DCC

Defence Cyber Certification

Level 1 Applicant Guide

Introduction

The Defence Standard (Def Stan) 05-138 was introduced in 2015 as part of the UK government's national cyber security programme, responding to escalating cyber threats. Over the past decade, the defence standard has evolved, and its latest iteration, issue 4, marks a pivotal shift. This version expands the Defence Standard's scope beyond solely protecting MOD-identifiable information to enhancing the overall resilience of an organisation against threats.

The Ministry of Defence (MOD) recognises the importance of ensuring suppliers adhere to the Defence Standard. This document serves as a guide to help applicants prepare for an assessment against the Def Stan 05-138 i4.

By providing a structured and consistent approach to these assessments, MOD seeks to uphold the highest level of cyber security across its supply chain. The Defence Standard sets out the criteria for suppliers in its 148 controls, which are applied into four progressively stringent levels. MOD suppliers are expected to attain a level of security specified in their contracts with the MOD, which is referred to as the Cyber Risk Profile.

The overall aim of this certification scheme is to enhance the cyber resilience of the organisations applying for certification. Whilst some organisations may already meet the controls others may be deficient in some areas, as part of the application these areas will become apparent and (if possible) remediated prior to assessment.

Defence Cyber Certification/Cyber Risk Profile Levels

A Cyber Risk Profile level will be assigned to any new procurement/contract or requirement by the MOD awarding body; this level then defines which controls the supply chain is required to adhere to.

The Defence Cyber Certification scheme is used to assess whether the controls have been met. It is important to note that the Cyber Risk Profile and Defence Cyber Certification levels are the same.

Applicant organisations may, under the new DCC scheme, apply for assessment and then certification at any level. This allows them to demonstrate compliance with the chosen level by means of a certificate and will remove the need for future assessments on a contract-by-contract basis for levels less than or equal to their certification.

There are 148 controls in total, but no single level contains all the controls. This is due to some controls overlapping or being replaced by more comprehensive controls at a higher level.

The Defence Cyber Certification Levels are:

Level 0 (3 controls)

Level 0 is normally assigned where there is a very low level of assessed cyber risk to a supplier delivering an output. It requires supplier organisations to demonstrate basic cyber security practices and forms the foundation level for all future assessments higher than level 0.

Level 1 (101 controls)

Level 1 is normally assigned where there is a low to moderate level of assessed cyber risk to a supplier delivering an output. It requires supplier organisations to demonstrate a comprehensive cyber security programme with good practices.

Level 2 (139 controls)

Level 2 is normally assigned where there is a high level of assessed cyber risk to a supplier delivering a contracted output. It requires supplier organisations to demonstrate advanced cyber security oversight and planning which drives robust organisational and cyber practices.

Level 3 (144 controls)

Level 3 is normally assigned where there is a substantial level of assessed cyber risk from a supplier delivering a contracted output. It requires supplier organisations to demonstrate expert cyber security capabilities that fully take advantage of the 'defence in depth' methodology to appropriately protect the organisation against new and evolving threats.

The Level 3 assessment will be conducted as part of a pilot scheme, incorporating a hybrid approach that combines both Level 2 and Level 3 controls. Applicants will be required to provide responses and evidence for all Level 2 controls as well as all Level 3 controls, totalling 145 controls.

- This pilot scheme is currently the only pathway to achieve Level 3 certification. It offers flexibility for organisations pursuing Level 3 by allowing them to:
- Achieve Level 3 certification if the Level 3 pass mark is met.
- Achieve Level 2 certification if the Level 2 pass mark is met but Level 3 pass mark is not achieved.

Defence Cyber Certification Process

For the DCC process please see the **DCC Process Guide**.

The process varies according to the level, please ensure you follow the correct process for your level.

Third Party Assistance

Except for work allowed to attain Cyber Essentials (CE) and Cyber Essentials Plus (CE+), the only assistance the assessing Certification Body can provide is in an advisory role; they cannot make any changes or perform any actions.

The assessing Certification Body may:

- Help the applicant prepare for, and attain CE/CE+
- Explain the DCC scheme and its levels
- Explain the DCC controls and how to meet them
- Clarify the question and identify the key components needed to provide a complete and accurate response
- Describe the necessary evidence needed to demonstrate that a control has been met
- Verify scope
- Supply blank template documents

The Certification Body may not:

- Implement any policy
- Implement any changes
- Answer any questions on behalf of the Applicant or dictate the answers
- Complete any documentation or prepare any answers or evidence that they will later assess

If you need additional support beyond the advisory role of the Certification Body, you have the option to engage a separate technology provider.

Determine Scope

For DCC scoping please see the **DCC Scoping Guide**.

Defence Cyber Certification Questions

DCC Core Questions/Controls Labelling

Below is an example of a question ID and control number you will encounter in completing this submission.

The levels indicated in brackets following the MOD question ID represent the corresponding DCC scheme levels to which this question or control applies.

IASME has retained these values from Def Stan and the MOD supply chain as follows;

EXAMPLE

0001.1 - (MOD 000011) - (L0-L3)

0001.1	MOD 000011	L0-L3
The question ID	The MOD supply chain portal Unique Question ID	The level covered

The questions have been taken from the MOD SAQ where possible, however there may be slight changes to the wording or new questions created if not available from the MOD at the time of writing. Where no question is available from the MOD it will have the identifier MOD 000XXX.

---LIVE QUESTIONS NOW FOLLOW---

0001 - Cyber Essentials

Terms

Cyber Essentials is a UK Government-backed certification scheme. It is aligned to five technical controls designed to prevent the most common internet-based cyber security threats.

Control Requirement

The Applicant shall have Cyber Essentials certification that covers the scope required for all aspects of the assessment and commit to maintaining this for the duration of the Defence Cyber Certification.

Jargon Buster

The Applicant must have Cyber Essentials certification that applies to all areas of the DCC certification scope that is applicable to Cyber Essentials within Cyber Essentials guidelines. The Applicant must keep this Cyber Essentials certification for as long as the Defence Cyber Certification lasts.

The Cyber Essentials scope of the Applicant organisation must align with the proposed scope of this Defence Cyber Certification assessment. It must be noted (as discussed during scoping) that Cyber Essentials scope is only internet-connected devices whereas DCC scope includes internet-connected and non-internet-connected devices. For clarification on Cyber Essentials please see the Cyber Essentials Knowledge Hub and for DCC scope, please see the separate DCC Scoping Guidance.

Your Assessor will verify that the Cyber Essentials and DCC scopes align as much as possible, but this will rarely be an exact match. A small organisation may be able to exactly align, but as DCC includes non-internet connected devices, there will usually be some differences between scopes. As such, it is important to add context to your answer so the Assessor can understand your Cyber Essentials scope and why it may vary from the DCC scope.

You should discuss your scope(s) with your chosen Certification Body as one of your first steps when answering the questions. If the Cyber Essentials scope does not adequately align, then it is an automatic failure.

Supplying a diagram showing which parts of the organisation/network fall within CE and how they relate to the DCC scope is recommended for all organisations.

0001.1 - (MOD 000011) - (L0-L3)

Does the organisation hold Cyber Essentials certification(s) that cover(s) the required scope for this activity?

Cyber Essentials has it's own guidelines for the devices that cannot be within scope, within those guidelines the Cyber Essentials scope must cover all of the applicable internet-connected devices/networks within the DCC scope.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, my Cyber Essentials certificate covers all of my internet-connected networks/devices but does not include my non-internet-connected operational technology (ICS/SCADA).
Expected Evidence: Your certificate number, Cyber Essentials self-assessment questionnaire/report, diagram showing CE scope in relation to DCC scope

0001.2 - (MOD 000625) - (L0-L3)

Does the organisation commit to maintaining Cyber Essentials certification for the duration of any function related to this activity or DCC certification?

You must consider the Cyber Essentials certification covering contracts for their duration.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: An attestation or history demonstrating regular renewal.

Objective A - Managing security risk

Managing security risk. The Applicant has appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to its network, and information systems, including all network and information systems that protect all data.

1100 - Governance

Term

Governance refers to the framework of policies, procedures, and guidelines that an organisation establishes to ensure its systems and data are protected, used properly, and align with its overall goals and legal requirements.

Control Requirement

The Applicant shall have appropriate management policies and processes in place to govern their approach to the security of the network and information systems supporting functions and protection of data.

Jargon Buster

This control is about you demonstrating you have clear policies and processes to methodically identify, evaluate, and control any threats to the security of your networks. These formal guidelines give you consistency in your handing of security risk.

1100.1 - (MOD 000366) - (L1-L3)

Does the organisation have documented management policies and processes in place that govern network and information system security?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered in our IT Management and Security policies.
Expected Evidence: The documented policies or processes.

1100.2 - (MOD 000013) - (L1-L3)

Are the organisation's management policies and processes:

Multiple selection

- ☐ Approved by management
- ☐ Communicated to all staff, including contractors
- ☐ Assigned an owner for ongoing maintenance and review
- ☐ Reviewed at least annually
- ☐ None of the above

Example: All employees and contractors are required to read essential policy and process documents as part of annual training. This is approved by management but is not assigned to an owner. (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Your Certification Body Assessor will want to see the policies/processes documented and we would expect to see many of these details in a revision history or record of changes. An example email or message screenshot showing this communicated to staff would also be accepted.

1102 - Roles and Responsibilities

Control Requirement

The Applicant shall have established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Jargon Buster

This control looks at whether you have assigned staff to protect you at every level, and if there is a clear path for staff to report and escalate security issues.

1102.1 - (MOD 000017) - (L1-L3)

Does the organisation have clearly defined roles and responsibilities for networks and information system security at all levels, with clear communication and risk escalation channels?

Jargon Buster

This question wants to know if your company has clearly defined who is responsible for keeping your networks and systems safe. Are there straightforward ways for your team to talk and raise concerns about security risks?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, responsibility is assigned to..., and the roles are detailed in the job description. Escalation channels are covered during training.
Expected Evidence: You might have an organisational chart outlining the hierarchy of your security, incident reports illustrating risk escalation in action or job descriptions showing responsibilities.

1200 - Risk Management

Control Requirement

The Applicant shall take appropriate steps to identify, assess, understand, and remediate security risks to the network and information systems that protect all data. This includes an overall organisational approach to risk management.

Jargon Buster

Businesses will often have a risk register or business plan as part of their risk management.

1200.1 - (MOD 000369) - (L1-L3)

How often does the organisation actively manage cyber security risks across the entire organisation?

Please select one option:

- ☐ At least quarterly
- ☐ Ad-hoc
- ☐ No risk management in place

Example: We review risks quarterly
Expected Evidence: Your Certification Body Assessor will need to see the two most recent versions of your company's risk registers, complete with dates to demonstrate how often they are updated.

1200.2 - (MOD 000020) - (L1-L3)

Does your organisation assign dedicated risk owners to identified risks?

All risks should have an assigned owner who is responsible for managing the risk (including tracking and remediation activities) within the defined timelines.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this can be seen in...

Expected Evidence: A document that shows identified risks and the owners of those risks.

1202 - Periodically Assess Risk

Control Requirement

The Applicant shall periodically assess the risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, resulting from the operation of organisational systems and the associated processing, storage, or transmission of data.

Jargon Buster

At its core, this control is checking that you regularly evaluate for potential dangers that could disrupt your day-to-day business, harm your company's reputation, or affect your staff and assets.

1202.1 - (MOD 000370) - (L1-L3)

How often does the organisation conduct a comprehensive risk assessment of your systems to protect operations, assets, individuals, storage and transmission of data?

Available answers (choose one):

- ☐ At least annually
- ☐ Ad-hoc
- ☐ No risk assessment in place

Example: We conduct this annually.
Expected Evidence: Minimum of the latest two risk assessments to demonstrate a history or commitment to identifying risk.

1203 - Network Diagrams

Terms

Network diagrams are a visual representation of a computer network's architecture used to help you plan, keep track of, and fix network issues. These diagrams should show the different components, such as routers, switches, nodes, firewalls, and how they are connected. They make it easier to see how the network is laid out and help in understanding how each part talks to the others.

<u>Control Requirement</u>

The Applicant shall create and maintain up to date network diagrams detailing the network boundaries, internal and external connection, and systems within the operational environment.

1203.1 - (MOD 000025) - (L1-L3)

Does the organisation maintain up-to-date network diagrams showing network boundaries, internal and external connections, and operational systems?

Network diagrams should include the following details:

- All pertinent systems, connections, and network devices
- Definition of system boundaries and operating environments
- Documented implementation details, highlighting connections to other systems
- Regular updates to ensure accuracy and alignment with any changes in systems, boundaries, or security requirements.

Available answers (choose one):

☐ Yes
☐ No

Example: Yes, we update the diagrams every time an operational system is added or removed.
Expected Evidence: Latest network diagram(s)

1300 - Asset management

Control Requirement

The Applicant shall reasonably ensure everything required to deliver, maintain, or support networks and information systems that support delivery of all functions which protect all data are determined and understood. This includes people and systems, as well as any supporting infrastructure (such as power or cooling).

Jargon Buster

Asset management involves understanding and managing all resources, or assets, that are critical to your organisation's operation. Assets include the people you work with, such as staff, contractors, students, volunteers, and others, as well as physical supporting infrastructure like power and cooling systems. It also includes the hardware, software, and technology related resources that you own, lease or use in your operations.

1300.1 - (MOD 000031) - (L1-L3)

Does the organisation have a documented asset management policy?

A strong asset management policy should clearly describe how to:

- Identify and categorise the company's valuable items,
- Assign responsibility for them,
- Track and safely dispose of them, and
- Protect them.

It should also follow recognised best practices and standards for asset management.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have an asset management policy, it covers.... .
Expected Evidence: Policy detailing the asset lifecycle from start to finish.

1300.2 - (MOD 000033) - (L1-L3)

Does the organisation have an asset classification process in place? (An asset classification process shall include defining asset types and value.)

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, asset classification is detailed in our policy.
Expected Evidence: Policy or other supporting evidence showing asset classification process is in place.

1300.3 - (MOD 000373) - (L1-L3)

Are all resources necessary for network and information system operation documented in an asset inventory? (This includes people, systems and supporting infrastructure.)

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a comprehensive inventory which documents... and helps us track...
Expected Evidence: Asset register or other evidence showing the necessary resources.

1400 - Supply chain

Control Requirement

The Applicant shall understand and manage security risks to functions and data that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third-party services are used.

Jargon Buster

This control is about you taking steps to manage the risks that come with depending on other companies for services or products, ensuring they also have strong security measures to protect your business's operations and data.

1400.1 - (MOD 000630) - (L1-L3)

Does the organisation have policies and procedures in place to manage the cyber security requirements of its supply chain?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set cyber security requirements for our supply chain in..., it covers ..., and defines... It was last updated [date]
Expected Evidence: a copy of the policies and procedures.

1400.2 - (MOD 000375) - (L1-L3)

Does the organisation assess security risks associated with dependencies on suppliers?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered during our... risk assessment
Expected Evidence: A sample risk associated with a supplier

1400.3 - (MOD 000376) - (L1-L3)

When does the organisation assess security risks related to its suppliers?

Choose all applicable answers:

- ☐ Before supplier selection
- ☐ At least annually, for all existing suppliers

Example: We assess the risk when first onboarding and then annually.
Expected Evidence: Sample risk assessments of new and existing suppliers.

1400.4 - (MOD 000377) - (L1-L3)

Which of the following does the organisation do to ensure suppliers maintain appropriate security measures?

Available answers (choose all applicable):

- ☐ Determine appropriate security requirements for the supply chain.
- ☐ Review supplier contracts to ensure security requirements are met.
- ☐ Monitor third-party security arrangements.
- ☐ None of the above.

Example: As part of our supplier review process, we... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: You would be expected to...

1400.5 - (MOD 000378) - (L1-L3)

What actions does the organisation take if a supplier fails to meet security requirements?

Available answers (choose one):

- ☐ Manage the risk through the organisation's risk management process.
- ☐ Implement corrective actions or terminate the contract, where appropriate.
- ☐ No defined process for addressing non-compliance.

Example: We assess the failing and require the supplier to remediate within a suitable time frame. (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Sample of when a supplier has been found to be failing to meet requirements or a policy/process defining what actions would be taken.

1401 - External provider trusted relationships

Control Requirement

The Applicant shall establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships.

Jargon Buster

You need to create, record, and keep up trusted partnerships with outside service providers. These should be based on clear security and privacy expectations that define what makes a trustworthy relationship.

1401.1 - (MOD 000036) - (L1-L3)

Are Service Level Agreements with IT infrastructure suppliers clearly documented?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Service Level Agreements are in all of our contracts.
Expected Evidence: Sample of a contract showing the agreed timescale.

1401.2 - (MOD 000040) - (L1-L3)

Do the organisation’s agreements with suppliers include information security, confidentiality, and data protection requirements?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We flow down the security requirements to our suppliers.
Expected Evidence: Evidence of requirements shared with suppliers, e.g. SLA or contracts.

1401.3 - (MOD 000379) - (L1-L3)

Do you impose restrictions on all subcontractors handling customer data to prevent unauthorised data sharing?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, these are stipulated in our contractual requirements

Expected Evidence: Sample agreements showing restrictions on handling data.

1500 - Physical access controls

Control Requirement

The Applicant shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where data is stored or processed to its authorised personnel by implementing industry-standard physical access controls. Examples of such controls include but are not limited to:

- Swipe card technology
- Monitored CCTV
- Remotely monitored alarm systems
- On-premises security guards
- Photographic access credentials
- Visitor escort
- Physical access logs
- Authorised access lists.

The Applicant shall review physical access logs regularly or in the event of a physical or cyber security incident.

Jargon Buster

This control is about how you control access to real life locations.

1500.0 - (MOD 000XXX) - (L1-L3)

Does the organisation have physical premises?

If you believe you have no physical premises it is essential to discuss this with the Assessor prior to submission. Organisations without physical premises do not need to answer 1500.1–1503.2 as they relate to physical premises, but this must be adequately explained and demonstrated to the assessor's satisfaction.

Available answers (choose one):

- ☐ Yes
- ☐ No

1500.1 - (MOD 000044) - (L1-L3)

Does the organisation have a documented physical security policy in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements for physical security in..., it covers ..., and defines... It was last updated [date]
Expected Evidence: A copy of the policy.

1500.2 - (MOD 000380) - (L1-L3)

Does the organisation ensure physical access to facilities where sensitive data is stored or processed is restricted to authorised personnel?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, access is restricted to limited roles.
Expected Evidence: Evidence of how access is restricted, such as policy, description, or image of restriction method (e.g. door lock).

1500.3 - (MOD 000381) - (L1-L3)

Does the organisation ensure records are retained of all physical access to facilities where sensitive data is stored or processed?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, swiping into the facility is logged on...
Expected Evidence: An entry log or record showing someone's access to a facility.

