Levels 0-3 Applicant Guide

Version 2.2

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.

History of key revisions

Date issued:	Description:
2 September 2025	Version 1.3
6 May 2026	Version 2.0 Combined levels 0-3
24 June 2026	Version 2.1 Refined scoring system section
October 2026	Version 2.2 Adding additional guidance as per DCPP IWG request

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.

Level 2/3 hybrid (145 controls)
The Level 3 assessment will be conducted using a hybrid approach incorporating both Level 2 and Level 3 controls. Applicants will be required to provide responses and evidence for all Level 2 and Level 3 controls, amounting to a total of 145 controls.

This 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 the Level 3 pass mark is not achieved.

If the pass mark for Level 2 is not met, then the Applicant has failed the assessment for Levels 2 and 3.

Applicants may consider a hybrid approach for other levels, such as Level 1/2; this must be discussed and agreed with the assessing Certification Body.

DCC Scoring Guide

The DCC scoring system evaluates compliance, with each level having specific requirements for passing. Controls are scored as follows:

- **0 points:** Not met (None of the control questions meet the baseline)
- **1 point:** Partially met (Some control questions meet the baseline, while others do not)
- **2 points:** Fully met (All control questions meet the baseline)

The total score for each objective is calculated based on the number of controls within that objective. To pass, you must meet the specific requirements outlined for each level.

Level 0

- To pass Level 0, you must meet 100% of the controls.
- This means all controls must be fully met, with no partial compliance allowed.

Level 1

To pass Level 1, two conditions must be met:

- You must achieve at least 80% of the total points available per objective.
- Each control within the objective must be at least partially met (i.e., no control can score 0 points).

For example, if an objective contained 10 controls, the maximum possible score would be 20 points (10 controls × 2 points each). To pass, you would need 16 points and there would be various ways to achieve this:

- 10 controls fully met: 20 points (10 × 2)

- 9 controls fully met and 1 control partially met: 19 points (9 × 2) + (1 × 1)
- 8 controls fully met and 2 controls partially met: 18 points (8 × 2) + (2 × 1)
- 7 controls fully met and 3 controls partially met: 17 points (7 × 2) + (3 × 1)
- 6 controls fully met and 4 controls partially met: 16 points (6 × 2) + (4 × 1)

Any combination scoring less than 16 points or including a control that is Not Met (0 points) will result in this objective being failed. For example:

- 5 controls fully met and 5 controls partially met: 15 points (5 × 2) + (5 × 1) - Fail (does not meet the 80% threshold).
- 7 controls fully met, 2 controls partially met, and 1 control not met: 16 points (7 × 2) + (2 × 1) + (1 × 0) - Fail (a control is ""Not Met"").

Level 2

To pass Level 2, the same rules as Level 1 apply:

- You must achieve at least 80% of the total points available per objective.
- Each control within the objective must be at least partially met (i.e., no control can score 0 points).

Compliance is assessed per objective, and both conditions must be satisfied to achieve a passing score.

Level 3

- To pass Level 3, you must meet 100% of the controls.
- This means all controls must be fully met, with no partial compliance allowed."

Assessor Judgement

When reviewing a control, Applicants must consider what the control is aiming to achieve and apply it in the context of modern threats. The threats faced by one Applicant may not carry the same level of risk for another, so proportionate responses may differ.

There is no blanket rule that says, "If you do X, you are safe from Y." For this reason, Assessors will review what you do, how you do it, and whether your approach is proportionate and adequate for your organisation.

Following this logic, there may be occasions where a control includes multiple questions or requirements (e.g. five), but an organisation can only answer some of them positively (e.g. three out of five) because the way it operates means that some questions do not apply. In these circumstances, we do not expect Applicants to increase their attack surface or reduce their overall security simply to answer more questions. For example, an Applicant using passkeys should not roll back to less secure password settings to meet a requirement written for passwords, nor should an Applicant introduce a VPN where there is no business need.

Assessors will use their professional judgement to determine how well an Applicant is meeting a control and may adjust the control score to reflect this. They can add or remove a point where appropriate.

