM-1228
CSF	DE.AE-02, DE.AE-04, DE.AE-08, RS.MA-01
800-171r3	03.06.01, 03.06.02, 03.14.06
AESCSF	RESPONSE-1b, RESPONSE-2a, RESPONSE-2d

IT.DET-03.2

Action: Use indicators from across identities, applications, data and infrastructure activity rather than isolated signals when identifying cyber security incidents.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Investigation relies on single-source alerts with no cross-source correlation.	PE-1: Some correlation exists but is limited to specific data source pairs.	FE-1: Correlation rules and investigation procedures consider signals across identities, applications, data and infrastructure.
NE-2: Correlation rules do not consider signals from multiple data sources.	PE-2: Cross-source investigation is performed manually but not supported by automated correlation.	FE-2: Automated correlation supports detection of multi-stage adversary activity.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-2116, ISM-0120, ISM-2117
E8	ISM-1228
CSF	DE.AE-03, DE.AE-04, DE.AE-07, DE.AE-08
800-171r3	03.03.05, 03.14.06, 03.06.01
AESCSF	RESPONSE-1d, SITUATION-3f, RESPONSE-2i

DET-05 - Detection capability efficacy

Principle: Cyber security event detection capabilities are regularly evaluated for effectiveness and continuously refined, including by using current strategic and sector-specific cyber threat intelligence, to improve the detection of cyber security events.

IT.DET-05.1

Action: Review detection coverage periodically to identify gaps arising from new assets, services or architectural changes.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No review of detection coverage has been conducted within the period defined by the organisation.	PE-1: A review of detection coverage has been conducted but does not cover all recently deployed assets or services.	FE-1: A detection coverage review has been completed within the cycle defined by the organisation.
NE-2: No process exists to assess new assets and services for log coverage or detection applicability.	PE-2: Detection gaps have been identified and remediation is planned, but remediation has not been executed within timeframes defined by the organisation.	FE-2: New assets and services are assessed for log coverage and detection rule applicability.
		FE-3: Identified detection gaps are remediated within risk-based timeframes defined by the organisation.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1526, ISM-1617, ISM-0120
E8	ISM-1807
CSF	DE.CM-09, ID.IM-02, ID.IM-03, GV.OV-03
800-171r3	03.12.03, 03.03.01, 03.14.06
AECSF	RESPONSE-1e, SITUATION-2i, SITUATION-2c

Respond principles

RES-05 - Cyber security incident coordination

Principle: Cyber security incident roles and responsibilities are defined, documented and exercised to support the internal and external coordination and management of cyber security incidents, including responsibilities for declaring cyber security incidents and undertaking pre-approved response and recovery activities.

IT.RES-05.1

Action: Integrate external coordination obligations into cyber security incident response activities where required.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: External coordination requirements for Cyber security incident response activities are neither identified nor documented.	PE-1: External coordination requirements are documented but are not integrated into operational response procedures.	FE-1: Cyber security incident response procedures include documented external coordination requirements with defined triggers, contacts and timeframes.
NE-2: No defined triggers, contacts or timeframes exist for external reporting.	PE-2: Contacts and triggers are defined for some but not all required external parties.	FE-2: Requirements cover all relevant external parties identified by applicable legal, regulatory, contractual and organisational obligations. FE-3: Coordination procedures have been exercised or invoked and lessons learned have been incorporated.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0043, ISM-1784, ISM-0576
E8	ISM-0140
CSF	RS.CO-02, RS.CO-03, GV.OC-03, RS.MA-01
800-171r3	03.06.02, 03.06.05, 03.12.05
AESCSF	RESPONSE-3c, RESPONSE-3f, RESPONSE-3j

RES-03 - Cyber security incident response

Principle: Cyber security incidents are contained, eradicated and recovered from in a timely manner.