1501 - Physical access device management

Term

A physical access device is a tool used to operate locks (to lock or unlock them), such as a key, keycard, keypad or biometric scanner.

Control Requirement

The Applicant shall manage and maintain an inventory of all physical access devices used on their premises. The inventory should contain a unique identifier for the device regardless of the type (e.g. access fob, Radio Frequency Identification (RFID) card or door key) as well as the named individual who it is assigned to.

Jargon Buster

This control is about how you keep track of your physical access devices.

1501.1 - (MOD 000382) - (L1-L3)

Does the organisation assess physical security controls of supply chain facilities where sensitive data is stored or processed by them?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We review third-party security controls when onboarding to ensure they meet our standards.
Expected Evidence: Sample onboarding requirement or flow down to supplier, or other supporting evidence.

1501.2 - (MOD 000047) - (L1-L3)

Does the organisation maintain an inventory of all physical access devices used at its premises? (e.g. RFID cards, access fobs, door keys, keypads, biometric scanners)?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we maintain a register of RFID tokens and who they are assigned to.

Expected Evidence: Document showing evidence of inventory such as a register or list.

1502 - Physical access restrictions

Terms

A sensitive area is part of your site where confidential work is conducted or where sensitive information is stored and or processed. Only authorised individuals with official permission may access these areas.

Control Requirement

The Applicant shall restrict physical access to sensitive areas within an organisation's premises to only those who are authorised to have access. The supplier shall maintain and manage an inventory of those staff who have privileged physical access. If no office buildings are used, then please note it below.

Jargon Buster

This is about making sure that only certain people, who have permission, can get into private or sensitive areas at your organisation's sites.

1502.1 - (MOD 000048) - (L1-L3)

Does the organisation restrict physical access to sensitive areas to authorised personnel only?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Only our IT team have access to the server room.
Expected Evidence: Evidence of how access is restricted, e.g. access policy or register of keys/token for access and who they are assigned to.

1502.2 - (MOD 000049) - (L1-L3)

Does the organisation maintain an up-to-date inventory of personnel authorised to access sensitive areas?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, access is role based.
Expected Evidence: Policy or process that covers the recording and updating process of the inventory, sample or screenshot of inventory

1503 - Visitor access management

Control Requirement

The Applicant shall ensure the following controls are applied to all visitors visiting the organisation's premises:

- Visitor entry and exit times are recorded.
- Visitors always wear ID badges that are clearly different from those of employees.
- Visitors are always accompanied while on the premises.
- Visitors return their badges at the end of their visit.

If no office buildings are used, then please note it.

Jargon Buster

This control is about the rules you have for visitors to your organisation's sites.

1503.1 - (MOD 000050) - (L1-L3)

Does the organisation manage visitor access to non-public areas of its premises, including logging their entry and exit?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, access to the main site is logged in our visitor book, access to the research lab is further logged in the...
Expected Evidence: A copy of the record or records if there is more than one level of access.

1503.2 - (MOD 000051) - (L1-L3)

Does the organisation require visitors to always wear approved identification badges while on its premises?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered in our Visitor policy and vistors are told this by reception

Expected Evidence: Visitor or admission policy

Objective B - Protecting against cyber attack

The Applicant has proportionate security measures in place to protect the networks and information systems supporting all functions from cyber-attack.

2100 - Resilience policy and process development

Terms

Resilience is the ability to withstand or quickly recover from cyber-attacks or technical failures. To mitigate is to make something less severe or serious.

This control focuses on the strategic or procedural approach to resilience. A later control (2500, Resilient networks and systems) overlaps with 2100, however, both controls are assessed separately.

Control Requirements

The Applicant shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on functions and protection of data.

Jargon Buster

This control is about the policies and processes, focused on cyber security and resilience, that you've created. These policies are meant to reduce the risk of harm to your organisation's operations and to keep your data safe.

2100.1 - (MOD 000384) - (L1-L3)

Does the organisation have documented policies and procedures in place that cover both cyber security and cyber resilience?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, these are covered in...

Expected Evidence: The policies and procedures you believe cover cyber security and cyber resilience.

2100.2 - (MOD 000386) - (L1-L3)

Does the organisation review its cyber security and cyber resilience policies and processes at least annually?

Available answers (choose one):

- ☐ Within 12 months
- ☐ Longer than 12 months

Example: Annually, our last review was...
Expected Evidence: The same policies from 2100.1 should answer this question, you ought to be able to direct your Certification Body Assessor to a change log, history revision or something similar on those documents.

2200 - Identity and access control

Terms

Removable storage media & devices are portable devices like USB drives, external hard drives, and CDs that can store and transfer data.

Verified means to confirm that something is true or accurate.

Authenticated/ authentication is the process of determining whether someone or something is who or what they say they are.

Authorised/ Authorisation is the permission to access certain data or systems.

Control Requirement

The Applicant shall understand, document and manage (i.e. create, review and disable) access to networks, information systems, and removable storage media & devices supporting functions and protection of data. All accounts and identities, including users, system and automated functions that can access data or systems are appropriately verified, authenticated and authorised.

Jargon Buster

This control is about you making sure you know who has access to what and using technology to manage that access.

2200.1 - (MOD 000392) - (L1-L3)

Does the organisation have documented policies and procedures in place that cover identity management?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, ... and ... cover this.
Expected Evidence: The documentation (policies or procedures) outlining your approach to identity management.

2200.2 - (MOD 000393) - (L1-L3)

Does the organisation have documented policies and procedures in place that cover access control?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, ... and ... cover this.
Expected Evidence: The documentation (policies or procedures) outlining your approach to access control.

2200.3 - (MOD 000394) - (L1-L3)

Before granting access to non-public resources, does the organisation ensure that the following are in place:

Available answers (choose all that apply):

- ☐ Users are authenticated
- ☐ Users are authorised
- ☐ User identities are verified
- ☐ None of the above

Example: Before granting access to non-public resources, we... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Think about the steps you take and how you can demonstrate those steps in action.

The principle of least privilege/functionality

Jargon Buster

The principle of least privilege and the principle of least functionality are related, but they focus on different aspects:

- Principle of Least Privilege: This is about user access. It ensures that users (or processes acting on their behalf) have only the minimum levels of access or permissions needed to perform their tasks. For example, an employee in the finance department may have access to the financial records but not to the human resources records because their job does not require it.
- Principle of Least Functionality: This is about system functionality. It focuses on limiting the software, services, and features that are active on a system to only those that are necessary for the required operation. For example, if a server is dedicated to storing files, the principle of least functionality would dictate that you disable all other services and applications on that server that aren't needed for file storage.

By applying these principles, if a user's account was compromised, the hacker would also be limited by these same restrictions. They would only have access to the specific areas and functions the user had, reducing the potential damage they could do.

2204 - Principle of least functionality

Control Requirement

The Applicant shall ensure that all information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, programmes and services that are not integral to the operation of that information system.

Jargon Buster

The principle of least functionality states that information systems must be configured to provide only essential capabilities. This control focuses on functionality.

2204.1 - (MOD 000395) - (L1-L3)

Does the organisation remove or restrict the use of non-essential functions within information systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a process to identify essential features/services and understand the user needs. From there, we adjust configurations to remove non-essential functions and conduct regular reviews to ensure security is balanced with functionality.

Expected Evidence: Your Assessor will want to see evidence of disabled functionality; this might be in your system configurations, system hardening or application settings. It could appear in group policy objects or in some form of configuration management tool.

2205 - Least privilege

Term

The principle of least privilege, also known as the principle of minimal privilege or the principle of least authority, is a key security practice that means people or programs should only have the minimum level of access required to do their work. This approach helps to protect the system by ensuring no one has more permissions than they need to complete their tasks. Privilege covers both permissions to data and rights to perform system tasks.

Control Requirement

The Applicant shall closely manage all user accounts and employ the principle of least privilege to networks and information systems supporting all functions and protecting all data.

2205.1 - (MOD 000068) - (L1-L3)

Does the organisation provide user access to resources based on business need and the principle of least privilege?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we implicitly deny and control user privileges using a capability list.
Expected Evidence: Your Assessor will want to see how you are controlling access. This could include you demonstrating the mechanisms you have in place or the approach you are using.

2206 - Separation of Duties

Term

Separation of duties is a concept that ensures no single person has enough access to misuse a system by themselves.

For example, from a wider industry perspective, an insurance company employee is able to create a fake insurance policy, that employee can raise a fake claim against the fake policy. Lastly that employee is able to pay out against the fake claim. Because there was no separation of duties one person was able to do all three steps, ideally the final step should have been for another person or department to make the payout having first checked the validity of the claim.

This principle applies to any multistage process where authority is required for each stage.

Control Requirement

The Applicant shall develop a policy and implement a separation of duties methodology for standard and privileged accounts which support functions and protect data.

2206.1 - (MOD 000396) - (L1-L3)

Does the organisation's access control policy include a separation of duties methodology?

(For small and micro-organisations, the methodology may require separation of duties only as the organisation expands.)

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: The section of your access control policy that addresses separation of duties. This is expanded in the following question.

2206.2 - (MOD 000397) - (L1-L3)

Has the organisation implemented a separation of duties methodology which considers:

Available answers (choose all that apply):

- ☐ The criteria for when separation is needed
- ☐ How user accounts (standard and privileged) will be provisioned to facilitate separation
- ☐ Cover for duties during staff absence
- ☐ None of the above

Example: Yes, we cover... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: The section of your access control policy that addresses separation of duties, demonstrating how the above has been considered.

2207 - Least Privilege - Audit System

Control Requirement

The Applicant shall limit access to systems' audit/security logging data and functionality to privileged user groups that have a confirmed requirement in accordance with the principle of least privilege.

This control is about making sure that only certain employees can see and work with systems that generate, store, or manage audit/security logging data.

When thinking about their privileges, consider the control of actions such as reading, writing, creating, modifying, or deleting logs, and what system tasks these users can perform.

2207.1 - (MOD 000070) - (L1-L3)

Does the organisation limit access to your systems' audit/security logging data to privileged user groups with a confirmed requirement for access to logging data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we limit access to...
Expected Evidence: Your Assessor will expect to see something outlining your policies on restrictions, and some form of implementation such as an access control list or role-based access control dashboard.

2210 - Limit to authorised transactions

Control Requirement

The Applicant shall issue, manage, verify, revoke, and audit identities and credentials to authorised transactions, users, and processes.

Term

A transaction is an event which can be observed and can have a positive, negative or neutral effect on the object. The object is accessed by a subject. An example of this could be a system account accessing a logfile to add an entry. The subject is the system account and it's privileges, the object is the logfile and the transactions associated with are; open object (logfile) by the subject (system account) and read from the object and then write to the object with a new log entry. The subject (system account) then needs to save and close the object (logfile).

2210.1 - (MOD 000401) - (L1-L3)

Does the organisation have a documented process for issuing, managing, verifying, revoking, and auditing identities and credentials for authorised users, processes and transactions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements for this in..., it covers ..., and defines... It was last updated [date]

Expected Evidence: A copy of the documented process.

2210.2 - (MOD 000402) - (L1-L3)

Has the organisation implemented measures to ensure that only authorised individuals and processes can access systems using issued identities and credentials?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: In other words, if a system account is not able to access an object and perform a transaction, we would expect to see an error in the audit logfile. We would also expect to see confirmation or success in conducting the transaction if it were suitably permissioned.
Expected Evidence: Audit entries in the log. Failures, successes, mapping subjects to objects etc.

2211 - Secure first-time password management

Control Requirement

The Applicant shall employ secure practices for the secure storage, transmission, and management of first-time and one-time passwords. These practices include, but are not limited to:

- Secure storage of first-time passwords prior to use
- Secure transmission of first-time and one-time passwords to their new user
- Require that first-time and one-time passwords are immediately changed after first logon.

Jargon Buster

The Secure First-time Password Management control focuses on the initial setup and delivery of passwords.

2211.1 - (MOD 000079) - (L1-L3)

Does the organisation secure the storage, transmission and management of first-time and one-time passwords?

Available answers (choose one):

☐ Yes
☐ No

Example: Yes, we store passwords in..., transmit them using..., and have the following restrictions on the management of first-time and one-time passwords...
Expected Evidence: For each section of this question (storage, transmission and management), your Assessor may expect to see policy outlining the approach for each area, as well as evidence of the technical implementation.

2211.2 - (MOD 000080) - (L1-L3)

Does the organisation require first-time and one-time passwords to be changed immediately after the first login?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, users are automatically prompted to reset their password on their first login.

Expected Evidence: The evidence you provide will depend on how you enforce the requirement. If you use policy, the Assessor will want to review the document. If it's set through an automated process, they will expect to see a demonstration or review the configuration setting in your Active Directory, IAM platforms or other management platform.

2213 - Automated password quality check

Control Requirement

The Applicant shall deploy technical controls to manage the quality of credentials across all identifiers. The technical controls should reflect industry standard requirements such as password length, complexity requirements (e.g. uppercase, lowercase, numbers and symbols), reuse history, prevent reuse of identifiers for a defined period, banned words and insecure pattern recognition (e.g. 1234), as appropriate.

Jargon Buster

The Automated Password Quality Checks control is about the tools or features used to assesses the strength of passwords. It wants to confirm you are making sure passwords meet certain quality standards or best practices.

2213.1 - (MOD 000403) - (L1-L3)

Does the organisation's password policy mandate that systems require standard user passwords to have at least a minimum length of 8 characters?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements for password length in policy document...
Expected Evidence: A copy of the policy

2213.2 - (MOD 000404) - (L1-L3)

Does the organisation's password policy restrict the re-use of at least the last 5 passwords for user accounts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set reuse requirements for passwords in policy document...

Expected Evidence: A copy of the policy

2214 - Repeated unsuccessful logon handling

Control Requirement

The Applicant shall employ policies and processes to appropriately manage unsuccessful login attempts to standard and privileged accounts. The Applicant shall lock accounts after at most ten unsuccessful login attempts for a minimum of 15 minutes, the duration of which should increase between multiple account lockouts.

Jargon Buster

What happens when you keep getting your username or password wrong? This control is about how you handle repeated unsuccessful login attempts.

2214.1 - (MOD 000407) - (L1-L3)

Does the organisation have policies and procedures in place for managing unsuccessful login attempts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is set in our… documents, they cover …, and define… they were last updated [date].
Expected Evidence: A copy of the policies and procedures

2214.2 - (MOD 000408) - (L1-L3)

Are there automated mechanisms in place to detect and respond to multiple unsuccessful login attempts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we…

Expected Evidence: Your Assessor will expect to see how you have configured your automated mechanism and then see a demonstration of an account failing to log in.

2214.3 - (MOD 000410) - (L1-L3)

Are unsuccessful login attempts regularly monitored and reviewed for signs of suspicious activity?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we can track login attempts through our...
Expected Evidence: Your Assessor will want to see how you monitor login activity and may ask you to explain what indicators you are looking for.

2214.4 - (MOD 000411) - (L1-L3)

Are there designated individuals or teams responsible for managing unsuccessful login attempts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is the responsibility of...
Expected Evidence: The contact details of this individual or team as your Assessor may want to follow up with an interview.

2214.5 - (MOD 000405) - (L1-L3)

How many incorrect password attempts are allowed before a standard user account is locked?

Available answers (choose one):

- ☐ At most 10 failed attempts
- ☐ More than 10 failed attempts

- ☐ No limit set

Example: No more than ten incorrect attempts.
Expected Evidence: Your Assessor will want to see how you have set up your incorrect password lockout feature. Similar to 2214.2, they may also request a demonstration showing an account being locked after several unsuccessful login attempts.

2214.6 - (MOD 000406) - (L1-L3)

How long are user accounts locked out for after failed login attempts?

Available answers (choose one):

- ☐ Less than 15 minutes
- ☐ 15 minutes or more

Example: Fifteen minutes
Expected Evidence: Your Assessor will want to see how you have set up your lockout feature.

2214.7 - (MOD 000089) - (L1-L3)

Does the duration of the account lockout increase on further unsuccessful login attempts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the lockout increases to...
Expected Evidence: Your Assessor will want to see how you have set up your lockout feature.

2215 - Replay-resistant authentication

Term

Replay attack: An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorised effect or gaining unauthorised access. (NIST definition)

Control Requirement

The Applicant shall enforce technical controls to protect against the capture of transmitted authentication or access control information and its subsequent retransmission i.e. replay attacks.

2215.1 - (MOD 000090) - (L1-L3)

Does the organisation implement technical controls to prevent replay attacks?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use...
Expected Evidence: There are a number of techniques to prevent replay attacks, your Assessor will want to see which countermeasures you have put in place. Penetration testing reports or a vulnerability scan could serve as supporting evidence.

2217 - Service accounts

Control Requirement

The Applicant shall inventory all generic, service, and system accounts used on the network. Every account shall be owned by a single named individual who is responsible and accountable for the account and its usage.

Term

A service account is a digital identity used by software applications or services to communicate, machine-to-machine, with other applications or the operating system. Service accounts execute automated tasks and functions without requiring direct human involvement.

Jargon Buster

The control wants to see how your organisation is implementing proper account management practices for generic service and system accounts. You should be able to demonstrate that you track these accounts with clear ownership and accountability for their management.

2217.1 - (MOD 000093) - (L1-L3)

Does the organisation maintain an inventory of all generic, service, and system accounts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this list can be found in...
Expected Evidence: Your Assessor will want to see how you are keeping an inventory of the accounts in question.

2217.2 - (MOD 000094) - (L1-L3)

Are generic and system accounts assigned a named individual responsible for the account and its usage?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the same list shows who is assigned...
Expected Evidence: Your Assessor will want to see a named individual for each account.

2218 - System users and processes

Control Requirement

The Applicant shall identify system users, processes acting on behalf of users, and devices.

Jargon Buster

The goal of this control is to ensure that every entity interacting with the system, whether it's a person, an automated process, or a device, can be uniquely identified.

2218.1 - (MOD 000095) - (L1-L3)

Does the organisation have a method of identifying system accounts and processes acting on behalf of actual users?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, users, processes acting on behalf of users, and devices are clearly distinguished using...
Expected Evidence: Your Assessor will want to see that tools are in place to support the identification of users, processes acting on behalf of users, and devices. They may want to see a list of tools used and are likely to ask for screenshots demonstrating how these tools are configured and utilised for monitoring.

2300 - Data security

<u>Control Requirement</u>

The Applicant shall appropriately protect data stored or transmitted electronically from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on functions or data. Such protection extends to how authorised users, devices and systems access critical data necessary for the operation of functions and use of data. Additionally, it covers information that would assist an attacker, such as design details of networks and information systems.

Jargon Buster

This is about data security and CIA fundamentals. After this control, we move onto two deeper data controls that look at data in transit and 'understanding data'.