Example 1:
If an Applicant can only demonstrate compliance with three out of five requirements, the Assessor may still judge that the control is effectively met overall. In this case, the control score may be changed from **partially met** to **fully met.**

Example 2:
Conversely, if the Assessor determines that the Applicant's approach to meeting a control is not adequate, a point may be deducted. For example, if a control has two questions: (1) whether a policy exists and (2) whether the policy is followed, and the Assessor sees no evidence that the policy is

implemented or followed in practice, they may deduct a point and mark the control as **not met** rather than **partially met**.

Due to the nature of the defence industry, there is a wide range of Applicants who will operate in differing ways but may still meet the same controls. Applicants should treat the control questions as a way to draw out evidence of how they meet a control, rather than as a prescriptive checklist of requirements that must be met in a specific way.

If an Applicant follows NCSC and NPSA guidance, they may exceed the expectations implied by the control questions, but the questions may not fully capture that in a simple "yes/no" format. For this reason, it is essential that the Assessor understands how you meet the control so that the scoring accurately reflects your approach. Individual controls include additional guidance on this flexibility in assessment.

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

As an Applicant, you are permitted to seek third party assistance to help you achieve certification, provided it aligns with the following guidelines.

Role of Certification Bodies

Certification Bodies (CBs) are there to support you through the certification process while maintaining the credibility and fairness of the scheme. They are required to:

- Act impartially and provide unbiased guidance.
- Promote your organisation's resilience without creating dependency or exploiting the process.
- Maintain transparency and fairness in their advisory and assessment roles.
- Ensure you fully understand what is expected of you, as outlined in the Applicant Guide.
- Mark all of your answers against the applicable controls and scheme guidance.

How Certification Bodies Can Support You

Certification Bodies can provide valuable assistance to help you navigate the certification process. They are permitted to:

- Explain the DCC scheme and its certification levels.
- Clarify the controls and provide guidance on how to meet them.
- Help you understand the questions and identify the key components needed for a complete and accurate response.
- Describe the evidence required to demonstrate that a control has been met.
- Verify the scope of your assessment.
- Provide blank template documents for your use.
- Offer support to help you meet Cyber Essentials or Cyber Essentials Plus, as allowed under the current Cyber Essentials scheme.
- Facilitate Clarification Rounds (as defined later in the process).

- Help you achieve Cyber Essentials/Cyber Essentials Plus

What Certification Bodies Cannot Do

To ensure fairness and maintain the credibility of the scheme, there are limits to the support Certification Bodies can provide. They are not allowed to:

- Implement policies, controls, or technical changes on your behalf.
- Answer questions for you or dictate your responses.
- Complete documentation or prepare answers or evidence that they will later assess.

Additional Support

If you require more extensive help, such as consultation or implementation services beyond the advice a Certification Body can provide, you are encouraged to engage a separate technology provider. This provider does not need to be a DCC Certification Body it can be any provider of your choice. However, selecting a provider familiar with the DCC scheme may be beneficial to streamline the process.

By understanding the role of Certification Bodies and the support they can offer, you can make the most of the resources available to you while ensuring your organisation meets the requirements of the DCC scheme.

It is strongly recommended that you consult the guidance provided by the National Cyber Security Centre (NCSC) and the National Protective Security Authority (NPSA) to adopt best practices for increasing your organisation's security and resilience.

Conflict of Interest Statement

While Certification Bodies are required to remain impartial and avoid conflicts of interest, there may be instances where they have assisted Applicants in achieving Cyber Essentials certification. This is permissible, as Applicants may need to update their Cyber Essentials scope in preparation for the DCC assessment. It is important to note that Cyber Essentials and

Cyber Essentials Plus are separate schemes, each with their own moderation processes.

To ensure transparency, all assessments from Level 1 and above require a Conflict of Interest statement. This statement must be signed by both the Certification Body and the Applicant at an early stage to confirm both parties are aware of any potential conflicts that could impact the Certification Body's ability to proceed with the assessment.