IT.RES-03.1

Action: Use documented, tested and approved cyber security incident response procedures when responding to cyber security incidents.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: No documented cyber security incident response plan or procedures exist. NE-2: Incident response activities are conducted on an ad hoc basis without any defined roles, escalation paths, procedures or response objectives. NE-3: Available incident records demonstrate systemic failures to contain, eradicate or recover from cyber security incidents within organisationally defined timeframes, and the causes of these failures are not addressed.	PE-1: A cyber security incident response plan exists but has not been exercised or invoked within the organisationally defined test cycle. PE-2: The cyber security incident response plan defines roles, escalation paths, and response procedures, but target timeframes or intended response outcomes are not clearly defined. PE-3: Incident records or exercise results demonstrate that response activities do not consistently meet organisationally defined timeframes or intended outcomes, but identified deficiencies are documented and subject to improvement actions.	FE-1: An approved cyber security incident response plan is in place and defines roles, escalation paths, response procedures, target timeframes and intended containment, eradication and recovery outcomes. FE-2: The incident response plan and associated procedures have been exercised or invoked within the organisationally defined test cycle. FE-3: Incident records demonstrate that cyber security incidents are contained, eradicated and recovered from within organisationally defined target timeframes and achieve the intended response outcomes, taking into account incident severity, complexity and business impact. FE-4: Where target timeframes or intended outcomes are not achieved, the causes are analysed, improvement actions are assigned and tracked, and relevant plans, procedures and controls are updated. FE-5: Where no relevant cyber security incident has occurred during the assessment period, appropriately scoped exercises demonstrate the organisation's capability to achieve its target timeframes and intended response outcomes.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-0576, ISM-0043, ISM-1784
E8	ISM-1819
CSF	RS.MA-01, RS.MA-02, ID.IM-01, GV.OV-01
800-171r3	03.06.01, 03.06.05, 03.06.03
AESCSF	RESPONSE-3d, RESPONSE-3e, RESPONSE-3g

RES-04 - Cyber security incident insights

Principle: Lessons learnt from cyber security incidents are captured, and areas for improvement are identified, prioritised and actioned in a timely manner.

IT.RES-04.1

Action: Perform post-cyber security incident reviews to identify the security gaps that enabled each stage of the cyber security incident.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Post-incident reviews are not conducted.	PE-1: Post-incident reviews are conducted for some incidents but not all that meet the severity threshold defined by the organisation. PE-2: Reviews are conducted but findings are not documented or actioned.	FE-1: Post-incident reviews are conducted for all incidents meeting the severity threshold defined by the organisation. FE-2: Findings identify the specific gaps that enabled each stage of the incident. FE-3: Remediation actions arising from findings are implemented and tracked to closure.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1803, ISM-0125, ISM-1526
E8	N/A
CSF	RS.AN-03, RS.AN-08, ID.IM-01, ID.IM-02
800-171r3	03.06.02, 03.06.01, 03.11.01
AESCSF	RESPONSE-3h, RESPONSE-3i, RISK-2a

IT.RES-04.2

Action: Evaluate the monitoring coverage and cyber security incident response procedures following cyber security incidents.

Domains: Visibility and response; **Mitigated Techniques:** N/A;

Indicators of Good Practice

Not effective	Partially effective	Fully effective
NE-1: Detection rules, monitoring coverage and response procedures are not reviewed following incidents.	PE-1: Reviews are conducted but do not result in documented changes to detection or response capabilities. PE-2: Some improvements are made but not systematically tracked or validated.	FE-1: Detection rules, monitoring coverage and cyber security incident response procedures are reviewed following incidents, with identified lessons incorporated into updates. FE-2: Changes are documented, tested and validated for effectiveness.

Potential evidence sources

Framework	References
ISM (excl. E8)	ISM-1784, ISM-1617, ISM-1526
E8	N/A
CSF	RS.AN-03, ID.IM-01, ID.IM-03, GV.OV-01
800-171r3	03.06.03, 03.06.05, 03.12.03
AESCSF	RESPONSE-3h, RESPONSE-3g, SITUATION-2i

Annex A - Domains

Domain	Description	Priority phases
Governance and culture	Policies, risk management processes, roles and security culture that underpin the cyber security program	Phase 1, Phase 2, Phase 3
Visibility and response	Procedures and capabilities for detecting, analysing and responding to cyber security events and incidents.	Phase 1, Phase 2, Phase 3
Boundary services	Assets at network boundaries that broker connectivity between environments of different trust levels, including internet-facing services and edge devices.	Phase 1
Identity services	Enterprise-wide identity, credential and access management services such as directories, authentication and authorisation services or credential stores.	Phase 1
Critical processes and services	Core processes and services that are critical to delivering primary organisational outcomes.	Phase 2
Privileged environments	Systems and services that support privileged activities, management services and high-impact administrative functions.	Phase 2
Business systems	Supporting enterprise functions that collectively enable organisational operations.	Phase 3
User devices	Endpoints issued to the workforce, including desktops and laptops.	Phase 3

**For more information, or to report a
cyber security incident, contact us:**

cyber.gov.au

1300 CYBER1 (1300 292 371)

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the entity's logo, third party content, and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license

<https://creativecommons.org/licenses/by/4.0/>

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license

<https://creativecommons.org/licenses/by/4.0/legalcode.en>

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website

<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>