This control is about your responsibility to ensure that electronic data stays confidential, keeps its integrity, and remains available only to those with permission to use it.

2300.1 - (MOD 000642) - (L1)

Has the organisation identified and documented where data meets the following criteria?

Available answers (Choose all that apply):

- ☐ Data is critical to the operation of Functions.
- ☐ Unauthorised access, modification or deletion could cause adverse impacts.
- ☐ Data could assist an attacker, such as network or system design details.
- ☐ None of the above.

Example: Yes, this was defined and documented in… (document name or reference)
Expected Evidence: Your Assessor will require documentation that demonstrates how the organisation has identified and documented data meeting the above criteria.

2300.2 - (MOD 000646) - (L1)

If none of the above criteria applied, does the organisation have policies in place to ensure only authorised users, devices, and systems have access to this data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will review the organisation's policies to confirm that access to this data is restricted to authorised users, devices, and systems.

2300.3 - (MOD 000647) - (L1)

Additionally, if you selected "None of the above" for question 2300.1, does the organisation have technical and procedural controls in place to protect this data from unauthorised access, modification, or deletion?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will review the organisation's technical and procedural controls to verify how the data is protected from unauthorised access, modification, or deletion.

2303 - Management of established network connections

Control Requirement

The Applicant shall terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Jargon Buster

This control wants you to confirm you are ending network connections when sessions finish or after a set time of no activity.

2303.1 - (MOD 000424) - (L1-L3)

Does the organisation require network connections to be terminated under the following conditions?

Available answers (Choose all that apply):

- ☐ At the end of sessions
- ☐ After a defined period of inactivity, no greater than 24 hours
- ☐ None of the above

Example: We terminate network connections when… (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Your Assessor will want to see how your network is set up to terminate connections, this could include a screenshot or screenshare of the rules, configurations or settings that would cause a connection to terminate.

2304 - Wireless network access control

Control Requirement

The Applicant shall ensure that the following controls apply to trusted organisational wireless networks:

- All users and devices must be authorised and authenticated prior to granting access to the network via the wireless network.
- The data transferred over the wireless network must be encrypted using WPA2 or above methodology.

Jargon Buster

This control sets the security expectations for your organisation's wireless network (Wi-Fi). It requires that anyone using Wi-Fi is both authorised (given permission to access the network) and authenticated (verified as who they say they are). It also expects you to be using at least WPA2. WPA2, which stands for Wi-Fi Protected Access 2, is a security protocol that helps protect your wireless network by encrypting the data being sent over it.

2304.1 - (MOD 000425) - (L1-L3)

Does the organisation require all trusted organisational wireless networks to authenticate users and devices and authorise them before granting access?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will want to see the access control settings for the network and may want you to show a device connecting to the network. They may want you to expand on how you (1) authenticate users, and (2) authorise users.

2304.2 - (MOD 000426) - (L1-L3)

Do all trusted organisational Wi-Fi networks require Wi-Fi Protected Access 2 (WPA2) or newer encryption standards?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will want to see the network settings showing that WPA2 is enabled.

2304.3 - (MOD 000468) - (L1-L3)

Does the organisation require visitors without trusted devices to use separate wireless networks which are segregated from trusted organisational networks?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the guest network is named... and is segregated from our trusted network.
The expectation is you either have a guest Wi-Fi, or you prohibit the connection of guests to your corporate Wi-Fi network. Anything else is considered a fail.

Expected Evidence: If you have a guest wireless network, your Assessor will want to see how it is isolated from the trusted network. For example, by separate hardware or subnetting.

2305 - Remote Access - VPN (Virtual Private Network)

Control Requirement

The Applicant shall ensure the following controls are enforced for staff to connect to organisational networks and systems using remote access technologies, for example VPN:

- Enable MFA prior to establishing a remote connection to the network.
- Encrypt all data transmitted over a VPN connection.
- Disable split-tunnelling to ensure all Data is only transmitted via organisation-controlled channels.

Jargon Buster

This control sets the security expectations for your organisation's Virtual Private Network (VPN). It requires the use of multi-factor authentication, expects that all data transmitted via the VPN is encrypted, and prohibits split tunnelling.

Split tunnelling is a networking technique that allows users to direct some traffic through the VPN while sending other traffic directly to the internet. This practice leads to inconsistencies and increases the possibility of data being exposed.

2305.1 - (MOD 000427) - (L1-L3)

Does the organisation require Multi-Factor Authentication (MFA) for users connecting remotely to its networks and systems?

Available answers (choose one):

☐ Yes
☐ No

Example: Yes, we have enabled MFA by…
Expected Evidence: Your Assessor will want to review the configuration settings that confirm MFA is enabled. They may also ask for a demonstration of someone connecting to the VPN or an explanation of the MFA method or approach implemented.

2305.2 - (MOD 000112) - (L1-L3)

Does the organisation encrypt all data transmitted through Virtual Private Network (VPN) connections?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will want to review the configuration settings that confirms encryption is enabled.

2305.3 - (MOD 000428) - (L1-L3)

Does the organisation disable split-tunnelling for users connecting remotely to its networks and systems, to ensure all Data is only transmitted via organisation-controlled channels?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will want to see the VPN configuration settings to confirm that split tunnelling is disabled. You can provide a screenshot or screenshare to show the specific settings where split tunnelling is turned off.

2306 - Remote access sessions

<u>Control Requirement</u>

The Applicant shall employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Jargon Buster

This control wants to confirm you use encryption to secure your remote access sessions and keep them private.

2306.1 - (MOD 000429) - (L1-L3)

Does the organisation use cryptography to secure remote access sessions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use...
Expected Evidence: You may have several types of remote access to consider, and your Assessor will want to work through them in a methodical manner.

2307 - Managed access control points

Control Requirement

The Applicant shall route remote access via managed access control points.

Jargon Buster

This is all about controlling traffic, such as routing external traffic through a firewall, secure gateway, or other network security device. When thinking about managed access control points, you can break down the wording into managed, which refers to it being monitored, configured, and maintained by IT or security personnel, and access control, which involves enforcing rules and policies to regulate and restrict access to the network or system, ensuring only authorised users and devices can connect.

2307.1 - (MOD 000115) - (L1-L3)

Does the organisation route all remote access connections through managed access control points?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, remote access connections are routed through... these are managed by... with access controlled through...
Expected Evidence: Your Assessor will expect to see a network architecture diagram showing how traffic is routed and managed.

2310 - Removable media

Term

Removable media refers to any type of storage device that can be easily inserted and removed from a computer or other electronic system. Examples include USB flash drives, external hard drives, memory cards, CDs, and DVDs. These devices are used to store, transfer, or backup data and can be taken from one computer to another.

Control Requirement

The Applicant shall:

- Maintain and manage an inventory of corporately owned removable storage media and devices.
- Encrypt removable media using secured and industry best practice methods.
- Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions.
- Prohibit the use of removable storage media and devices that are not corporately owned or authorised.

Jargon Buster

This control is about how you track your removable media and prevent the use of unapproved removable media. It's also about the steps you take, like encryption, to ensure the information on these devices is kept private.

2310.1 - (MOD 000122) - (L1-L3)

Does the organisation maintain an inventory of all its managed Removable Storage Media & Devices (RSM&D)?

Available answers (choose one):

☐ Yes
☐ No

Example: Yes, that can be found here...

Expected Evidence: The Assessor will review your inventory system for removable media, focusing on security-related details such as unique identifiers (e.g., serial numbers or asset tags), assigned owners, and the physical or logical location of each item. They may look for evidence to confirm the inventory is current and actively managed.

2310.2 - (MOD 000639) - (L1-L3)

Which encryption algorithm(s) does the organisation implement for its managed Removable Storage Media & Devices (RSM&D)?

Multiple-selection answers:

- ☐ Advanced Encryption Standard (AES) 256.
- ☐ Those approved by a national authority.
- ☐ Those approved by FIPS-140-2 or later.
- ☐ Other.

Example: We use... as covered in policy....
Expected Evidence: Your Assessor will need to see evidence that the policy is followed, such as a screenshot of the encryption process showing the encryption algorithm. This can be demonstrated by accessing the media, showing that it is initially inaccessible, decrypting it (e.g., entering a password or using a security key), and then accessing the files once the media is successfully decrypted. This can be presented through screenshots or a live demonstration during onsite visits.

2310.3 - (MOD 000432) - (L1-L3)

Does the organisation allow only corporately owned removable media & devices (RSM&D) to have read/write permissions?

Available answers (Choose all that apply):

- ☐ Granting read/write permissions only to authorised RSM&D.
- ☐ Prohibiting staff and visitors from using unauthorised RSM&D.
- ☐ None of the above.

Example: Yes, we... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Your Assessor will want to understand how you are meeting the requirement, whether through administrative policies, procedural controls, or technical solutions. The expected evidence will be dependent on your chosen measures but must show how your implementation sufficiently meets the requirement. Additionally, your response and evidence should address the management of legacy removable storage media to ensure comprehensive compliance. For example, avoid focusing solely on USB drives.

2311 - Authorised working locations

<u>Control Requirement</u>

The Applicant shall maintain and update a list of authorised working locations which are not the organisation's premise and communicate these locations to all employees and contractors.

Jargon Buster

This control is about the locations, other than a company main office, where your staff and contractors can work.

2311.1 - (MOD 000126) - (L1-L3)

Does the organisation maintain and update a list of authorised working locations (outside of the organisation's premises) and inform all staff of these locations?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements for authorised work locations in..., it covers ..., and defines... It was last updated [date]
Expected Evidence: A copy of the policy

2312 - Security at alternate working locations

Control Requirement

The Applicant shall employ technical security controls and educate users to reduce the security risks to employees while working outside the organisation's premises. Technical security controls for consideration may include, but are not limited to:

- Always-on VPN to protect data in-transit.
- Screen privacy protector to prevent shoulder surfing.
- Disabling USB ports on devices.
- Full disk encryption.

User awareness topics may include, but are not limited to:

- Risks of using public Wi-Fi.
- Avoid taking confidential phone calls within earshot of unauthorised individuals.
- Shoulder surfing.
- Avoid leaving devices unattended.

Jargon Buster

This control is about making sure that you are using both technology and training to keep your company information secure when employees work outside the office. This includes setting up secure connections, protecting screens from prying eyes, locking down ports to prevent unauthorised access, and encrypting data on devices. It also involves teaching employees how to stay safe when using public networks, discussing sensitive information, and handling their devices in public spaces.

2312.1 - (MOD 000433) - (L1-L3)

Does the organisation provide privacy protectors for devices when staff work in environments with an unacceptable risk of oversight from bystanders?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, all of our staff can request a privacy screen for their laptops. This is detailed in our Off-Site Working policy.
Expected Evidence: Policy or other evidence showing a suitable form of privacy protection solution.

2312.2 - (MOD 000128) - (L1-L3)

Does the organisation's user awareness training cover the cyber security risks of working outside the organisation's premises?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. This is detailed in our Off-Site Working policy, also part of our onboarding and annual refresher training.
Expected Evidence: Policy detailing the risks and solutions available, examples of user training and record of users completing the training.

2312.3 - (MOD 000434) - (L1-L3)

Does the organisation enforce the use of "always-on" Virtual Private Network (VPN) for endpoints where remote users are at risk?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. If a device is not connected directly to our internal network, then the VPN must be on; otherwise, the device is unable to send or receive any data to or from the internet.
Expected Evidence: Security or other policy covering VPN usage, VPN configuration

2312.4 - (MOD 000435) - (L1-L3)

Does the organisation manage and restrict the connection of peripherals/media to physical ports (e.g. USB, card reader, network port etc), except when authorised by policy?

This should be enforced by technical controls in addition to process and policy.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We disable USB ports by default and allow only company-supplied peripherals to be used.
Expected Evidence: Acceptable Use Policy, IT management or device configuration policy.

2312.5 - (MOD 000436) - (L1-L3)

Does the organisation risk assess and, unless required, disable USB and other physical ports on laptops and portable devices?

You may determine that some roles are automatically permitted to have ports enabled in order to perform their duties, e.g. penetration testers. Roles which do not require enabled ports should have them disabled by default configuration. Additionally, you must have a method for assessing the risks associated with enabling these ports

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We disable USB ports by default and allow only company-supplied peripherals to be used. If a port needs activation, this can be requested via the IT team unless it is already allowed as part of the role requirements.
Expected Evidence: Acceptable Use Policy, IT management or device configuration policy.

2312.6 - (MOD 000437) - (L1-L3)

Has the organisation implemented full disk encryption on all devices used by employees when working outside the organisation's premises?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, all devices (mobiles and laptops) have full encryption by default.
Expected Evidence: Policy or device image configuration document, screenshot of device configuration

2314 - Ensure UK GDPR compliance

Control Requirement

The Applicant shall align with the processing of personal data is conducted in compliance with the UK Data Protection Act 2018 (UK DPA).

This control wants you to show how you comply with UK Data Protection Act 2018. It is recommended to follow the guidance of the Information Commissioner's Office. The Defence Cyber Certification scheme assessment is limited in scope and does not guarantee compliance with GDPR.

A GDPR policy must adhere to core principles, regardless of business size. These principles include lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

2314.1 - (MOD 000447) - (L0-L3)

Does the organisation have documented policies and procedures which ensure compliance with obligations under the UK General Data Protection Regulation (GDPR)?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this can be found in…
Expected Evidence: The policies or procedures documenting how you are complying with UK General Data Protection Regulation. This may be a dedicated policy or incorporated within other company documentation, such as a risk register detailing the risks to the data subject. The size and nature of the organisation will determine the exact evidence available as smaller organisations may have simpler documentation compared to larger, more complex organisations.

2314.2 - (MOD 000446) - (L0-L3)

Does the organisation conduct Data Protection Impact Assessments (DPIAs) against data types it stores or processes?

Data Protection Impact Assessments (DPIAs) may include identifying data processing activities, assessing data types, identifying risks and impacts, mitigating risks and documenting them.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we rigorously conduct assessment by...
Expected Evidence: To show that you're thoroughly conducting Data Protection Impact Assessments, you could provide: the procedure you use outlining how you conduct Data Protection Impact Assessments, the template or tool used to complete an assessment, or a report showing the output from assessments.

2315 - Email authentication methods

Terms

Email spoofing involves crafting email messages with a falsified sender address. To combat this, several methods have been developed:

- The **Sender Policy Framework (SPF)** is an open standard specifying a technical method to prevent sender address forgery.[1]
- **DomainKeys Identified Mail (DKIM)** lets a recipient verify that an email sent from a domain was actually authorised by the domain's owner.
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** extends the above email authentication mechanisms to improve and monitor protection of the domain from fraudulent email.

Control Requirement

The Applicant shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.

Jargon Buster

You should be able to demonstrate the implementation of each of these by examining the headers of sent or received emails.

2315.1 - (MOD 000448) - (L1-L3)

Does the organisation implement Domain-based Message Authentication, Reporting and Conformance (DMARC) for all internet-facing email services?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: Your Certification Body Assessor will want to see configuration screenshots showing DMARC settings.

2315.2 - (MOD 000449) - (L1-L3)

Does the organisation implement DomainKeys Identified Mail (DKIM) to enhance trust in all internet-facing email services?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered in policy/process....

Expected Evidence: Your Certification Body Assessor will want to see configuration screenshots showing DKIM settings. You might also be able to present a sample email header that includes a valid DKIM signature.

2315.3 - (MOD 000450) - (L1-L3)

Does the organisation implement the Sender Policy Framework (SPF) to protect internet-facing email domains against spoofing?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered in policy/process....

Expected Evidence: Your Certification Body Assessor will want to see configuration screenshots showing SPF settings. You might also be able to present a sample email header that includes a received SPF pass result.

2316 - Personal and/or Personally Identifiable Information (PII) processing/transparency - control flow

Control Requirement

The Applicant shall employ systems to monitor and control the flow of all Personal and/or Personally Identifiable Information (PII) and all government information (e.g. OFFICIAL and above) provided or produced during the contract throughout the information lifecycle in accordance with approved authorisations, required legislation and contractual requirements.

Jargon Buster

This control wants you to show that you are tracking and managing information, shared or created during the contract. This includes Personal or Personally Identifiable Information (PII) and government information.

2316.1 - (MOD 000454) - (L1-L3)

Does the organisation have procedures in place to identify and authorise the flow of the following types of information?

Available answers (choose all that apply):

- ☐ Personal information provided or produced during a contract.
- ☐ Government information provided or produced during a contract.
- ☐ None of the above.

Example: Our… procedure identifies and authorises the flow of… (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: A procedure document or documents.

2316.2 - (MOD 000455) - (L1-L3)

Does the organisation require the flow of personal and government information to be controlled in accordance with the following?

Available answers (choose all that apply):

- ☐ Approved authorisations
- ☐ Applicable legislation
- ☐ Contractual requirements
- ☐ None of the above.

Example: We control the flow of personal and government information in accordance... (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: You may have forms or records linked to authorisation, a policy or section of a policy covering a legislative requirement or a clause in your contractual obligations.

2316.3 - (MOD 000456) - (L1-L3)

Does the organisation maintain documentation/diagrams of authorised personal and government information flows between the following?

Available answers (choose all that apply):

- ☐ Users
- ☐ Systems
- ☐ Networks
- ☐ Jurisdictions
- ☐ None of the above.

Jargon Buster

This question is looking at how you outline the flow of information.

Example: Yes, this information can be found in the...

Expected Evidence: Anything that illustrates how information flows and who has access to it, either in documents or diagrams.

2316.4 - (MOD 000457) - (L1-L3)

Does the organisation employ systems to control the authorised flow of personal and government data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Jargon Buster

This question is looking at how you've implemented the previous question's answer- for example, mechanisms or systems that manage that flow of information.

Example: *Yes, we use...*

Expected Evidence: *Something to show the previous answer in practice.*

2316.5 - (MOD 000458) - (L1-L3)

Does the organisation employ systems to monitor personal and government data flows to ensure compliance with its authorisations?

Available answers (choose one):

- ☐ Yes
- ☐ No

Jargon Buster

This question is checking if you've set up tools or processes that keep an eye on the movement of the data.

Example: *Yes, we use...*

Expected Evidence: *Your Certification Body Assessor will probably want to see a screenshot or screenshare of the tolls you are using.*

2317 - Endpoint encryption

An endpoint is any device that connects to a computer network and serves as a point of communication or interaction. Endpoints are typically user-facing devices that can send, receive, or process data. For example, laptops, desktops, smartphones etc...

Control Requirement

The Applicant shall implement and maintain full disk-level encryption on all endpoints to industry standard solutions, for example, full disk encryption solutions using AES-256 encryption algorithm or FIPS equivalent.