It is important for both the Applicant and Certification Body (CB) to identify and disclose any affiliations or ties to organisations that may have performed work for the Applicant, as these relationships could impact the CB's ability to remain impartial. E.g. If CB1 and CB2 are subsidiaries of the same parent company, any work conducted by CB1 may prevent CB2 from carrying out the assessment. Similarly, if an Assessor works for both CB1 and CB2 and has previously supported the Applicant with remediation work under CB1, this would also constitute a potential conflict of interest when conducting the assessment under CB2.

The statement must clearly state:

- Whether the Assessor or Certification Body has a current or previous relationship with the Applicant, along with details of the services provided or the nature of the relationship.
- Whether a conflict of interest exists. If so, it must specify the conflict, the controls it affects, and the steps taken to ensure the assessment remains impartial.
- If you, the Applicant, have used the same Certification Body to achieve Cyber Essentials (or Plus) then this must be included in the statement along with what work was undertaken.

Example Conflict of Interest Statement

We, CB XYZ Ltd have performed the last three years of Cyber Essentials assessments for customer ACME Ltd. For this client, we have carried out:

1. Cyber Essentials gap analysis and suggested remediations (MFA solutions)
2. Supplied blank templates for Cyber Essentials

For DCC we expect to:

1. Perform limited gap analysis as part of Theoretical Scoring (high level advice only, no implementation carried out or other services/products sold)
2. Supply blank template documents
3. Provide a detailed report after the assessment detailing the assessment results and detailed remediation advice for any failed controls

Our CE work will affect the following controls:

1. 0001 (Cyber Essentials) – The CE assessment and support was carried out by person A who is a member of the DCC assessment team. The DCC Lead Assessor will check and validate their work
2. 2201 (Access control - multi-factor authentication)/2305 (Remote Access - VPN (Virtual Private Network))/2512 (Email authentication methods) – Our CE gap analysis highlighted a lack of MFA; we suggested multiple solutions from which the customer chose and implemented one. Our DCC Lead Assessor will review these controls to ensure impartiality and correct implementation

Signed by CB's Lead Assessor:

Signed by Applicant:

If there are any doubts as to whether the conflict may be too great and prevent an impartial assessment this should be checked with the Certification Body (and/or IASME) before starting the assessment.

Failure to declare a conflict of interest may result in the whole assessment being failed.

Determine Scope

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

Applicant's Responsibilities

The Applicant is responsible for:

- Determining the scope of the assessment
- Accurately documenting and recording the scope
- Completing the Assessment Submission Record
- Assisting the Assessor
- Document storage and retention
- Maintaining certification

Determining, Documenting, and Recording the Scope

As the Applicant, you must have a comprehensive understanding of your organisation, its operations, and the critical elements required for it to function. Therefore, it is solely your responsibility to ensure that the DCC scope is both adequate and accurate. Before determining what falls within or outside the scope of the DCC, you **must** consult the DCC Scoping Guide. You are required to produce clear and detailed documentation that defines what is included and excluded from the DCC scope. This documentation should include business organisation diagrams, network diagrams, and lists of systems. It must also explicitly indicate which systems fall within scope of the CE/CE+ certification.

The Assessor, as well as other relevant parties, must be able to fully understand the scope based solely on the documentation and scoping attestation provided by you, the Applicant. The Assessor may challenge the scope but ultimately the Applicant is responsible for the whole submission.

If the Assessor determines that the scope, documentation/recording is inadequate, the entire assessment will be failed.

Completing the Assessment Submission Record and Providing Accompanying Evidence

The Assessment Submission Record (ASR) is the document where the Applicant provides responses to the questions contained within this Applicant Guide. It is not sufficient to simply restate the answers provided in the guide; additional context must be included to explain in detail how each control is met. When answering the questions, you must consider the associated control and provide sufficient detail, as this additional context can be the determining factor in whether a control is deemed to be met.

The Applicant must answer all questions for the level they wish to attain. In addition to your responses, you must provide evidence to demonstrate that your organisation is actively implementing the measures described. The evidence must be relevant, appropriate and directly aligned with the question and the control it supports. Evidence can range from a simple screenshot to a comprehensive policy document. However, it is essential to clearly indicate the specific section or part of the evidence that supports your answer. For example, if a 100-page policy document is used as evidence for multiple questions/controls, you must explicitly reference the exact sections relevant to each answer. If the Assessor cannot easily identify the specific part of the evidence that supports your response, they may request clarification or mark the question as failed.