2317.1 - (MOD 000632) - (L1-L3)

Does the organisation implement and maintain full disk-level encryption on all endpoints?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have full disk encryption on all endpoints covering laptops, desktops smartphones, ...

Expected Evidence: There are multiple ways to demonstrate Full Disk Encryption to an Assessor, ranging from checking the encryption status to providing reports, demonstrating key management, or using compliance tools.

2317.2 - (MOD 000459) - (L1-L3)

Which encryption algorithm(s) does the organisation implement for endpoint full disk encryption?

Available answers (choose all that apply):

- ☐ AES-256
- ☐ Other algorithms employed within Endorsed Encryption Products notified by MOD Industry Security Notices
- ☐ Other algorithms approved by FIPS-140-2 or later

☐ Additional algorithms not covered above

Example: We use... for... and...

Expected Evidence: Your Certification Body Assessor will expect to see documentation specifying the encryption used for full disk encryption - for example, your hardening guide - and will likely want to see a screenshot showing the configuration in a tool such as an endpoint manager.

2318 - Approved cryptographic methods

<u>Control Requirement</u>

The Applicant shall employ appropriate nationally or departmentally approved cryptography when used to protect all data (e.g. FIPS 140-2 or comparable standards)

Jargon Buster

Control 2318 looks at cryptography with a focus on digital certificates and the way you handle them using Certificate Authority (CA).

A certificate authority or certification authority (CA) is an entity that stores, signs, and issues digital certificates. In cryptography, digital certificates are used to prove the validity of a public key which are used in asymmetric cryptography.

2318.1 - (MOD 000631) - (L1-L3)

Does the organisation have a policy governing the use of cryptographic methods?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set governing cryptographic methods in..., it covers ..., and defines... It was last updated [date].
Expected Evidence: A copy of the policy.

2318.2 - (MOD 000633) - (L1-L3)

What cryptographic methods does the organisation use when protecting data with encryption?

Available answers (choose all that apply):

- ☐ Methods approved in FIPS-140-2 or later.
- ☐ Methods approved by a national authority.
- ☐ None of the above.

Example: Our cryptographic methods are…
Expected Evidence: Depending on the selected answer, your Certification Body Assessor may expect to see - Documentation or screenshots showing FIPS compliant modes are enabled or something to show your chosen cryptographic methods on a list approved by a national authority or MOD.

2319 - Securely manage cryptographic keys

Control Requirement

The Applicant shall establish and manage cryptographic keys for cryptography employed in organisational systems using appropriate nationally or departmentally approved solutions (e.g. FIPS 140-2 or comparable standards).

Jargon Buster

Control 2319 looks at cryptography with a focus on the management of cryptographic keys themselves.

2319.1 - (MOD 000460) - (L1-L3)

Does the organisation’s encryption key management policy and procedures cover the following aspects?

Available answers (choose all that apply):

- ☐ Required key lengths
- ☐ Secure storage, distribution and update of cryptographic keys
- ☐ Cryptographic keys revocation
- ☐ Management of lost, corrupt and expired keys
- ☐ Maintenance of cryptographic key backups
- ☐ Cryptographic key activation and deactivation dates
- ☐ Restriction of cryptographic key access to authorised individuals
- ☐ Compliance with local legal and regulatory requirements for cryptography
- ☐ None of the above

Example: Yes, we set encryption key management requirements in..., it covers ..., and defines... It was last updated [date] (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: The procedure/procedures or policy/policies where this information is documented.

2321 - Publicly accessible data

Control Requirement

The Applicant shall:

- Designate individuals authorised to make information publicly accessible.
- Train authorised individuals to ensure that publicly accessible information does not contain non-public information.
- Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included.
- Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.

Jargon Buster

Publicly accessible information could include press releases, social media updates, product road map etc. Non-public information would cover data that has been classified or labelled as non-public.

2321.1 - (MOD 000161) - (L1-L3)

Does the organisation have designated individuals authorised to make information publicly available?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is....
Expected Evidence: Something to show who this is. Something to show their job title, role or description.

2321.2 - (MOD 000162) - (L1-L3)

Does the organisation train designated individuals to ensure that publicly accessible information does not contain non-public information?

Training should include topics such as data classification, data privacy regulations, security best practices, and identifying non-public information that should not be disclosed.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a training program in place.
Expected Evidence: Something to prove you're doing training. Copies or screenshots of the training materials and a record of attendance for the last ... training sessions.

2321.3 - (MOD 000163) - (L1-L3)

Does the organisation review proposed content before posting it to publicly accessible systems to ensure that non-public information is not included?

Jargon Buster

Before making content available on a public system, does your organisation conduct a review to make sure private information is not included?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the formal process is detailed in...
Expected Evidence: You may use something like a policy that outlines the steps taken, checklists or guidelines used by the reviewer, or records of content reviews.

2321.4 - (MOD 000164) - (L1-L3)

Does the organisation periodically review the content on publicly accessible systems for non-public information and remove such information if discovered?

Jargon Buster

Is your organisation reviewing the content on its public systems to make sure that non-public information has not been inadvertently disclosed, and to remove such information if it is found?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the organisation conducts regular reviews of all content in line with...

Expected Evidence: Something to show the activity is being carried out such as minutes from meetings, a report from the last review cycle, and something to show how often this review takes place.

2322 - Mobile devices/Bring Your Own Device (BYOD)

Control Requirement

The Applicant shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.

2322.1 - (MOD 000463) - (L1-L3)

Does the organisation ensure all mobile devices accessing its corporate environment/Data are appropriately configured and managed using Mobile Device Management (MDM) or equivalent solutions?

Jargon Buster

Is a Mobile Device Management (MDM) system in place to monitor company mobile devices?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we are using … to manage mobile devices.
Expected Evidence: You may consider using screenshots of the current configuration profile, logs or reports produced by your MDM system.

2322.2 - (MOD 000169) - (L1-L3)

Does the organisation have a process to disable or wipe organisation data if the mobile device is stolen or lost?

Jargon Buster

Can you remotely disable or wipe data from a device in case it is stolen or lost?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the MDM system includes the capability to remotely disable access to the device and wipe data.
Expected Evidence: You might consider the following: a technical document or manual showing the MDM capability, a screenshot of the MDM interface showing the remote wipe/disable options, or a procedure or guidance document showing how to remotely wipe a device.

2323 - Secure destruction

Control Requirement

The Applicant shall, where not otherwise stated explicitly by country, legislation or authority instructions, implement procedures to ensure that all data is securely destroyed when no longer needed, or at the expiration or termination of the agreement.

Supplier shall:

- Secure and confirm the erasure of data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal.
- Provide attestation of destruction, where specified by contract with authority.
- Require that any third parties engaged to process the data shall securely dispose of such data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or authority instructions.

Jargon Buster

This control is about how you clear data from devices once it is no longer needed.

2323.1 - (MOD 000465) - (L1-L3)

Has the organisation implemented procedures to ensure that all Data is securely destroyed when no longer required?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we've established comprehensive data destruction procedures to...
Expected Evidence: You should have a documented data destruction policy that outlines the methods and circumstances under which data should be securely destroyed.

2323.2 - (MOD 000173) - (L1-L3)

Does the organisation ensure any third parties engaged to process Data securely dispose of such Data when no longer required?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we've made sure that our third-party contracts specify …
Expected Evidence: You may reference contracts or service agreements with third-party providers which specify the requirement. You may refer to certificates of destruction provided by third parties. You may have a process for monitoring and verifying that third parties comply with data destruction requirements.

2400 - System security

Control Requirement

The Appliant shall ensure that network and information systems and technology critical for the operation of business functions and protection of data are protected from cyber-attack. An organisational understanding of risk to business functions and protection of data informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

Jargon Buster

Have you hardened your network and devices? This control expects you to firstly identify critical systems and understand risks, then apply appropriate security measures.

2400.1 - (MOD 000466) - (L1-L3)

Does the organisation identify the systems and technologies critical to the operation of its Functions and protection of Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the organisation employs a risk-based security strategy, conducting...
Expected Evidence: A risk assessment policy and/or report should demonstrate this.

2400.2 - (MOD 000640) - (L1-L3)

Does the organisation protect critical systems from cyber-attacks by implementing system security measures based on its understanding of risks to Functions and Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, once we've identified the critical systems and their risks, we...
Expected Evidence: Your Assessor will want to trace a risk identified in your risk assessment to a security measure you implemented to mitigate it. For example, if you changed your network infrastructure and identified it as a risk, you might have needed to update your firewall, and they would want to see the newly created rule.

2401 - Secure configuration

Control Requirement

The Applicant shall securely configure the network and information systems that support the operation of business functions and that protect data.

Jargon Buster

This control expects you to have mechanisms in place to support secure configuration of network and information systems that support the operation of business functions that protect data.

This may be using automated configuration scripts, infrastructure as code, manual configurations with a checklist or even build images containing preconfigured and standardised settings used as a baseline. At a minimum, these mechanisms must apply to endpoints and servers, but ideally, they should cover all systems capable of supporting the mechanisms.

These mechanisms should include configurations for:

i. Endpoint encryption
ii. Limiting the write functionality on removable media (inc. mobile devices)
iii. Password protected screen saver automatically applies after 15 minutes
iv. Restricting the ability to install unauthorised software
v. Restricting the ability to execute privileged functions such as editing the register

2401.1 - (MOD 000649) - (L1-L3)

Does the organisation have mechanisms in place for securely configuring the network and information systems that support its Functions and protect data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have documented build processes for all of our devices.

Expected Evidence: Build process policy/process, device onboarding process

2401.2 - (MOD 000XXX) - (L1-L3)

Do the mechanisms include the below?

Available answers (choose all that apply):

- ☐ Endpoint encryption.
- ☐ Limiting the write functionality on removable media (inc. mobile devices).
- ☐ Password protected screen saver automatically applies after 15 minutes.
- ☐ Restricting the ability to install unauthorised software.
- ☐ Restricting the ability to execute privileged functions such as editing the register.

Example: Yes. Our build process covers all of the above
Expected Evidence: Onboarding/build policy/process showing the mechanisms used and the resulting configurations.

2401.3 - (MOD 000XXX) - (L1-L3)

Does the organisation have mechanisms to ensure secure configurations are maintained?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we review our device onboarding/build policy/process at least annually or when a new device type is onboarded. We ensure existing device configurations are up to date and maintained with automated configuration scripts and MDM.
Expected Evidence: Build process policy/process, device onboarding process, document history showing reviews and changes, logs of updates

2402 - Vulnerability management

Control Requirement

The Applicant shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by:

- Performing vulnerability scans on a monthly basis and during any major system or application updates
- Implementing vendor patches or fixes prioritising using the CVSS v3 scoring
- Developing a Risk Treatment Plan to address identified vulnerabilities

The Applicant shall address vulnerabilities in accordance with the Applicant's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.

Jargon Buster

In essence, this control is about making sure you're taking proactive and systematic steps to keep your systems secure, by regularly scanning and addressing vulnerabilities.

2402.1 - (MOD 000473) - (L1-L3)

Does the organisation have a vulnerability management process in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our process for vulnerability management is set out in…, it covers …, and defines… It was last updated [date]
Expected Evidence: A copy of the process

2402.2 - (MOD 000474) - (L1-L3)

Does the organisation ensure systems are scanned for vulnerabilities:

Available answers (Choose all that apply):

- ☐ At least monthly.
- ☐ Following major system or application updates.
- ☐ None of the above.

Example: We scan systems…[when]
Expected Evidence: Vulnerability scan logs or a series of vulnerability scan reports will probably be enough to show your Assessor if you are achieving the selected answers.

2402.3 - (MOD 000475) - (L1-L3)

Does vulnerability scanning include all:

Available answers (Choose all that apply):

- ☐ Web services
- ☐ Applications
- ☐ Infrastructure / Networks
- ☐ None of the above

Example: Our scans cover… (in your answer consider both in house versus third party testing. The routine, schedule or frequency of the various scopes your organisation may have and the degree of maturity which these systems demonstrate.)
Expected Evidence: Your Assessor will want to see the scope of your vulnerability scans and compare this against the scanner configuration and scan reports.

2402.4 - (MOD 000183) - (L1-L3)

Does the organisation develop risk treatment plans to address (remediate or mitigate) identified vulnerabilities promptly?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use the CVSS, KEV and EPSS scores to determine the risk and priority for remediation. Our risk management plans then detail how to address the vulnerability depending upon the most appropriate process.
Expected Evidence: Risk management/treatment plan/policy, log or history of actions taken, notes from meetings discussing mitigating/remediating vulnerabilities.

2402.5 - (MOD 000184) - (L1-L3)

Does the organisation have defined timelines for addressing vulnerabilities?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is defined in...
Expected Evidence: A copy of the document that defines timelines for addressing vulnerabilities.

2402.6 - (MOD 000476) - (L1-L3)

Is the organisation's timeline for addressing critical severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Available answers (choose one):

- ☐ Within 15 days
- ☐ Outside 15 days

Example: Vulnerabilities with these CVSSv3 scores are dealt with in... days

Expected Evidence: Ideally, your Assessor would like to see documentation or tracking records that demonstrate vulnerabilities being identified, assigned to an owner, remediated (e.g., fixed or patched), and validated as remediated within the specified remediation timeframe.

2402.7 - (MOD 000477) - (L1-L3)

Is the organisation's timeline for addressing high severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Available answers (choose one):

- ☐ Within 30 days
- ☐ Outside 30 days

Example: Vulnerabilities with these CVSSv3 scores are dealt with in... days
Expected Evidence: Ideally, your Assessor would like to see documentation or tracking records that demonstrate vulnerabilities being identified, assigned to an owner, remediated (e.g., fixed or patched), and validated as remediated within the specified remediation timeframe.

2402.8 - (MOD 000478) - (L1-L3)

Is the organisation's timeline for addressing medium severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Available answers (choose one):

- ☐ Within 90 days
- ☐ Outside 90 days

Example: Vulnerabilities with these CVSSv3 scores are dealt with in... days
Expected Evidence: Ideally, your Assessor would like to see documentation or tracking records that demonstrate vulnerabilities being identified, assigned to an owner, remediated (e.g., fixed or patched), and validated as remediated within the specified remediation timeframe.

2402.9 - (MOD 000479) - (L1-L3)

Is the organisation's timeline for addressing low severity vulnerabilities (as defined by the Common Vulnerability Scoring System v3):

Available answers (choose one):

- ☐ Within 180 days
- ☐ Outside 180 days

Example: Vulnerabilities with these CVSSv3 scores are dealt with in... days
Expected Evidence: Ideally, your Assessor would like to see documentation or tracking records that demonstrate vulnerabilities being identified, assigned to an owner, remediated (e.g., fixed or patched), and validated as remediated within the specified remediation timeframe.

2403 - Penetration testing

<u>Control Requirement</u>

The Applicant shall conduct penetration testing (minimum every 12 months) against externally facing systems used to support the operation of functions and that protect data. The penetration testing programme shall be based upon industry standards and performed by approved subject matter experts. The Applicant shall ensure that any deficiencies identified are remediated in a timely manner in line with their risk to the network. The Applicant shall retain records including:

- The scope and methodology utilised.
- The number of critical, high, and medium severity findings.
- The name of the tester.
- The date of the testing.
- Timelines and actions for a remedial plan.

Jargon Buster

Fundamentally, this control wants to confirm that your organisation is undergoing annual penetration tests carried out by an approved and qualified tester who is following industry testing standards. It also requires you to keep your penetration test reports which should cover the details in the bulleted points.

A redacted pen-test report may answer multiple questions in this control.

2403.1 - (MOD 000480) - (L1-L3)

Does the organisation ensure that penetration testing is conducted on externally facing systems at least every 12 months?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last penetration test was [date]

Expected Evidence: The last three penetration test reports, or as many as are available if your organisation has been operating for less than three years.

2403.2 - (MOD 000192) - (L1-L3)

Is the organisation's penetration testing programme based on industry standards and conducted by subject matter experts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use a third party, their testing is based on...
Expected Evidence: Your Assessor would expect evidence to show the standard followed and proof of the tester's qualifications. This could include a sample penetration test report showing the methodology used or evidence of the tester's certifications and expertise.

2403.3 - (MOD 000481) - (L1-L3)

Which of the following does the organisation's penetration testing records include?

Available answers (choose all that apply):

- ☐ Test scope and methodology
- ☐ Findings by severity
- ☐ Name of the tester (organisation / individual)
- ☐ Testing date
- ☐ Remedial action plan with timelines
- ☐ None of the above

Example: Our reports cover...
Expected Evidence: A sample penetration test report will cover all of the above.

2404 - Change management

Control Requirement

The Applicant shall formally document, publish and annually review (minimum every 12 months) the change control procedures to manage changes to information systems, supporting infrastructure and facilities.

The change management policy includes:

- Definitions of the types of changes (e.g. standard, critical, emergency) along with their associated processes.
- Roles and responsibilities for those involved in the change, or approving the change.

Prior to implementing any changes, Applicant shall:

- Establish acceptance criteria for production change approval and implementation.
- Require stakeholder approval prior to any change implementation.
- Formally record the change in a centralised repository.
- Document the findings of business impact analysis outcomes and document back-out procedures should the change fail.
- Keep a full audit trail of the change request, testing conducted, associated documentation, approvals and outcomes.
- Document and record the outcomes of security impact analysis outcomes along with any mitigating actions.

2404.1 - (MOD 000482) - (L1-L3)

Does the organisation have formal change management policies, processes and procedures in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is covered in...

Expected Evidence: A copy of the policy, process or procedure document.

2404.2 - (MOD 000483) - (L1-L3)

Are the organisation's change management policies, processes and procedures reviewed at least annually?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this was last updated [date]
Expected Evidence: Your Assessor will want to examine the revision history of the provided document to check for updates or annual reviews.

2404.3 - (MOD 000484) - (L1-L3)

Which of the following are included in the organisation's change management policy?

Available answers (Choose all that apply):

- ☐ Roles and responsibilities for change management
- ☐ The types of change (e.g. standard, normal, emergency)
- ☐ Required processes and procedures
- ☐ None of the above

Example: The policy covers… (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Your Assessor will need to identify where your chosen answers are located within the provided policy document.

2404.4 - (MOD 000485) - (L1-L3)

Prior to implementing a change, which of the following are undertaken?

Available answers (Choose all that apply):

- ☐ Acceptance criteria are established
- ☐ A change record is kept in a central repository
- ☐ Business impact of change failure is analysed
- ☐ Security impact of change is analysed and recorded
- ☐ Any security mitigations required are documented
- ☐ Back-out procedures are documented
- ☐ Stakeholder approval is obtained
- ☐ None of the above

Example: Yes, we... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: Your Assessor will want to see documented proof to support each selected answer, so consider how you are recording each step. If you are tracking changes, they will expect to see a well-maintained and up-to-date log. For changes that require approval, they will want evidence of who granted the approval. You may choose to walk your Assessor through specific change scenarios that you have managed, demonstrate the process and outcomes whether they were successful, unsuccessful, or reverted changes.

2404.5 - (MOD 000486) - (L1-L3)

Which of the following are retained as an audit trail of a change?

Available answers (choose all that apply):

- ☐ Test history & documentation
- ☐ Approvals
- ☐ Change outcome
- ☐ None of the above

Example: We retain...
Expected Evidence: If you say you retain them, the Assessor will expect to review them.

2405 - Patch management

Control Requirement

The Applicant shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Applicant shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline.

The Applicant shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.

2405.1 - (MOD 000199) - (L1-L3)

Does the organisation have a patch management policy and programme in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the policy is..., the policy/programme covers ..., and defines... It was last updated [date]
Expected Evidence: A copy of the policy

2405.2 - (MOD 000487) - (L1-L3)

Does the organisation monitor its technology vendors to ensure timely awareness of updates for its endpoints, network devices, and software?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we do this by….
Expected Evidence: Your Assessor will want to see how you monitor this; It could be as simple as email notifications or something more advanced like an automated monitoring system.

2405.3 - (MOD 000488) - (L1-L3)

Does the organisation assess which vendor updates address vulnerabilities?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we install patches/security updates as soon as they are available and have been tested. We install software feature updates at a slower pace as most are not required.
Expected Evidence: Patching/update policy/process, update history/log

2405.4 - (MOD 000489) - (L1-L3)

Does the organisation ensure patches are tested before deployment to critical production environments?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we test patches and updates on test devices before starting a phased rollout deploying them to the rest of the estate.

Expected Evidence: Patching policy/process, logs showing how updates/patches are tested and rolled out

2405.5 - (MOD 000490) - (L1-L3)

Does the organisation ensure systems are patched promptly, and within 14 days of an update being released which addresses a vulnerability classified by the product vendor as 'critical' or 'high risk'?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, all critical or high-risk updates are applied within 14 days.
Expected Evidence: Patching policy/process, update history/log, meeting notes where vulnerabilities have been discussed. CE/CE+ report may also be used to show this control is met.

2405.6 - (MOD 000491) - (L1-L3)

Does the organisation have processes in place to enable out-of-band emergency patching?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our… policy has a special process for emergency patching, it covers … was last updated [date] and was last used [date]
Expected Evidence: Your Assessor will want to see the steps you follow for emergency patching. This could include documentation such as a playbook or procedure that outlines how you handle unscheduled, security-critical updates. If tooling plays a part in your process, they may also wish to see the tooling used. They may also want to review real-world examples of the process in action. If you've used your emergency patching in the past, they may want to discuss what happened.

2407 - Privacy warning notices - specific handling

Control Requirement

The Applicant shall ensure that users accept appropriate warning notices prior to information system access where information systems contain information with specific handling requirements imposed by the UK or its International Partners.

Such warnings must only be provided to authenticated users. At a minimum, users must be warned that:

- The information system contains information with specific requirements imposed by the UK and/or international partner nations.
- Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.

Jargon Buster

This control requires you to ensure that only authenticated users are presented with and accept warnings before accessing systems containing sensitive information. These warnings must clearly explain the rules for handling and using the information.

2407.1 - (MOD 000204) - (L1-L3)

Does the organisation ensure users acknowledge warning notices before accessing systems with specific handling requirements, where mandated by the UK and/or international partner nations?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: The Assessor will expect to see copies or screenshots of the warning notices used. During an onsite visit the Assessor may want to see proof that the notice is presented to the user once accessing the system.

2407.2 - (MOD 000205) - (L1-L3)

Which of the following are included within your warning notices for systems which have specific handling requirements imposed by the UK or its International Partners:

Available answers (Choose all that apply):

- ☐ The information system contains information with specific requirements imposed by the UK and/or international partner nations
- ☐ Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.
- ☐ None of the above

Example: All of the above. Once a user has successfully logged in, they are shown a warning notice detailing the specific handling requirements.
Expected Evidence: The Assessor check that the notices clearly include words to the effect of the selected statements.

2407.3 - (MOD 000492) - (L1-L3)

Does the organisation ensure that warning notices regarding specific handling requirements are only provided to authorised and authenticated users?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will expect to see an example notice clearly explaining the specific handling requirements for the information system.

2408 - Screen locking/timeouts

Control Requirement

The Applicant shall have controls in place to automatically lock user sessions after a predefined period. The lock screen shall conceal all information previously displayed on the screen and prevent unauthorised viewing of data.

2408.1 - (MOD 000206) - (L1-L3)

Does the organisation automatically lock user sessions on all devices after a predefined period of inactivity?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is set for 5minutes and is set by a defined build configuration.
Expected Evidence: Your Assessor will want to see a screenshot of the system configuration that shows the automatic session lock settings. Alternatively, they may accept documentation or a policy that defines the period of inactivity. A live demonstration onsite is unlikely to be required.

2408.2 - (MOD 000493) - (L1-L3)

Is the organisationally defined period of inactivity for users:

Available answers (choose one):

- ☐ 15 minutes or less
- ☐ More than 15 minutes

Example: The period is…, as defined in…..
Expected Evidence: Your Assessor will likely ask for a screenshot of the system configuration that displays the inactivity timeout setting. They may also accept documentation or a policy that specifies the defined period of inactivity.

2408.3 - (MOD 000208) - (L1-L3)

Do locked user sessions and lock screens conceal all information previously displayed on the screen?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Configuration settings, screenshot. Your Assessor will expect a demonstration showing that when a device is locked, no information from the previous session is visible on the screen.

2409 - Identify allowed programs

Control Requirement

The Applicant shall identify software programs authorised to execute on the corporate environment. For all other programs employ a block by default, permit-by-exception policy.

Jargon Buster

We need you to show how you manage the software running on your systems. Your responses should explain how you determine which programs are allowed to run and how you make sure all other programs are blocked by default. If you allow exceptions for certain blocked programs, describe the process you use to review and approve them. Control 2410 is very similar but focuses on the periodic review and management of the authorised software list. For control 2409, focus on how you identify and manage the software programs that are allowed to run.

2409.1 - (MOD 000209) - (L1-L3)

Does the organisation maintain an up-to-date list of authorised software?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the authorised list can be found... it was last updated [date]
Expected Evidence: Your Assessor will want to see where the authorised software is logged. This could include screenshots, a copy of the list, or, during an onsite, access to the system where the list is maintained.

2409.2 - (MOD 000210) - (L1-L3)

Does the organisation implement a 'block by default, permit-by-exception' policy for software not on the authorised list?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is defined in the... policy. We enforce it by...
Expected Evidence: Your Assessor will want to see documentation or proof that the 'block by default, permit-by-exception' policy is in place. This might be proven by a copy of the relevant policy document or screenshots or reports from tools used to enforce the policy.

2410 - Review the list of approved software

Control Requirement

The Applicant shall review and manage the list of authorised software programs at least every 90 days.

Jargon Buster

Control 2409 is very similar but focuses on identifying and managing the software programs that are allowed to run. For control 2410, focus on how you periodical review and manage your authorised software list.

2410.1 - (MOD 000211) - (L1-L3)

Does the organisation review its list of authorised software programs at least every 90 days?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last review was [date]
Expected Evidence: Your Assessor will want to see the list and will look to verify that it has been updated at least every 90 days.

2411 - Secured internet access

Control Requirement

The Applicant shall ensure the following internet controls are enforced on endpoints:

- Technical controls to prevent malware infection from internet browsing are in place.
- Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.)
- Prevent code being launched on the corporate host.
- Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan.
- Automatically block suspicious traffic and communications.
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)

2411.1 - (MOD 000494) - (L1-L3)

Does the organisation enforce endpoint controls for internet access, in line with its internet access policy, to block the following?

Available answers (choose all that apply):

- ☐ Malware infections from internet browsing
- ☐ Access to undesirable internet resources (e.g. malicious websites, inappropriate content, etc...)
- ☐ Web Application Software
- ☐ Execution of code on the endpoint
- ☐ Downloads without sandboxing and anti-malware scanning
- ☐ Suspicious traffic and communications

- ☐ None of the above

Example: Yes, we ... (For each selected answer, clearly explain how you are doing what you say you are doing.)
Expected Evidence: For each selected answer, your Assessor will expect to see evidence such as logs or reports from the tools or technical solutions, screenshots or configuration settings, or examples of alerts and notifications.

2411.2 - (MOD 000495) - (L1-L3)

Where the organisation's policy permits any of the above activities due to business need, does it ensure processes and technologies are in place to mitigate the additional risk?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our organisation permits some of the above activities due to specific business needs, and we have implemented... (clearly explain how you are doing what you say you are doing.) OR no, our organisation does not permit any of the above activities.
Expected Evidence: If you permit any of the above activities, your Assessor will expect to see evidence of the processes or technologies you have implemented as a work around. This may include demonstrating your understanding of the risk, how you planned and implemented mitigation measures, how you monitor or enforce these controls, and how you review them to ensure they effectively address the risk. If you do not permit the above activities, 2411.1's evidence will cover you.

2411.3 - (MOD 000496) - (L1-L3)

Does the organisation ensure auditing is enabled for internet access endpoint controls?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will expect to see an example of the audit reports generated by the endpoint controls monitoring internet access.

2411.4 - (MOD 000497) - (L1-L3)

Does the organisation ensure security operators are alerted to blocked internet activity?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will expect to see an example of the alert generated by blocked internet activity.

2411.5 - (MOD 000498) - (L1-L3)

Does the organisation ensure systems terminate connections to internet resources at the end of sessions or after a defined period of inactivity?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will likely ask for a screenshot of the system configuration that displays the inactivity timeout setting.

DCC
Defence Cyber Certification

iasme

2412 - Voice over Internet Protocol (VoIP)

Control Requirement

The Applicant should establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and ensure controls are in place to authorise, monitor, and control the use of VoIP within the information system.

2412.0 - (MOD 000XXX) - (L1-L3)

Does the organisation use Voice over IP (VoIP) technologies?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use VOIP technology…
Expected Evidence: Details of technology in use such as app on a device, any policy/process documentation covering its use.

2412.1 - (MOD 000643) - (L1-L3)

Does the organisation have a documented policy in place for the use of Voice over IP (VoIP) technologies?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements for VoIP in…, it covers …, and defines… It was last updated [date]
Expected Evidence: A copy of the policy.

2412.2 - (MOD 000644) - (L1-L3)

Has the organisation's Voice over IP (VoIP) policy been informed by a risk assessment of malicious VoIP usage?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we assessed VOIP technology before implementing it
Expected Evidence: Your Assessor will want to see the risk assessment.

2412.3 - (MOD 000645) - (L1-L3)

Are all VoIP technologies in the organisation:

Available answers (Choose all that apply):

- ☐ Authorised before deployment or use
- ☐ Monitored for unauthorised or malicious use
- ☐ Controlled, such as through firewall rules and endpoint controls
- ☐ None of the above

Example: This question is for informational purposes only and is not scored. However, we encourage you to provide a detailed response to help Assessors understand your approach.
Expected Evidence: As above.

2413 - Mobile code management

Control Requirement

The Applicant shall define acceptable and unacceptable mobile code, and ensure controls are in place to identify, authorise, monitor, review, and control the use of mobile code within the organisation.

Term

The National Institute of Standards and Technology (NIST) defines mobile code as a software program or a part of a program that is obtained from remote systems, transmitted over a network, and executed on a local system without requiring the recipient to explicitly install or run it.

Mobile code isn't a traditional app you install on your computer or phone. Instead, it's a program sent to your device by a server over the internet. It runs seamlessly within an application like your browser, letting you jump straight into the action without any extra steps.

A workplace example would be online training delivered through a Java program.

2413.1 - (MOD 000500) - (L1-L3)

Does the organisation define acceptable and unacceptable use of mobile code?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we documented this in...
Expected Evidence: A copy of the document or the location where it is recorded.

2413.2 - (MOD 000501) - (L1-L3)

Does the organisation ensure controls are in place to identify, authorise, monitor, review, and control the use of mobile code within the organisation?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have implemented several controls designed to... (Clearly describe each control you have in place and explain its intended purpose and explain what it is designed to do and how it operates.)
Expected Evidence: The Assessor will expect to see evidence such as policies or procedures detailing how mobile code is managed, logs or reports showing monitoring and authorisation activities, and screenshots or configurations enforcing restrictions or permissions. They may also look for examples of alerts triggered by unauthorised activity, records of periodic reviews or audits, and evidence of staff training or awareness programs on mobile code risks and controls. This evidence should demonstrate that the organisation effectively identifies, authorises, monitors, and controls mobile code use.

2414 - Communication authenticity protection

Control Requirement

The Applicant shall use secure network management and communication protocols to protect session authenticity addressing communications protection at the session level.

Jargon Buster

Some protocols are not very secure, and ways have been found to exploit this weakness. Other protocols are unencrypted, which may allow someone to read your network traffic. The insecure/unencrypted versions should be disabled, and newer versions of the protocols should be used.

2414.1 - (MOD 000502) - (L1-L3)

Does the organisation protect communication sessions requiring authenticity by enforcing secure communication protocols?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We have disabled FTP, HTTP, Telnet, POP3, SSL and other weak protocols.
Expected Evidence: Configuration policy/processes, configuration screenshots, Security Policy, hardening guides.

2417 - Authorise remote execution of privileged commands

<u>Control Requirement</u>

The Applicant shall ensure that all remote users acquire appropriate authorisation prior to accessing and/or executing privileged functions.

2417.1 - (MOD 000224) - (L1-L3)

Does the organisation ensure that appropriate authorisations and approvals are granted before privileged actions are carried out remotely?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. All external connections must authenticate being before allowed access. Remote users who are authenticated must then undergo further authentication before being allowed to perform privileged functions. Approval to perform privileged functions must be sought via our IT team who will grant them to the user if appropriate.
Expected Evidence: Policy governing remote access connections, logs demonstrating authorisation requests and approvals to carry our privileged functions.

DCC
Defence Cyber Certification

iasme

2418 - Baseline configurations and inventories

Control Requirement

The Applicant shall implement, update, and document system hardening procedures. The Applicant shall also implement, update, and document baseline configuration settings for all information technology products deployed in organisational systems. This shall include the restriction of user actions and of unsupported software and hardware.

Jargon Buster

Some software or hardware is shipped with all services enabled to allow for easier installation and use. This may include accounts with administrator privileges using default usernames and passwords.

2418.1 - (MOD 000505) - (L1-L3)

Has the organisation established baseline configurations for all organisational systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we create a baseline configuration for any system when it is first onboarded.
Expected Evidence: Register of baselines and policy/process of how they are determined for all organisational systems.

2418.2 - (MOD 000472) - (L1-L3)

Does the organisation incorporate system hardening procedures into its system baselines?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Hardening is included in our baselines.
Expected Evidence: Example of baseline or policy/process showing how hardening is applied.

2418.3 - (MOD 000506) - (L1-L3)

Do the organisation's baseline configurations include restrictions on the following?

Available answers (choose all that apply):

- ☐ User actions
- ☐ Use of unsupported software and hardware
- ☐ None of the above

Example: Both, our baseline configurations include restrictions on user actions as well as the use of unsupported hardware and software.
Expected Evidence: Examples of baseline configuration

2418.4 - (MOD 000507) - (L1-L3)

Are the organisation's baseline configurations:

Available answers (choose all that apply):

- ☐ Documented
- ☐ Implemented
- ☐ Updated when changes are made to the baseline
- ☐ Reviewed at least annually
- ☐ None of the above

Example: All of the above. Our Baseline policy details how configurations are determined, updated, implemented, and reviewed.
Expected Evidence: Policy or process showing the above, showing version history to display configuration reviews/updates.

2419 - Obscure authentication information

<u>Control Requirement</u>

The Applicant shall configure systems to obscure authentication information, for example, passwords to ensure that they are not displayed as cleartext when a user is inputting their credentials.

Jargon Buster

This basic but essential security measure protects users from simple attacks like shoulder surfing, which can lead to the unintentional exposure of credentials in public or shared spaces. Shoulder surfing involves an attacker observing a person as they enter sensitive information, such as passwords or PINs, by watching 'over their shoulder'. As well as shoulder surfing, there is a risk of screen capture either from software (malware) or accidental exposure such as screen sharing on a video call.

2419.1 - (MOD 000228) - (L1-L3)

When users type their login details, are their passwords hidden (e.g., shown as dots or asterisks) instead of being visible as plain text?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, password fields are automatically obscured. This is configured as part of our baseline image used when devices are onboarded.
Expected Evidence: Policy showing requirement for password to be obscured, configuration settings showing this.

2420 - Authentication feedback

Control Requirement

The Applicant shall configure systems to minimise feedback information from failed logons to ensure that the system does not provide any information that would allow unauthorised individuals to compromise authentication mechanisms. e.g. explicitly stating that the password is the incorrect authentication component.

Jargon Buster

Authentication feedback, which you might know as user enumeration, occurs when a system unintentionally confirms that a username exists. This usually occurs when error messages or system responses vary depending on whether the provided username is valid or not. Think about what happens when you log in to a system. You might mistype your password and get a response like "Password entered is incorrect". To an attacker, this confirms that the username is valid. This type of feedback can be exploited by attackers to gather a list of valid usernames, which can then be used in brute force attacks to guess passwords or to target default username-password combinations.

This is a fancy way of saying you'll prevent account enumeration.

2420.1 - (MOD 000508) - (L1-L3)

Does the organisation have controls in place that obscure authentication information?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our applications ensure consistent and generic error messages for invalid account names, passwords, or other user credentials entered during the login and password recovery processes, and a generic message during the account setup process.

Expected Evidence: Your Assessor will expect a screenshot or demonstration showing that the organisation has controls in place to obscure authentication information.

2421 - Network Time Protocol (NTP)

Control Requirement

The Applicant shall implement a Network Time Protocol (NTP) to a recognised authoritative source, to synchronise the clocks of every network device to ensure accurate and consistent timestamps for audit records on associated system logs.

Jargon Buster

Network Time Protocol (NTP) is essential for ensuring accurate and synchronised time across all devices in a network. This precise timekeeping matters in security, as it guarantees event logs have consistent and reliable timestamps. Accurate timestamps are vital for identifying and analysing issues, carrying out audits, and conducting forensic investigations, as they provide a clear and chronological sequence of events, helping to detect and respond to potential threats effectively.

2421.1 - (MOD 000509) - (L1-L3)

Does the organisation synchronise the time across all devices by using the Network Time Protocol (NTP)?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is part of the basic device config
Expected Evidence: Your Assessor will expect a technical demonstration showing the status of the NTP service and evidence verifying that time synchronisation is correctly configured and functioning across devices.