For further guidance on completing the ASR and providing evidence, please refer to the information on the front cover of the ASR or speak to your Certification Body.

If your assessment is chosen for a quality review or moderation, and the guidance has not been followed, e.g. the moderator deems that the ASR does not contain adequate details then the moderation may result in a failure and loss of certification.

Assisting the Assessor

Before the assessment begins, you should discuss your organisation's readiness for the assessment with the Assessor. This discussion should include any factors that may hinder the assessment process to ensure a smooth and efficient review. While the Assessor can help clarify the scheme and its requirements, their primary role is to evaluate the answers and evidence you provide to determine whether the controls are met. It is essential the Applicant understands the assessment process as detailed in the Process Guide. The assessing Certification Body (CB) can also help clarify the process to Applicants.

During the Theoretical Scoring phase, the Assessor will review your answers and supporting evidence. At this stage, the Assessor may request additional clarification if needed - this process is referred to as a Clarification Round. If the Assessor determines that the Applicant is at risk of failing the Practical Scoring phase, they may allow the Applicant time to address the issues, remediate, and resubmit an updated ASR at a later stage. However, for this to occur, the Applicant and Assessor must agree in advance on the number and extent of Clarification Rounds. For more information, please see the Process Guide or consult with your CB.

The Applicant should openly communicate any factors that could possibly hinder the assessment process. These factors may include, but are not limited to, site inductions for on-site visits, staff availability, or the need for security clearances. It is important to address these issues in advance to avoid delays and complications. If the Assessor is unable to complete the assessment due to time constraints, any remaining controls will be marked as not met. It is in the Applicant's best interest to ensure that sufficient time is allocated for the assessment and that the Assessor is provided with the necessary support throughout the process.

If the Assessor requests the Applicant to capture a screenshot for evidentiary purposes, this must be done promptly and saved in accordance with the Assessor's instructions.

In order to assist the scoring and evidence collection, the Assessor may request that all video calls and screenshares are recorded on the

Applicant's systems. This must be complied with. Access to the ASR, accompanying evidence, and any recordings must be granted to the Assessor and/or IASME as required for up to three and a half years after completion of the assessment.

Hashing

Why You Are Asked to Provide a Hash Value

As part of the submission process, the Applicant and Assessor are required to provide a hash value for the final compressed assessment folder. This hash value acts as a unique "digital fingerprint" of the assessment, ensuring that the submitted work can later be verified for integrity and authenticity against the certificate. It safeguards against disputes by providing a reliable way to confirm that the assessment matches the original file submitted.

What Is a Hash Value?

A hash value is a unique string of characters generated by applying a mathematical algorithm (called a hash function) to the contents of a file. It acts as a digital fingerprint for the file, uniquely identifying its contents. Even the smallest change to the file will result in a different hash value.

In the below example a minor alteration was made to ExampleFile.zip resulting in a completely different hash value.

Original - 0590d282304d54e30d840c6a37f41de7da29855f ExampleFile.zip
Tampered - 5517e1523e4bb0908717032637080bf034bd3e39 ExampleFile.zip

Key Features of a Hash Value:

1. Uniqueness: Each file has a unique hash value. If two files have the same hash value, they are identical.
2. Fixed Length: Regardless of the size of the file, the hash value is always a fixed length, depending on the algorithm used (e.g. SHA-256 produces a 256-bit hash).
3. Irreversibility: A hash value is a one-way function, meaning it is impossible to reverse engineer the original files from the hash value. This ensures that none of the assessment data is at risk of being leaked or exposed when you share the hash value.

Why Irreversibility Matters:

When IASME takes the hash value, you are not sharing the actual contents of your assessment file. Instead, you are sharing a secure, irreversible representation of the file. This means that even if someone gains access to the hash value, they cannot use it to reconstruct or access your original file. This makes hash values a safe and secure way to verify the integrity of your submission without exposing your data.