2422 - Physical and logical access restrictions

Control Requirement

The Applicant shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.

Jargon Buster

This control focuses on managing the risks associated with making changes to organisational systems. Changes can significantly affect a system's security and functionality, so it's essential to enforce both physical and logical access restrictions.

- Physical access restrictions relate to protecting the tangible components of a system such as server racks, cabling, and server rooms. For example, only authorised and trained personnel should be allowed to access secure areas or handle physical equipment when making changes, upgrades, or modifications.
- Logical access restrictions deal with controlling digital access to systems and resources. This includes managing user permissions for software, automating workflows to ensure proper oversight, and using abstract layers (e.g. external interfaces) to make changes instead of directly modifying systems.

Beyond access restrictions, organisations should implement a clear change management process to regulate how and when changes are made. For instance, you might use change windows specific timeframes designated for making changes to minimise disruptions and maintain system stability.

2422.1 - (MOD 000510) - (L1-L3)

Does the organisation enforce physical and logical access restrictions for making changes to organisational systems, including upgrades and modifications?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (consider both physical and logical access restrictions in your answer)
Expected Evidence: Your Assessor will require evidence to support each restriction you describe. The easiest way to show this may be demonstrations of previous changes, for instance, records of physical access controls during change windows (e.g., sign-in logs or keycard access reports). Documentation of logical access permissions granted specifically for system changes (e.g., temporary elevated privileges). Change management logs showing who accessed systems and when.
Evidence of monitoring or auditing of access during system changes.

2422.2 - (MOD 000511) - (L1-L3)

Does the organisation ensure that the physical and logical access restrictions for its organisational systems are defined, documented, and approved?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the... defines and documents our approved restrictions
Expected Evidence: Your Assessor will need proof that access restrictions are clearly defined, documented, and formally approved. This evidence will likely be found in a document such as a policy or procedure. Again, focus on restrictions related to change periods, and think about the answer to 2422.1. It may be that the access restrictions used as evidenced there, are already defined, documented, and approved in a way that satisfies this question.

2423 - Trusted source repository

Control Requirement

The Applicant shall identify, register and maintain an inventory of system components using automated tooling for those assets that support business Functions and protect Data in an asset register, and at a minimum, include data location and asset ownership information.

This control focuses on ensuring that the software and firmware you use are obtained from official, trusted sources, thereby reducing the risk of compromise. For example, if you need to install Windows, you might use a verified, known-good version stored on a secure server within your organisation or download it directly from a trusted source, such as Microsoft. You would not want to install a version of Windows from an unknown third-party site as it may contain malware or worse.

Organisations that maintain baseline images for devices (e.g., servers, workstations, network devices, etc.) should have a documented list of software included in these systems. They must also specify trusted sources for obtaining software and firmware, such as official vendors or internal repositories. This process should be governed by clear documentation or policies, and the system component inventory must be kept up to date using automated tools to ensure accuracy and consistency.

2423.1 - (MOD 000512) - (L1-L3)

Does the organisation deploy automated tools to identify, register, and maintain a trusted inventory of its critical system components?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Defender on MS servers maintains a list of software installed and version details. Software asset management tools such as SNOW would provide similar capabilities across other operating systems.
Expected Evidence: Sight of the output of such automated tools.

2423.2 - (MOD 000513) - (L1-L3)

What data is recorded in these inventories?

Available answers (choose all that apply):

- ☐ The location of critical system components
- ☐ Function of the critical components
- ☐ Ownership of the asset
- ☐ Hash values independently verified for each image/software package
- ☐ None of the above

Example: All of the above. The data is gathered automatically and is stored in our software repository along with the software.
Expected Evidence: Policy or process covering how data to be recorded is determined, how data is verified and maintained, hashing process carried out, sample of the inventory logs showing details captured

2426 - Anti-malware capabilities

<u>Control Requirement</u>

The Applicant shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.

Jargon buster

Malware is short for **malicious software,** which is software that is designed to cause harm by disrupting, damaging or gaining access to a computer, without the owner's knowledge. Malware is typically designed to cause extensive damage to data and systems or gain unauthorised access. Viruses, worms, trojan horse, spyware, adware and ransomware are all different types of malware that cause harm in different ways.

Not all devices are capable of running anti-malware, but those that easily can should run an anti-malware solution. As part of the maturity of your organisation, you should check that your anti-malware solution is in place, up to date, and effective.

2426.1 - (MOD 000518) - (L1-L3)

Has the organisation implemented anti-malware capabilities on its systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have X installed on our Windows devices and Y on our Macs. Our internal servers also run a solution.
Expected Evidence: Security policy, build image showing anti-malware solution, software licence, device configuration.

2426.2 - (MOD 000519) - (L1-L3)

Does the organisation ensure that malware signatures and software are updated promptly when new releases are made available?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our solutions are set to update daily (and then perform a scan) and software updated within a week of a new version being available.
Expected Evidence: Security policy, solution configuration, scan schedules, MDM logs showing devices are updated.

2426.3 - (MOD 000520) - (L1-L3)

Does the organisation regularly audit its anti-malware implementations to ensure they are:

Available answers (choose all that apply):

- ☐ Being updated routinely and promptly
- ☐ Functional (e.g. performing real-time scans as well as periodic scans)
- ☐ Under active management
- ☐ Detecting sample malware
- ☐ Reporting detections correctly
- ☐ None of the above

Example: Yes, all of the above. Our MDM and device management software alert us if updates or scans are not taking place. Every month we test the solution is working by using a benign malware sample to check it is detected and reported correctly. If a high threat malware is released, we check our solution can detect it.
Expected Evidence: Logs showing malware detected correctly, reports of audits, incident reports, other testing by external parties.

2427 - Monitor/protect communications at boundaries

<u>Control Requirement</u>

The Applicant shall monitor, control, and protect communications (i.e., information transmitted or received by organisational systems) at the external boundaries except where prohibited by Applicable Law and key internal boundaries of those organisational systems. This includes all staff including all remote workers to carry out their duties.

2427.1 - (MOD 000521) - (L1-L3)

Does the organisation, at its external boundaries and key internal boundaries of organisational systems, do the following?

Available answers (choose all that apply):

- ☐ Control communications
- ☐ Monitor communications
- ☐ Protect communications
- ☐ None of the above

Example: Yes, we control, monitor, and protect communications. Remote workers must VPN into our network where our boundary devices restrict inbound/outbound traffic, monitor for sensitive data and ensure communications are securely encrypted.
Expected Evidence: Network diagrams, remote working policy, Security policy, boundary device configuration.

2428 - Verify/limit access to external system connections

<u>Control Requirement</u>

The Applicant shall control and limit connections to external systems by an allow-list on the network boundary.

2428.1 - (MOD 000246) - (L1-L3)

Does the organisation control and limit connections to external systems using an allow-list at the network boundary?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our boundary devices check connections against an allow list determined by our IT team.
Expected Evidence: Security policy, network diagram, boundary device configuration, example of allow list and policy showing how the list is determined, monitored, updated and reviewed.

2429 - Verify/limit access from external system connections

Control Requirement

The Applicant shall block unauthorised inbound connections by default. Inbound firewall rules are approved and documented by an authorised person and include the business need within the documentation.

2429.1 - (MOD 000522) - (L1-L3)

Does the organisation block all inbound connections from external systems, unless approved in an allow-list?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a very limited allow list for inbound connections. This is managed by our IT team.
Expected Evidence: Network diagram showing inbound connection points, boundary device configuration, allow list.

2429.2 - (MOD 000523) - (L1-L3)

Does the organisation ensure firewall rules are managed, approved, and documented by an authorised and competent person?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Our IT team manage the allow list which is then used to determine our firewall configuration. Any changes to the firewall rules must be approved, documented, and authorised before being added to the firewall.
Expected Evidence: Firewall rule change process, examples of firewall change requests (successful and not successful), firewall configuration showing rules.

DCC
Defence Cyber Certification

iasme

2500 - Resilient networks and systems

Control Requirement

The Applicant shall build resilience against cyber-attack and system failure into their design, implementation, operation and management of systems that support the operation of business Functions and protection of Data.

Jargon Buster

Although this control contains just two yes/no questions, it's important not to underestimate its significance. Resilience is a vast and vital concept that should be woven into the very fabric of your organisation, fortifying it as a whole.

We want you to demonstrate that.

When answering these questions, the control is looking for a few key elements. Let's break down the requirement:

Firstly "build resilience against cyber-attack and system failure". The best way to start understanding the requirement is to focus on the word resilience. Resilience is "the quality of being able to return quickly to a previous good condition after a problem".

Consider the ways in which you have strengthened the systems that support your organisation's operations and protect its data. Beyond prevention, this requirement emphasises resilience and recovery.

This should encompass the entire lifecycle of those systems, from design and implementation to operation and ongoing management. Specifically:

- Design: When you are planning systems.
- Implementation: When you begin acting on those plans.
- Operation: When systems are actively used as part of your organisation's main business functions.
- Management: The ongoing oversight, maintenance, and governance of the systems.

2500.1 - (MOD 000452) - (L0-L3)

Has the organisation assessed the degree to which its systems must be resilient to cyber-attack and system failure?

Jargon Buster

Focus your answer on the steps you took to evaluate how robust and secure your systems would need to be to withstand cyber-attacks.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We conducted a risk assessment and...
Expected Evidence: The evidence will vary according to organisation size and complexity. A micro sized company may only have a brief document showing the risks, whereas a large organisation will have multiple documents (including a risk register) to show the risks. The evidence must be tailored to the company size, service provided, and risks faced. You must show what systems are essential (which may be your scope) and the risks.

2500.2 - (MOD 000453) - (L0-L3)

Has the organisation built resilience into its systems to meet its resilience needs?

Jargon Buster

Focus your answer on the implementation of resilience into your systems.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We have redundant network and endpoints...
Expected Evidence: The evidence should demonstrate tangible, practical actions taken to build resilience into your systems. The evidence should clearly show how these directly address the resilience needs identified in your earlier assessment. Avoid referencing policy documents or high-level plans. Focus instead on the

concrete actions and tools that ensure your systems can withstand and recover from disruptions, for example, implementing automated backups or uninterruptible power supplies.

2501 - Design for resilience

Control Requirement

The Applicant shall design the network and information systems supporting their Functions and protect Data to be resilient to cyber security incidents and system failure. Systems shall be appropriately segregated and resource limitations mitigated.

2501.1 - (MOD 000525) - (L1-L3)

Does the organisation design its network and information systems, which support its Functions and protect Data, to be resilient to identified cyber security incidents and system failures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Our Security policy details how we design and implement our systems to be resilient.
Expected Evidence: Network diagrams, Security policy, DR/BCR plans.

2501.2 - (MOD 000526) - (L1-L3)

Do the organisation's resilient designs consider the appropriate level of segregation between systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is factored into our network planning
Expected Evidence: Network diagrams, Security policy, DR/BCR plans.

2501.3 - (MOD 000527) - (L1-L3)

Do the organisation's resilient designs account for the levels of resources required for systems to operate?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our design allows for suitable resource allocation. Systems are assessed when onboarded and required resources calculated and allocated during this stage.
Expected Evidence: Network diagrams, Security policy, DR/BCR plans.

2502 - Resilience preparation

Control Requirement

The Applicant shall develop recovery plans for all systems that deliver Functions and protect Data.

Jargon Buster

2052 (L1) and 2503 (L2-3)are very similar controls which will demonstrate different levels of maturity or exactness in your approach to resilience and recovery planning. At this lower level, the emphasis is on having plans in place. Testing is not explicitly required at this level, but your response should still demonstrate that you've taken steps to make sure recovery is possible.

2502.1 - (MOD 000528) - (L1)

Does the organisation develop recovery plans for all systems to ensure recovery from cyber-attacks and system failures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a master recovery plan and several playbooks for specific scenarios.
Expected Evidence: Your Assessor would expect to see the documented plans. You may also wish to describe or talk through the processes or measures and explain how recovery would work. This may be linked to the 1200 control family which could trigger the writing of plans.

2504 - Backups

Control Requirement

The Applicant shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include:

- Appropriate encryption technology
- Integrity validation

Jargon Buster

Backups are copies of data and information that are created and stored separately from the original data. They serve as a safeguard to ensure that an organisation can recover its data in the event of accidental deletion, hardware failure, or malicious attacks like ransomware.

Control 2504 outlines the fundamental requirements for maintaining backups of data and information. Backups are a vital component of your ability to respond to and recover from incidents such as data loss, system failures, or cyber-attacks.

2504.1 - (MOD 000531) - (L1)

Does the organisation ensure that accessible and secure backups of data are maintained to support the recovery of its functions and protect data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have established a documented backup strategy that outlines the process for creating, storing, and testing backups to ensure data recovery and protection, and we actively implement on a [frequency] basis.
Expected Evidence: To demonstrate that you are adequately backing up, your Assessor will want to see evidence of your backup strategy and its implementation. This might include a documented backup policy or procedure,

screenshots or logs of recent backups, and evidence of regular testing or verification of the backup and recovery process.

2504.2 - (MOD 000532) - (L1)

Does the organisation secure backups with appropriate encryption technology to prevent unauthorised parties from viewing or tampering with backup data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we secure backups with [encryption method] to prevent unauthorised parties from viewing the data and implement measures such as ... to ensure the data cannot be tampered with.
Expected Evidence: Your Assessor will want to see evidence demonstrating how you are encrypting your backups and protecting them from tampering. This might include documentation of the encryption method used, configuration settings or policies, and evidence of additional measures such as access controls, integrity checks, or the use of tamper-proof storage solutions.

2504.3 - (MOD 000533) - (L1)

Does the organisation perform backup integrity validation to ensure backups are completed without error and are accessible?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our backup integrity check process is... This includes testing the restoration of data and verifying the integrity of backup files.
Expected Evidence: Your Assessor will want to see evidence demonstrating how you validate the integrity of your backups. This might include logs or reports from backup validation tests, documentation of the validation process, records of successful restoration tests, or policies outlining the frequency and methods of integrity checks.

2507 - Deny traffic by default at interfaces

Control Requirement

The Applicant shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.

Jargon Buster

Deny Traffic by Default at Interfaces is about making sure that only approved network connections are allowed through the organisation's firewalls. By default, all traffic is blocked unless explicitly approved. Any exceptions to this rule must be regularly reviewed and removed if no longer needed.

2507.1 - (MOD 000272) - (L1-L3)

Does the organisation ensure that firewalls block all network connectivity paths and services by default, unless explicitly authorised by the appropriate Change Advisory Board (CAB) or equivalent?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes
Expected Evidence: Your Assessor will want to see policy documentation that explains the "deny by default" approach and the process for authorising exceptions through the Change Advisory Board (CAB). They will also expect a screenshot of the firewall settings showing the default "deny all" rule and any explicitly authorised exceptions. Additionally, if a Change Advisory Board (CAB) review has been conducted, they will want to see records of approvals for exceptions, including justification and a review date.

2507.2 - (MOD 000540) - (L1-L3)

Does the organisation ensure that enabled network connectivity paths and services are regularly reviewed and removed if there is no ongoing business need?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we review this every.... And our review process/policy is....
Expected Evidence: Your Assessor will want to see policy documentation outlining the process for reviewing enabled network connectivity paths and services. They may also request logs or reports from recent reviews to confirm that unnecessary paths or services have been identified and removed.

2508 - Separate public and internal subnetworks

<u>Control Requirement</u>

The Applicant shall implement network segmentation for publicly accessible system components to ensure logical and/or physical separation from internal network components.

Jargon Buster:

2508 - Separate Public and Internal Subnetworks is about keeping public-facing systems (like websites or services accessible from the internet) separate from internal systems (like employee databases or internal tools). This separation is achieved through network segmentation, which can be done physically (using separate hardware) or logically (using virtual networks or firewalls). The goal is to prevent unauthorised access to sensitive internal systems if a public-facing system is compromised.

2508.1 - (MOD 000541) - (L1-L3)

Does the organisation ensure that publicly accessible systems and networks are physically and/or logically segregated from internal systems and networks using network segmentation?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have... (Clearly describe the methods used to segment the networks, such as firewalls, VLANs, or separate physical hardware, and explain how these controls prevent unauthorised access to internal networks.)
Expected Evidence: Your Assessor will want to see evidence that publicly accessible systems and networks are segregated from internal systems and networks. This might include:

- *Network Architecture Diagram: A diagram showing the separation between public and internal networks, including details of segmentation methods (e.g., firewalls, VLANs, or separate physical hardware).*

- *Firewall or Router Configuration*: *Screenshots or exports of firewall or router settings demonstrating the rules that enforce segmentation between public and internal networks.*
- *Policy Documentation*: *A documented policy or procedure outlining the organisation's approach to network segmentation and the controls in place to enforce it.*

2509 - Managed email filtering

Control Requirement

The Applicant shall implement appropriate tooling or methods to detect, block and report malicious or spam emails coming into the network. Such tooling or methods may include learning capabilities for more effectively identifying legitimate communications.

Jargon Buster

2509 - Managed Email Filtering is about protecting the organisation from harmful or unwanted emails, such as phishing attempts, malware, or spam. This is done by using tools or methods that can identify and block these emails before they reach employees. Some tools may also have learning capabilities to improve their ability to distinguish between legitimate and harmful emails over time.

2509.1 - (MOD 000276) - (L1-L3)

Does the organisation use tools or methods to detect, block, and report malicious or spam emails attempting to enter the organisation?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use [specific tools or methods]. (Clearly describe the tools or methods in place, such as spam filters, anti-phishing tools, or machine learning-based solutions, and explain how they work to protect the organisation.)
Expected Evidence: Your Assessor will want to see proof that the organisation has implemented effective email filtering tools or methods. This could include screenshots of tool configurations, documented policies, or logs and reports demonstrating recent detections, blocks, or flagged malicious or spam emails.

2510 - Diagnostic programmes

Control Requirement

The Applicant shall check all media containing diagnostic and/or test programs for malicious code prior to use on the organisational network.

Term

A diagnostic programme is a tool or software used to test, troubleshoot, and monitor the performance of a system – similar to the device a mechanic uses check your car for issues. In the context of IT and organisational networks, diagnostic programmes are often used to identify problems, run tests, or perform maintenance on hardware or software systems.

Jargon Buster

'2510 - Diagnostic Programmes' is about making sure that any media (e.g., USB drives, CDs, or external hard drives) containing diagnostic or test programs are scanned for malicious code before being used on the organisation's network. If malicious code is detected, the organisation should follow its incident handling policies and procedures to address the issue and prevent further risks.

2510.1 - (MOD 000542) - (L1-L3)

Does the organisation check all media containing diagnostic and/or test programs for malicious code prior to use?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use [specific tools or methods] to scan all media before use. (Clearly describe the tools or methods in place, such as antivirus software, endpoint protection tools, or sandboxing.)
Expected Evidence: Your Assessor will want to see evidence that the organisation has a process to scan media for malicious code before use and handle incidents if malicious code is detected. This could include documented policies outlining

the scanning requirements and incident response steps, screenshots of antivirus or endpoint protection tool configurations, and logs or reports showing recent scans and their results.

2511 - Maintenance activities

<u>Control Requirement</u>

The Applicant shall ensure that relevant good practice tooling, techniques and mechanisms are authorised or provided to maintenance personnel in order to carry out their duties.

Jargon Buster

2511 Maintenance Activities is about making sure maintenance personnel only use tools, techniques, and mechanisms that are either authorised by the organisation or directly provided to them. This helps maintain control over what is used during maintenance activities, reducing the risk of unauthorised or unsafe tools being introduced into the organisation's systems or networks.

2511.1 - (MOD 000543) - (L1-L3)

Does the organisation ensure the tools, techniques and mechanisms used by maintenance personnel are either authorised or provided by the organisation?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use [specific processes or methods]. (Clearly describe how tools are authorised, such as through an approval process, and explain how the organisation ensures only approved tools are used, such as maintaining an inventory or providing tools directly.)
Expected Evidence: Your Assessor will want to see evidence that the organisation has controls in place to ensure maintenance personnel only use authorised or provided tools, this might be in a documented policy, or in an inventory or list of approved tools and mechanisms.

2512 - MFA for remote maintenance activities

Control Requirement

The Applicant shall require multi-factor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when non-local maintenance is complete.

Jargon Buster:

2512 - MFA for Remote Maintenance Activities ensures that remote maintenance sessions (i.e., when someone connects to a system from outside the organisation's network to perform maintenance) are secure. This is achieved by requiring Multi-Factor Authentication (MFA) to access the system. Once the maintenance is complete, the remote session must be terminated to prevent unauthorised access.

2512.1 - (MOD 000282) - (L1-L3)

Where non-local maintenance sessions are required to resolve an issue, does the organisation ensure Multi-Factor Authentication (MFA) is enabled to verify the identity of the individual before granting access to the system?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use [specific MFA solution]. (Clearly describe the MFA solution in place, such as hardware tokens, authenticator apps, or biometric verification, and explain how it ensures only authorised individuals can access the system.)
Expected Evidence: Your Assessor will want to see evidence that MFA is required for remote maintenance sessions, such as a documented policy outlining the requirement or screenshots showing the MFA configuration for remote access.

2512.2 - (MOD 000544) - (L1-L3)

Once non-local maintenance activity is complete, does the organisation ensure all remote sessions are terminated?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe the process or tools in place to terminate sessions, such as automated session timeouts, manual disconnection procedures, or monitoring by administrators.)
Expected Evidence: Your Assessor will want to see evidence that remote sessions are terminated after maintenance, such as a documented policy outlining the requirement, logs showing recent session terminations, or screenshots of settings for session timeouts or termination procedures.

DCC Defence Cyber Certification

iasme

2513 - Maintenance personnel supervision

Control Requirement

The Applicant shall designate authorised, suitably qualified and experienced personnel to supervise maintenance personnel who do not possess the required physical access authorisations.

Jargon Buster:

2513 - Maintenance Personnel Supervision ensures that maintenance workers who do not have the required physical access permissions are supervised by authorised, qualified, and experienced staff, i.e., they get followed around. This supervision helps maintain security and ensures that unauthorised individuals do not gain access to sensitive areas or systems during maintenance activities.

2513.1 - (MOD 000284) - (L1-L3)

Does the organisation require authorised, qualified, and experienced staff to supervise any maintenance workers who lack the necessary physical access permissions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe the process for assigning supervisors, the qualifications required, and how supervision is carried out to ensure security.)
Expected Evidence: Your Assessor will want to see evidence that supervision is in place for maintenance workers without physical access permissions, for example, a documented policy or procedure outlining the requirement for supervision of maintenance personnel who lack physical access permissions. If you keep supervision records or logs, these will also be accepted.

26XX Family

The 2600 series of controls addresses various aspects of staff awareness, training, and behaviour that support your organisation's security. Each control has a distinct focus, ranging from general training programmes to leadership-driven culture, specific training, risk awareness, acceptable use policies, and practical exercises. Understanding the differences between these controls ensures that each requirement is addressed without overlap.

Key Differences

- 2600 - Staff Awareness and Training (L1-L3): Ensures the existence of a general programme to provide staff with the knowledge, skills, and awareness needed to protect the organisation.
- 2601 - Cyber Security Culture (L2-L3): Focuses on leadership's role in fostering a positive cyber security culture and encouraging secure behaviours.
- 2602 - Cyber Security Training (L2-L3): Specifies the content, frequency, and updates of training, including topics like phishing, advanced threats, and breach response.
- 2603 - Staff Risk Awareness(L1-L3): Ensures managers, administrators, and users are aware of security risks related to their roles and that these risks are reviewed and updated regularly.
- 2604 - Acceptable Use Policy (L1-L3): Requires a formal policy outlining restrictions on activities like social media use, clear desk policies, and handling corporate assets.
- 2605 - Annual Threat-Focused Training Feedback (L2-L3): Focuses on practical exercises aligned with current threats, conducted annually, and assessed with feedback provided to participants and supervisors.

2600 - Staff awareness and training

Control Requirement

The Applicant shall ensure that staff have appropriate awareness, knowledge, and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of business Functions and protection of Data.

Jargon Buster

2600 - Staff Awareness and Training is about ensuring that all employees have the general knowledge, skills, and awareness they need to contribute to the organisation's cyber security. This includes having a programme in place to provide training and awareness activities that help staff understand risks, identify threats, and follow security policies.

2600.1 - (MOD 000545) - (L1-L3)

Does the organisation have a cyber security awareness and training programme that ensures staff possess the appropriate cyber security knowledge, skills, and awareness for their roles?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe the process for delivering the training, the topics covered at a high level, and how the organisation ensures staff complete the training.)
Expected Evidence: Your Assessor will want to see evidence of a cyber security awareness and training programme, such as training records, phishing test results, and documented policies outlining the training process and requirements.

2603 - Staff risk awareness

Control Requirement

The Applicant shall ensure that managers, systems administrators, and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organisational information systems. The Applicant shall review and update these security risks at least every 12 months or when there is significant change within the organisation or threat.

Jargon Buster

2603 - Staff Risk Awareness is about making sure that everyone in your organisation understands the security risks tied to their roles. This includes being aware of relevant policies, standards, and procedures that help mitigate these risks. Regular reviews and updates should be happening to make sure their awareness remains current and aligned with evolving threats or organisational changes.

2603.1 - (MOD 000550) - (L1-L3)

Does the organisation review and update the security risks that system users, administrators and managers should be aware of:

Available answers (Choose all that apply):

- ☐ At least annually
- ☐ When there is significant organisational change
- ☐ When there is significant change to the threat
- ☐ None of the above

Example: We... (For each of your selected answers, clearly explain what actions you're taking and how they are being implemented.)
Expected Evidence: Your Assessor may request documentation of the reviews, such as meeting minutes, risk assessment reports, or updated risk registers. They may also require evidence of follow-up communications to staff, such as emails, training updates, or revised policies.

2603.2 - (MOD 000551) - (L1-L3)

Does the organisation ensure system users, system administrators, and management are made aware of relevant:

Available answers (Choose all that apply):

- ☐ Security risks
- ☐ System security policies
- ☐ System security standards
- ☐ System security procedures
- ☐ None of the above

Example: We... (For each selected answer, explain how you are establishing awareness. For instance, outline the processes or methods used to inform relevant staff about security risks.)
Expected Evidence: Your Assessor may request documentation such as training materials, attendance logs, or internal communications that demonstrate how awareness is maintained. They may also ask for copies of the relevant policies, standards, or procedures, along with evidence that these have been shared with staff (e.g., acknowledgment forms or email distribution records).

2604 - Acceptable Use Policy

Control Requirement

The Applicant's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on:

- Use of social media, social networking sites, and external sites/applications.
- Posting organisational information on public websites.
- Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications.
- Enforce clear desk and clear screen requirements.
- Handling of physical corporate assets outside the office environment.
- Locations for conducting duties.
- Remote activation of collaborative computing devices.
- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Jargon Buster

2604 - Acceptable Use Policy is about making sure employees understand and follow rules for using organisational resources responsibly. This includes restrictions on activities like using social media, handling sensitive information, and working in secure environments. The policy also covers physical and digital security practices, such as clear desk requirements and restrictions on remote activation of devices.

2604.1 - (MOD 000367) - (L1-L3)

Does the organisation have a formal Acceptable Use Policy in place?

Available answers (choose one):

☐ Yes
☐ No

Example: Yes, we have a formal Acceptable Use Policy.
Expected Evidence: A copy of the policy.

2604.2 - (MOD 000552) - (L1-L3)

Does the scope of the organisation's Acceptable Use Policy include appropriate restrictions on:

Available answers (Choose all that apply):

- ☐ Use of social media, social networking sites, and external sites/applications
- ☐ Posting organisational information on public websites
- ☐ Use of organisation-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications
- ☐ Clear desk and clear screen requirements
- ☐ Handling of physical corporate assets outside the office environment
- ☐ Locations for conducting duties
- ☐ Use, including remote activation, of any collaborative computing devices (e.g. remote meeting cameras)
- ☐ None of the above

Example: We... (Identify each selected answer in your policy document.)
Expected Evidence: The reference to the selected answer in your policy document.

2700 - Personnel pre-employment checks

Control Requirement

The Applicant shall, unless prohibited by Applicable Law, perform appropriate background verification checks on Personnel that have access to Data upon hire. The verification checks shall include:

- Verifying credentials
- Employment history
- Qualification checks
- Application or verification of BPSS (Baseline Personnel Security Standard)

Jargon Buster:

This control is about making sure that anyone hired to work with sensitive data has been properly vetted.

2700.1 - (MOD 000554) - (L1-L3)

Does the organisation conduct appropriate pre-employment background checks for staff who will have access to Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we ... (Briefly describe the organisation's overall approach to conducting pre-employment background checks for staff who will have access to Data. Focus on confirming that checks are conducted and that they are appropriate for the roles in question.)
Expected Evidence: Your Assessor will want to see a documented policy or procedure that confirms pre-employment background checks are conducted for staff with access to Data. The Assessor may also request anonymised examples of completed checks or confirmation records to demonstrate that the process is being followed.

2700.2 - (MOD 000297) - (L1-L3)

Which of the following are included within the organisation's pre-employment background checks?

Available answers (Choose all that apply):

- ☐ Verifying credentials
- ☐ Employment history
- ☐ Qualification checks
- ☐ Application or verification of BPSS (Baseline Personnel Security Standard)
- ☐ None of the above

Example: We... (For each selected answer, explain how your organisation covers them in its pre-employment background checks. For example, describe how credentials are verified...)
Expected Evidence: Your Assessor will want to see evidence that each selected element is included in the organisation's pre-employment background checks. This could be in a policy document that outlines the process. The Assessor may also request anonymised confirmation letters or examples of completed checks to confirm that the process is being followed consistently.

2701 - Personnel security vetting

Control Requirement

The Applicant shall define and implement a policy for applying BPSS and National Security Vetting (NSV) checks as appropriate for employees that support Functions and the protection of Data. *(It is recognised that application of NSV is normally only possible once a contract requiring such is in place. Potential suppliers who do not meet this requirement at time of submission must, however, be willing and be able to enforce their staff through appropriate levels of vetting within a timescale agreed with the project delivery team following contract award).

Jargon Buster:

This control is about making sure that employees who support Functions and the protection of Data are appropriately vetted.

- BPSS (Baseline Personnel Security Standard) is the recognised standard for the pre-employment screening of individuals with access to government assets.
- NSV (National Security Vetting) NSV has different levels of clearance, such as Security Check (SC), and Developed Vetting (DV). The level of clearance required depends on the sensitivity of the information or role.
- The decision to require NSV, and the level of clearance needed, is made by the departmental authority responsible for the post which the individual will assume.

While Applicants or Suppliers bidding for contracts do not need to have their staff vetted at the time of submission, they must be ready and able to comply with NSV requirements if they win the contract.

2701.1 - (MOD 000555) - (L1-L3)

Does the organisation have a defined and implemented policy for applying the UK Baseline Personnel Security Standard (BPSS) and National Security Vetting (NSV) checks, as appropriate, for personnel supporting Functions and for the protection of Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Because Applicants may or may not be delivering contracts with vetting requirements, there are two ways to approach this question and meet the control requirements.

***For Organisations Currently Delivering Contracts with Vetting Requirements**: We… (Briefly describe your organisation's policy for applying BPSS and NSV checks. Focus on how these checks are implemented for personnel supporting current contracts with vetting requirements.)*

***For Organisations Without Current Vetting Requirements**: We… (Briefly describe your organisation's readiness to apply BPSS and NSV checks, if required. Think about how the organisation will make sure it can implement these checks within an agreed timescale when mandated by a contract.)*

Expected Evidence: Your Assessor will need proof that your organisation is able to, or is ready to, carry out BPSS and NSV checks. This could include a documented process, agreements with vetting providers, internal policies on enforcing vetting, or anonymised records showing compliance with vetting requirements.

2702 - Joiners, movers and leavers

<u>Control Requirement</u>

The Applicant shall define and implement a joiners, movers and leavers policy to secure organisational hardware, software and systems.

Jargon Buster:

This control is about your process for managing employees as they join, move within, or leave your organisation.

2702.1 - (MOD 000556) - (L1-L3)

Does the organisation have a joiners, movers, and leavers policy in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we set requirements joiners, movers, and leavers in... It was last updated [date]
Expected Evidence: A copy of the policy.

2702.2 - (MOD 000557) - (L1-L3)

Does the organisation have procedures for new joiners to ensure the following?

Available answers (Choose all that apply):

- ☐ Access permissions are assigned based on roles and responsibilities.
- ☐ Appropriate cyber security training is undertaken.
- ☐ Understanding of relevant organisational cyber security policies and procedures is measured.
- ☐ None of the above.

Example: We... (For each selected answer, explain how)
Expected Evidence: A copy of the procedure. Alternately your Assessor may want to see an onboarding checklists or workflows, training records or completion certificates for new joiners.

2702.3 - (MOD 000558) - (L1-L3)

Does the organisation have procedures in place for staff moving roles or departments to ensure the following?

Available answers (Choose all that apply):

- ☐ Access permissions are reviewed.
- ☐ Permissions and data are securely transferred.
- ☐ Cyber security training for new responsibilities or systems is delivered.
- ☐ None of the above.

Example: We… (For each selected answer, explain how)
Expected Evidence: A copy of the procedure. Alternately your Assessor may want to see records of access reviews and updates for staff who have changed roles, training records for role-specific cyber security training specifically looking at staff that have moved.

2702.4 - (MOD 000559) - (L1-L3)

Does the organisation have procedures in place for staff leaving the organisation that promptly:

Available answers (Choose all that apply):

- ☐ Revoke access to systems and data
- ☐ Recover issued physical assets including laptops, device tokens, keys and physical identification passes
- ☐ Change authentication factors known to leavers, including shared credentials and physical door codes
- ☐ None of the above

Example: We… (For each selected answer, describe the process of how… access is revoked, how physical assets are recovered, and how shared credentials or door codes are updated.)
Expected Evidence: A copy of the procedure. Your Assessor may request logs or records showing access revocation for recent leavers, asset recovery checklists or records, documentation of changes to shared credentials or door codes.

2702.5 - (MOD 000560) - (L1-L3)

Does the organisation conduct exit interviews or otherwise communicate data security responsibilities to departing personnel?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: We... (Describe the process for conducting exit interviews or other methods.)
Expected Evidence: Your Assessor may request exit interview templates, records, or communications outlining data security responsibilities for departing personnel, and policies or procedures detailing how these responsibilities are addressed during offboarding.

DCC
Defence Cyber Certification

iasme

2703 – Whistleblowing

Control Requirement

The Applicant shall define and implement training and processes for employees and contractors to identify and report suspicious activities and/or behaviour including violations of information security policies and procedures without fear of recrimination. The Applicant shall define and implement a disciplinary process to act against employees who violate information security policies or procedures.

Jargon Buster

This control is about creating a safe and confidential way for your employees and contractors to report activities or security breaches, while also ensuring the organisation has a clear and fair process to investigate and address policy violations.

2703.1 - (MOD 000628) - (L1-L3)

Does the organisation encourage staff to report suspicious activities or cyber security policy violations by:

Available answers (choose all that apply):

- ☐ Providing processes for staff to report without fear of punishment
- ☐ Providing training on the reporting processes to staff
- ☐ None of the above

Example: Yes, we… (For each of your selected answers, clearly explain what actions you're taking.)
Expected Evidence: Your Assessor could ask you to provide; documentation of the reporting processes, training records for related courses or emails, posters and announcements from awareness campaigns.

2703.2 - (MOD 000561) - (L1-L3)

Does the organisation have a disciplinary process to investigate and take action when personnel are suspected of violating security policies or procedures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the process is covered in... which defines... It was last updated [date]

Expected Evidence: A copy of the process.

2704 - Environmental controls

Control Requirement

The Applicant shall, where appropriate, implement, install, and maintain the following environmental controls supporting Functions and protection of Data:

- Fire suppression systems.
- Temperature and humidity controls within a data centre or server room environment.
- Backup power technology (e.g. uninterruptible power supply, diesel generator, separate grid connection, etc.).

Jargon Buster

This control focuses on the physical safeguards in place to protect critical equipment, such as servers or data storage, from environmental risks like fires, overheating, humidity, or power outages.

Avoid Over-Answering: If your organisation does not require certain controls (e.g., no data centre), clearly state this in your response and provide evidence of the assessment that led to this conclusion.

2704.1 - (MOD 000626) - (L1-L3)

Does the organisation assess its need for environmental controls, including:

Available answers (Choose all that apply):

- ☐ Fire suppression systems
- ☐ Temperature and humidity controls (e.g. within data centre environments)
- ☐ Backup power technologies
- ☐ None of the above

Example: Yes, we… (Clearly describe the methods used to assess the need for each selected environmental control, such as conducting risk assessments, reviewing the physical environment, consulting with experts, or referencing industry standards. Explain how these assessments help determine the necessity of fire suppression systems, temperature and humidity controls, and backup

power technologies.) For 2704.1, only describe the assessment process (e.g., risk assessments or evaluations).
Expected Evidence: Your Assessor may expect; risk assessment reports or documentation showing the evaluation of environmental control needs, meeting minutes or records of discussions about environmental control requirements, policies or procedures outlining how environmental control needs are assessed.