How to Produce the Hash

The final hash value MUST meet the following guidelines:

1. File Format: The hash must be generated for the single compressed archive (e.g., .zip, .tar.gz, or .7z) that contains all required files - including evidence, ASR, marking sheet, scoping documentation, and conflict of interest documents.
2. Hash Algorithm: Use SHA-256 to generate the hash value.
3. Verification: The hash must be verified prior to submission, meaning it should be generated and then independently checked by the assessor to confirm repeatability.

IASME does not recommend the use of online hash generators and remember DO NOT DELETE THE COMPRESSED FILE!

Document Storage and Retention

The Applicant is responsible for securely hosting all documentation related to the assessment. Access to these documents must be provided to third

parties such as IASME, when required. Once the Applicant has submitted their documentation, no updates or amendments to the scoping attestation, ASR, or supporting artefacts are permitted unless explicitly requested by the Assessor. Any unauthorised changes may result in the assessment being marked as an overall fail.

After the assessment is complete, the Applicant must retain all related documents for a minimum of three and a half years without making any amendments. During this retention period, access to the documents must still be granted to third parties (e.g. MOD or IASME, for moderation purposes) upon request.

Should the Applicant wish to use the completed ASR as a starting point for a future assessment, be it renewal or uplift, we recommend making a copy of the original ASR and editing the copy. The original must stay intact and unchanged.

Maintaining Certification

Although the DCC assessment is a point in time evaluation, the certification is valid for three years, during which the Applicant has ongoing responsibilities. Failure to meet these responsibilities may result in the loss of certification.

The Key requirements are as follows:

- The Applicant is responsible for ensuring continued compliance with the controls throughout the certification period.
- The Applicant must maintain CE for all levels, and where applicable, CE+ certification for their DCC level (Levels 2-3).
- While minor operational changes are expected and do not need to be reported, significant changes must be discussed with the Certification Body (CB) to determine if recertification is necessary.
- An annual attestation must be completed to confirm that the scope of the certification has not changed significantly.

Defence Cyber Certification Questions

Updates to Controls and Guidance

DefStan 05-138 Issue 4 was finalised in May 2024. The controls within it are built around enduring security principles such as knowing what you have, controlling access, protecting information, monitoring for abnormal activity, and responding effectively to incidents. These principles remain relevant even as technologies and threats evolve.

Some controls include examples of technologies, standards, or implementation approaches that were common at the time the standard was written. Applicants should not treat these examples as the requirement itself. Instead, you should focus on the intent of the control and demonstrate how you achieve that intent using methods that are appropriate for your organisation and proportionate to the risks you face.

DCC guidance will continue to be updated to reflect changes in technology and current good practice, and to clarify how Applicants can meet the control intent using modern approaches. Applicants who follow relevant NCSC (National Cyber Security Centre) and NPSA (National Protective Security Authority) guidance will often meet or exceed the baseline expectation set by the DefStan controls. Where an Applicant's approach achieves the control intent using current good practice, Assessors should take that into account when scoring.

Applicants should also be aware that technologies not explicitly referenced in the controls may still need to be addressed where relevant. For example, while there may not be controls that mention specific emerging technologies, the risks they introduce (such as data exposure, insecure access paths, misconfiguration, or supply chain dependency) are typically covered by broader controls across the framework. Applicants are not expected to plan for every theoretical future threat; however, they are expected to understand their organisation's current risks and to apply controls appropriately.

DefStan 05-138 Issue 4 controls are unlikely to be revised frequently. Over time, minor differences may emerge between the wording of specific examples and the latest best practice. Where there is a mismatch between an example in a control and current industry/NCSC/NPSA guidance, Applicants should follow current good practice and be prepared to explain how their approach meets the intent of the control. If there is any doubt, Applicants should discuss their approach with the Certification Body and Assessor at an early stage.

Cyber security is not a one-off activity, and good practice does not stop once certification is achieved. Although Applicants may not be reassessed during the three-year validity period of a certificate, Applicants must continue to maintain and improve their security posture so that they continue to meet both the controls and their intent throughout the certification period. IASME may moderate assessments, and the MoD retains the right to audit suppliers.