2704.2 - (MOD 000641) - (L1-L3)

Does the organisation implement, install and maintain the environmental controls it has assessed as appropriate?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. For 2704.2, focus on the actual implementation and maintenance of the controls identified as necessary.
Expected Evidence: Your Assessor may request maintenance logs or service records for the environmental controls in place. These may be cross-referenced with your answers to 2704.2 to verify that the evaluation process resulted in the installation of appropriate systems. Photos of the installed systems could also support your response.

Objective C - Detecting cyber security events

The Applicant has capabilities which enable security defences to remain effective and detect cyber security events affecting, or with the potential to affect, Functions and protection of Data.

3100 - Security monitoring

<u>Control Requirement</u>

The Applicant shall monitor the security status of the networks and systems supporting the operation of business Functions and protection of Data in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Jargon Buster

This control focuses on the general monitoring of the security status of networks, systems (and may also include endpoint devices) to detect potential security issues and evaluate the effectiveness of protective measures.

3100.1 - (MOD 000562) - (L1-L3)

Does the organisation monitor the security status of networks and systems that support Functions and protect Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have... (Clearly describe the methods or tools used to monitor the security status of networks and systems, focus on the general security monitoring of networks and systems, and describe the coverage. Explain how these methods provide visibility into the security status of your systems.)

Expected Evidence: The Assessor may request logs or reports from monitoring tools, screenshots of monitoring dashboards, or policies outlining the organisation's approach to security monitoring.

3100.2 - (MOD 000563) - (L1-L3)

Does the organisation use security monitoring to detect potential security issues?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use... (Clearly describe the tools or processes in place to detect potential security issues and explain how these tools or processes help identify and respond to potential threats. Focus on how monitoring is used to detect issues.)
Expected Evidence: The Assessor may expect to see examples of alerts or reports generated by monitoring tools or incident logs showing detected issues.

3100.3 - (MOD 000564) - (L1-L3)

Does the organisation use its security monitoring to track the effectiveness of protective security measures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly explain how monitoring data is used to evaluate the effectiveness of protective security measures.)
Expected Evidence: In house testing reports of implemented security measures, network traffic monitoring showing metrics for failed attacks.

3101 - Monitor security controls

Control Requirement

The Applicant shall establish and document security event monitoring, which at a minimum, covers the following:

- Security events covered.
- Frequency of monitoring.
- Clearly defined roles and responsibilities.
- Escalation matrix.

Jargon Buster

This control requires you to establish, and then document, a structured process for security event monitoring. This should include:

- how you decide which events to monitor,
- how you baseline those events,
- how you manage automated alerting,
- how often you monitor,
- who does the monitoring and
- what to do if an event requires further investigation.
- what are the escalation paths
- who are the recipients of those escalations

It is not enough to have a defined process in place, you must show the process is being followed, defined alerts are being triggered correctly, and appropriate events are being investigated.

3101.1 - (MOD 000565) - (L1-L2)

Does the organisation have documented policies, procedures and controls in place for security event monitoring?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, security event monitoring is covered in our Security Monitoring policy. We have separate processes in place depending upon the type of event detected.
Expected Evidence: A copy of the policies, procedures, or controls.

3101.2 - (MOD 000566) - (L1-L2)

Which of the following are included in the organisation's security event monitoring procedures?

Available answers (Choose all that apply):

- ☐ Security events covered
- ☐ Frequency of monitoring
- ☐ Clearly defined roles and responsibilities
- ☐ Escalation matrix
- ☐ None of the above

Example: Our policies and procedures contain all of the above.
Expected Evidence: A copy of the policies, procedures, or controls.

3101.3 - (MOD 000567) - (L1-L2)

Does the organisation ensure security event monitoring is implemented in accordance with its established procedures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we follow our procedure when updating our monitoring and perform quality checks on samples to verify the procedure has been followed correctly.
Expected Evidence: Examples of security event monitoring showing procedure has been followed, incident response reports confirming security monitoring is implemented and working as expected.

3101.4 - (MOD 000316) - (L1-L2)

Does the organisation generate alerts for potential security events?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the type of events that will generate an alert are detailed in our Security Monitoring policy
Expected Evidence: a screenshot or copy of an alert, Incident Response reports.

3107 - Create, retain and correlate audit logs

Control Requirement

The Applicant shall generate event logs for systems that support the operation of Functions and protection of Data. The following criteria apply:

- Logs are archived for a minimum of 12 months.
- Logs capture (as a minimum) date, time (from a single NTP source), user ID, device accessed, and port used.
- Logs capture key security event types (e.g. critical files accessed, user accounts generated, multiple failed login attempts, logging failures from devices, events related to systems that have an internet connection).
- Access to modify system logs is restricted.
- Logs and security event logs can be made available upon request.
- Store audit records in a repository that is part of a physically different system.
- The Applicant shall ensure that systems logs are reviewed at least weekly to identify system failures, faults, or potential security incidents and corrective actions are taken to resolve or address issues within a reasonable timeframe.
- Review, at least every 6 months the event types selected for logging purposes to ensure these still meet business requirements.
- Capture the operational status of the logging system and alert on any failures which impact the system's operational capacity.

Jargon Buster

3107 covers the technical side of generation, retention, and correlation of logs.

3107.1 - (MOD 000580) - (L1-L3)

Does the organisation have documented policies and procedures in place for the creation, retention and correlation of auditing logs?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our Monitoring policy details the requirements for log generation, retention and correlation.
Expected Evidence: A copy of the policy and procedures, samples of logs/records, evidence of reviews.

3107.2 - (MOD 000581) - (L1-L3)

Does the organisation ensure that event logs are generated for all systems supporting the operation of Functions and the protection of Data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Log generation is configured and checked when a system is first onboarded, we then perform weekly checks to ensure the logs are being generated as per the configuration.
Expected Evidence: Log configuration policy/documentation, samples of system showing current log configurations and samples of generated logs.

DCC
Defence Cyber Certification

iasme

3107.3 - (MOD 000582) - (L1-L3)

Does the organisation ensure that it captures logs for all key security event types, as defined by its policies?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. When a system is onboarded, the logging configuration is determined by our Monitoring policy. We then check the configuration and the logs after a week to ensure the logs are being generated as expected.
Expected Evidence: Samples of logs showing the range of event types captured, reports reviewing captured logs or correspondence around this.

3107.4 - (MOD 000583) - (L1-L3)

Does the organisation review the event types selected for logging at least every 6 months to ensure they meet business requirements?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we review the logging configuration at least every 6 months, or sooner if required.
Expected Evidence: Monitoring policy, log or correspondence showing configuration changes.

3107.5 - (MOD 000584) - (L1-L3)

Does the organisation ensure that system event logs capture:

Available answers (choose all that apply):

- ☐ Event date/time from Network Time Protocol (NTP) source
- ☐ User ID
- ☐ Devices accessed
- ☐ Network ports used
- ☐ None of the above

Example: Yes, we capture all of the above.
Expected Evidence: Monitoring policy or log configuration process documentation, sample of logs or configuration.

3107.6 - (MOD 000585) - (L1-L3)

Does the organisation ensure that logs are available on request for analysis?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the logs are available as detailed in our monitoring policy.
Expected Evidence: Policy or process showing log retention, sample of logs in storage.

3107.7 - (MOD 000586) - (L1-L3)

Does the organisation ensure system logs are reviewed at least weekly to identify failures, faults and potential security issues?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we perform weekly checks to ensure the logs are being generated as per the configuration.

Expected Evidence: Monitoring policy, log review process, reports of log reviews/audits.

3107.8 - (MOD 000587) - (L1-L3)

Does the organisation ensure that logs are archived for at least 12 months?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our Monitoring policy states logs have to be kept for 18months.
Expected Evidence: Policy showing log retention requirements, samples of retained logs.

3107.9 - (MOD 000588) - (L1-L3)

Does the organisation ensure that access to modify system logs is restricted to prevent tampering?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, all our SOC analysts and Incident Response team have access to read the logs but permission to modify the logs is restricted to key senior SOC roles.
Expected Evidence: Log read/write/modify permissions/configuration defined by role, role/job description.

3107.10 - (MOD 000589) - (L1-L3)

Does the organisation store audit records in a separate physical system from the audited systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our audit records are stored on a separate physical system from the logs.
Expected Evidence: Network diagram or configuration records showing separation of storage.

3107.11 - (MOD 000590) - (L1-L3)

Does the organisation monitor the operational status of logging/auditing systems and alert on any failures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we monitor for a "heartbeat" from the systems and have alerts set for any failures. If no new logs are created within a determined time frame, an alert is triggered.
Expected Evidence: Monitoring policy or process document to determine the operational status of systems, sample of logs/alerts demonstrating whether systems are operational or not operational.

3107.12 - (MOD 000591) - (L1-L3)

Does the organisation have an effective audit reduction and report generation capability?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we baseline when onboarding a system and update the baseline for verified behaviours or changes. We have streamlined tooling to aid report generation by automatically collating logs and information.
Expected Evidence: Monitoring policy, process or other documentation supporting the answer and showing how this is done.

3108 - Audit reduction and report generation

Control Requirement

The Applicant shall provide and implement an appropriate audit record reduction and report generation capability that:

- Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
- does not alter the original content or time ordering of audit records.

Jargon Buster

3108 focuses on processing logs for actionable reporting, where possible, reducing the work involved and ensuring there is the capability for on-demand audit record review, analysis and reporting. It is similar to some elements of 3107 (create, retain and correlate audit logs) but is more focussed on how you make it easier and efficient to use the logs when investigating incidents that have already happened.

3108.1 - (MOD 000592) - (L1-L3)

Does this capability support the organisation's requirements for on-demand audit review, analysis and reporting?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our tooling allows us to automatically correlate logs and then produce on-demand record review, analysis and reporting.
Expected Evidence: Evidence of tooling and process implementation, tooling configuration showing correlation and ability to create reports on demand.

3108.2 - (MOD 000593) - (L1-L3)

Does use of this capability preserve the original content and time-ordering of audit records?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use tooling with "read-only" access to logs in order to ensure no data is modified and the data is preserved.
Expected Evidence: Evidence of tooling and process implementation, tooling configuration and proof data is not modified.

3109 - Integration of records with incident management

Control Requirement

The Applicant shall integrate audit record review, triage, analysis, and reporting processes with organisational governance and incident management structure.

Jargon Buster

This control looks at how the logging and incident response integrates with other parts of your organisation. It is not enough for Incident Response to detect and stop an attack. Who else needs to know about it to remediate the damage or prevent future incidents? For example, your SOC may receive an alert and respond to it by engaging incident response, who then coordinates with management, audit and governance teams. This control requires evidence of effective and timely coordination beyond the initial alert.

3109.1 - (MOD 000594) - (L1-L3)

Does the organisation integrate audit record review, triage, analysis, and reporting with its governance and incident management structures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our Incident Response policy contains flowcharts of how to respond to different types of incidents, which teams to coordinate with and their structures.
Expected Evidence: Incident Response policy, flowcharts or diagrams showing the integration of audit record review, triage, analysis and reporting processes with governance and incident management structures. Evidence may also include minutes of meetings and reports showing coordination between different teams.

3200 - Proactive security event discovery

<u>Control Requirement</u>

The Applicant shall detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of business Functions and protection of Data even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).

Jargon Buster

Signature based detection relies on predefined patterns or "signatures" of known threats. This method is effective once a signature is known, but it is ineffective against threats without a signature in the detection method. As a result, it cannot detect zero-day threats or polymorphic malware, which alter their code to evade detection.

3200.1 - (MOD 000629) - (L1-L3)

Does the organisation have procedures in place to proactively identify malicious activities within its networks and systems, including those that evade signature-based prevention and detection solutions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have EDR and SIEM, backed up with threat hunting activities and canary tokens.
Expected Evidence: Security Monitoring or detection policy and procedures detailing how the organisation detects such activities or threats. Examples of incident reports and threat hunting findings.

3201 - System abnormalities for attack detection

<u>Control Requirement</u>

The Applicant shall define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify. The Applicant shall take appropriate action upon identifying this behaviour.

3201.1 - (MOD 000597) - (L1-L3)

Does the organisation define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we define normal and abnormal behaviour for each system on our internal knowledge base, this is then used to create examples fed into our SIEM where it is used to create alerts for abnormal behaviour.
Expected Evidence: Process or policy document detailing how normal or abnormal system behaviour is defined, how examples are created and how they are then used for detection. Examples should show the full path from start to finish, including testing of the detection method.

3203 - Use indicators of compromise from alerts

Control Requirement

The Applicant shall monitor system security alerts and advisories and act in response using agreed and managed indicators of compromise.

3203.1 - (MOD 000599) - (L1-L3)

Does the organisation proactively search for known indicators of compromise across its systems and technologies to support detection efforts?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we automatically update our SIEM/EDR with the latest indicators as soon as they are available. We also perform threat hunting to strengthen our detection methods.
Expected Evidence: Policy or process document detailing how your organisation searches for known indicators of compromise, reports from threat hunting activities and incident reports.

3203.2 - (MOD 000600) - (L1-L3)

Does the organisation monitor alerts and advisories from trusted sources to identify new indicators of compromise?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a threat intelligence feed from a trusted source which we ingest to update our indicators of compromise for our SIEM/EDR. We also monitor advisories from our software vendors.
Expected Evidence: Sample of the feeds and how they are ingested and acted upon. These may include threat intelligence feeds, vendor and industry advisories or other sources.

3204 - Presence of unauthorised system components

Control Requirement

The Applicant shall implement proportionate measures to:

- Detect the presence of unauthorised hardware, software, and firmware components within the system using tooling.
- Take the following actions when unauthorised components are detected: disable network access by such components; isolate the components; notify systems administrators and/or security operations teams.

3204.1 - (MOD 000601) - (L1-L3)

Does the organisation use tools to detect unauthorised hardware, software, and firmware components in its systems?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have dedicated tooling that scans for unauthorised hardware, software and firmware components.
Expected Evidence: Policy detailing what the tooling should be looking for, an example of the tooling configuration showing how it is configured.

3204.2 - (MOD 000602) - (L1-L3)

Does the organisation require action to be taken when unauthorised components are detected, including, where appropriate and proportionate:

Available answers (choose all that apply):

- ☐ Disabling network access by such components
- ☐ Isolating such components
- ☐ Notifying systems administrators and/or security operations teams
- ☐ None of the above

Example: Yes, all of the above.

Expected Evidence: Policy detailing actions required when unauthorised components are detected and who should be notified. Configuration of the tooling showing currently configured actions and notification settings.

Objective D - Minimising the impact of cyber security incidents

The Applicant shall ensure capabilities exist to minimise the adverse impact of a cyber security incident on the operation of Functions and protection of Data, including the restoration of Functions and Data.

4100 - Response and recovery planning

<u>Control Requirement</u>

The Applicant shall implement well-defined and tested incident management processes that aim to ensure continuity of business Functions and protection of Data in the event of system or service failure. Mitigation activities are designed and where possible, automated to contain or limit the impact of a compromise.

4100.1 - (MOD 000603) - (L1-L3)

Does the organisation have clearly defined policies and processes in place for cyber security incident management?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have an incident management policy which covers defining and testing the policy and processes required for handling incidents and recovery.
Expected Evidence: Policy or other supporting evidence.

4100.2 - (MOD 000604) - (L1-L3)

Has the organisation tested its cyber security incident management processes?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we perform table-top exercises to test the policy and processes are suitable, we perform technical tests where possible.
Expected Evidence: Policy or other documentation such as reports showing how the cyber security incident management is tested.

4104 - Incident handling capability

<u>Control Requirement</u>

The Applicant shall establish an operational incident handling capability for organisational information systems that is consistently applied across the organisation and includes:

- Adequate preparation, detection, forensic analysis, containment, recovery, and user response activities.
- Tracking, documenting, and reporting incidents to appropriate organisational officials and/or authorities.
- Sufficient rigour, intensity and scope.

4104.1 - (MOD 000612) - (L1-L3)

Does the organisation have an incident handling capability that is robust and comprehensive enough to meet its incident management policy and incident response plans?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We regularly review the incident response plan and policy to ensure they remain comprehensive and robust.
Expected Evidence: Incident response policy and plan or other documentation outlining the requirements and processes.

4104.2 - (MOD 000613) - (L1-L3)

Does the organisation's incident handling capability include:

Available answers (choose all that apply):

- ☐ Preparation for incidents
- ☐ Detection of incidents
- ☐ Forensic analysis of incidents
- ☐ Containment of incidents
- ☐ Recovery from incidents
- ☐ Communication with users
- ☐ Tracking incidents
- ☐ Documenting incidents
- ☐ Reporting incidents to organisational officials and/or authorities
- ☐ None of the above

Example: Our Incident response plan covers all of the above.
Expected Evidence: Documentation such as incident response plan or policy showing the required capabilities. Incident reports can also show the elements and capabilities covered.

DCC
Defence Cyber Certification

iasme

4106 - Attempted unauthorised connections from staff

Control Requirement

The Applicant shall audit the identity of internal users associated with denied communications.

Jargon Buster

If a user has an outgoing connection detected and blocked, you should investigate what it was and who it was. Denied and unauthorised internal communications should also be investigated. These activities may need investigating further if the activity may be suspicious or a sign of compromise.

4106.1 - (MOD 000356) - (L1-L3)

Does the organisation audit the identities of internal users linked to denied communications?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we log all unauthorised/denied communication attempts, both internal and outgoing.
Expected Evidence: Policy or process documents detailing the logging requirements, thresholds for alerting, and any evidence of checks being carried out, such as incident reports.

4200 - Lessons learned

Control Requirement

The Applicant shall, when an incident occurs, incorporate root cause analysis and lessons learned information from incident response activities into incident response procedures, training and testing. The Applicant shall implement the resulting improvements immediately or, at minimum, within 30 days of the completion of the root cause analysis.

Jargon Buster

When things go wrong, do you investigate what happened and incorporate this into how you will respond in the future? If the improvements are small or simple, then they should be implemented quickly - if not immediately - once the analysis is complete. If the improvement requires a large/complex project, such as onboarding a new vendor to replace hardware - which may take months - a temporary fix must be implemented within 30 days (or sooner) after the analysis is completed. Once the changes have been made to policies and processes, they must be followed.

4200.1 - (MOD 000616) - (L1-L3)

Does the organisation have procedures in place to conduct root cause analysis following incidents?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, after each incident, we investigate and determine the root cause.
Expected Evidence: Incident response policy and process documentation

4200.2 - (MOD 000617) - (L1-L3)

Does the organisation incorporate and implement lessons learned from incidents into updated incident response procedures, training and testing?

This question is asking if you update your processes and procedures, training and testing, and other relevant documentation to include changes made due to the lessons learnt.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, after each incident we perform a debrief/washup and update our procedures/training/testing with the lessons learnt.
Expected Evidence: Incident response report, documents that were updated following the incident (e.g. policies/training/testing).