MoD policy, guidance, and standards may change over time. Where changes affect DCC expectations, IASME will update DCC guidance accordingly.

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 000431) - (L0-L3)

0001.1	MOD 000431	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.

0000 – Example Control

Terms
Terms sections are used to define or explain specific words, phrases, or concepts used in the control. When you see something labelled under "Terms," it is meant to clarify the terminology that will appear later, making sure the Applicant understands the meaning and context of key ideas.

Control Requirement
The control requirement section states the controls requirement directly from the Defence Standard 05-138 issue 4.

Jargon Buster
Jargon Buster sections are used to make the control requirements clearer and easier to understand. It aims to break down complex or technical language into straightforward, plain English, ensuring the meaning is accessible without oversimplifying or changing the intent.

0000.1 - (MOD 000000) - (L0-L3)

Example question, is coffee provided for security staff?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: The example answer section will display the beginning of a response to help guide you toward the expected type of answer, without fully providing it. I.e. Yes, as part of our resilience strategy our security team is kept well caffeinated. Alternate controls are applied in compliance with BS 6008:1980... Examples given are just that, examples. Other ways to achieve the control may exist and are by no means an exhaustive list.

Some examples given will be relevant to a particular size or complexity of organisation. Where this is the case the guide will stipulate small, medium, large or complex.

Expected Evidence: The expected evidence section lists suggestions for the types of evidence you can use to demonstrate that you are addressing the question and meeting the overall control. I.e. A coffee supply inventory or caffeine consumption statistics.

---LIVE QUESTIONS NOW FOLLOW---

000X Family - Cyber Essentials scheme

The 000X Family of controls focuses on the UK Government backed Cyber Essentials certification scheme, which is designed to protect organisations from the most common internet-based cyber security threats. This family of controls is about making sure that your organisation meets these baseline technical requirements by achieving and maintaining certifications for the duration of their Defence Cyber Certification.

- 0001 – Cyber Essentials (L0-L3): Focuses on achieving and maintaining the Cyber Essentials certification, which covers internet connected devices and networks. This certification is based on a self-assessment process.
- 0002 – Cyber Essentials Plus (L2-L3): at level 2 you are expected to build on the Cyber Essentials certification by achieving Cyber Essentials Plus. This requires a technical audit of IT systems to verify the implementation of the required controls.

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. Whilst DCC contains Cyber Essentials (and Cyber Essentials Plus) as a control, it must be noted that they are different schemes and as such do not completely align. It is also important to note that the Cyber Essentials scheme will receive updates, and these must be adhered to for the duration of the DCC certification.

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 required 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 its 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.

0002 - Cyber Essentials Plus

Terms

Cyber Essentials Plus is based on the same technical requirements as Cyber Essentials and starts with the Cyber Essentials verified assessment questionnaire. The difference is that Cyber Essentials Plus also includes a technical audit of your IT systems to verify that the controls are in place.

Control Requirement

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

The Cyber Essentials plus scope of the applicant organisation must align with the proposed scope of this Defence Cyber Certification assessment.

Jargon Buster

The Applicant must have Cyber Essentials Plus certification that applies to every part of the contract and must keep this certification for as long as the contract lasts.

0002.1 - (MOD 000012) - (L2-L3)

Does the organisation hold Cyber Essentials Plus (CE+) certification that covers the required scope for this activity?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our CE+ scope has been checked by our Certification Body and aligns with our DCC scope.

Expected Evidence: Your certificate number, CE+ report/questionnaire

0002.2 - (MOD 000365) - (L2-L3)

Does the organisation commit to maintaining CE+ certification for the duration of any contract relating to this activity?
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.

11XX Family - Governance

Effective security of network and information systems should be driven by organisational management and corresponding policies and practices. There should be clear governance structures in place with well-defined lines of responsibility and accountability for the security of network and information systems.

Senior management should clearly articulate unacceptable impacts to the business (often called risk appetite), which should take into account the organisation's role in the operation of essential functions, so decision makers at all levels can make informed decisions about risk without constantly referring decisions up the governance chain.

There should be an individual who holds overall responsibility and is accountable for security. This individual is empowered and accountable for decisions regarding how essential functions are protected. For small organisations, the governance structure can be very simple.

Your organisation's approach to security governance needs to be an appropriate fit for your organisation. Good security governance is integrated with your business's usual decision making structures and processes.

Decisions about risk can be made at all levels of your organisation when delegated effectively to people with the right security, business and technical knowledge, skills and experience. Clear lines of communication are also necessary. [1]

[1] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a1-governance

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.

1101 - Board Direction

Control Requirement

The Applicant shall have effective organisational security management led at board level and articulated clearly in corresponding policies.

Jargon Buster

Essentially, this control examines whether leadership is actively involved in ensuring the organisation's security and whether clear, written guidelines are in place to support this.

1101.1 - (MOD 000368) - (L2-L3)

Does the organisation have an individual or team that is responsible for leading organisational security management at the board level or equivalent?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our CISO is responsible for leading this.

Expected Evidence: The contact details for the individual or team.

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?

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.

1103 - Decision Making

Control Requirement

The Applicant shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all data are considered in the context of other organisational risks.

Jargon Buster

This control checks if your organisation has a senior staff member in charge of security who can assign decision-making to the right experts.

1103.1 - (MOD 000018) - (L2-L3)

Are senior-level leaders accountable for network and information system security, with appropriate delegation of decision-making authority?

The question wants to know if your organisation has managers in charge of keeping your networks and systems safe. It also wants to know if these leaders can assign decision-making responsibilities to others/subordinates.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, … is accountable for this, they sometimes delegate decision making to…

Expected Evidence: The details of the individual/position and job description or responsibilities, meeting minutes showing the individual is making decisions or appropriate delegating the decision making authority.

12XX Family – Risk Management

There is no single blueprint for cyber security and therefore organisations need to take steps to determine security risks that could affect the operation of essential functions and take measures to appropriately manage those risks.

Threats can come from many sources, both from within and external to an organisation. A good understanding of the threat landscape and the vulnerabilities that may be exploited is essential to effectively identify and manage risks. Such information may come from sources including NCSC, information exchanges relevant to the organisation's sector, and reputable government, commercial, and open sources, all of which can inform the organisation's own risk assessment process. Organisations may contribute to the understanding of threats and vulnerabilities in their sector by participating in relevant information exchanges and liaising with authorities as appropriate.

There should be a systematic process in place to ensure that identified risks are managed and the organisation has confidence mitigations are working effectively. Confidence can be gained through, for example, product assurance, monitoring, vulnerability testing, auditing and supply chain security.

NCSC provide risk management guidance to help choose an approach that's right for your organisation. Organisations responsible for essential functions are likely to benefit from a combination of a system based approach, which looks at the interactions between components of the function, and a component driven analysis, which considers the threats, vulnerabilities, and impacts relevant to particular critical components. Your organisation should choose a method or framework for managing risk that fits with the organisation's business and technology needs.

Whichever approach you choose, the scope of your programme must include all systems relevant to the operation of essential functions. Simply following the minimum requirements of a standard or applying blanket controls across the organisation is unlikely to adequately manage risks to

critical systems. Where industrial control and automation systems are in scope of the essential function, you should keep in mind that controls suitable for managing risks on the corporate IT network may be inappropriate or damaging in an operational technology environment. These systems will likely require a more tailored approach, and some frameworks and standards address specific concerns relating to such systems. [2]

[2] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a2-risk-management

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

This control primarily focuses on cyber security risks rather than broader business risks, such as cash flow, fire or flooding. Cyber security risks can evolve rapidly and have potentially catastrophic effects on a business. Therefore, it is crucial to understand how the organisation prioritises and manages specific technical/business security risks. These risks must be identified through various sources such as news reports, threat intelligence, staff expertise, vulnerability scans, or knowledge of external factors (e.g. a key vendor is likely to go out of business). Such risks may require ongoing monitoring or remediation. Unlike control 1202, which addresses broader business risks, this control specifically examines the organisation's awareness of new and existing risks to its network and information systems, as well as its ability to manage those risks effectively. For example, a server initially deemed unimportant, may become critical to the business due to increased usage, requiring higher prioritisation for support and remediation. Similarly, the organisation should track technologies that are nearing end of life or will no longer be supported after a certain date, ensuring it understands the impact on its operations. It is essential that the organisation can remediate these risks without compromising its security or operational effectiveness.

Businesses often maintain a risk register or business plan as part of their overall risk management strategy. Security risks can fluctuate due to both external and internal factors, making it essential for organisations to effectively assess, understand and address these risks. Remediation efforts should be carefully tracked and monitored to ensure that corrective actions are fully implemented, and risks are mitigated in a timely manner

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.

1201 - Risk Management Process

Control Requirement

The Applicant shall have effective internal processes for managing risks (to the security of network and information systems that protect all data) and communicating associated activities and solutions.

1201.1 - (MOD 000021) - (L2-L3)

Does the organisation maintain a central cyber risk register with logged risks, assigned owners, and regular reviews?

A risk register is a list where you keep track of potential problems that could affect your organisation, along with details on how likely they are to happen and what impact they could have. It is a means to help you manage and reduce risks.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is reviewed every quarter.

Expected Evidence: The last two risk registers.

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. These risks may include cyber risks but should also include non-cyber risks such as fire and flood.

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. Network diagrams must be included in the scoping statement.

Control Requirement

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)

1204 Threat intelligence capabilities

Terms

Threat intelligence is the process of gathering information about potential cyber-attacks and the criminals behind them. It helps businesses understand and prepare for these threats by providing insights into how the attacks work, what they target, and how to spot them.

Threat hunting is the proactive search for cyber threats that are lurking undetected in a network.

Advisories are official recommendations or alerts issued by organisations about potential or existing security threats.

Control Requirements

The supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response, and recovery activities.

Threat intelligence will often feed into multiple controls, such as 4105, that may lead to updating policies/processes in order to reflect the changes in the threat landscape and risks faced by the organisation.

1204.1 - (MOD 000026) - (L3)

Does the organisation have established threat intelligence capabilities?
Threat intelligence capabilities can include:

- A dedicated team, shared function or managed service that manages the threat intelligence feeds.
- Analysis of latest information to determine network impacts.
- Ensure any remedial action is recorded (this could include vulnerability remediation, Security Information and Event Management (SIEM) data enrichment or publishing educational materials).

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is part of our SOC team.

Expected Evidence: Job descriptions or team roles/responsibilities.

1205 - Assurance

Control Requirement

The Applicant shall gain validation for the effectiveness of the security of their technology, people, and processes in support of its functions and which store and/or process data.

Jargon Buster

This control checks whether you've tested your security measures against well-known standards and certifications. This may also include active testing methods such as penetration testing or social engineering.

1205.1 - (MOD 000417) - (L2-L3)

Does the Applicant have an assurance process in place to validate the effectiveness of security measures across its functions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have annual vulnerability scans, and we hold several ISO certifications.

Expected Evidence: We would expect to see the certificates and reports to support your answer.

1205.2 - (MOD 000418) - (L2-L3)

Are assurance activities regularly conducted to assess the security of systems that store and process data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we conduct... [activities] on a... [time frame] basis
Expected Evidence: The easiest way to demonstrate this would be to show the outputs of your activities.

1205.3 - (MOD 000419) - (L2-L3)

Are findings from assurance activities used to enhance the security posture of people, processes and technology?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, for example, following our last... [activity] we implemented...

Expected Evidence: We would expect you to be able to point to something that you have implemented as a direct result of an assurance activity.

1205.4 - (MOD 000420) - (L2-L3)

Does the organisation have a mechanism to address gaps identified during assurance activities?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, once a gap has been identified we determine if it can be dealt with by a single department or if a team from multiple departments are required to work of fixing the gap.

Expected Evidence: Reports on gaps found and how they were mitigated, minutes from meetings, evidence showing gaps have been remediated and how.

1205.5 - (MOD 000421) - (L2-L3)

Has the organisation obtained independent validation reports or certifications to demonstrate the security effectiveness of its technology, people, and processes?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we've achieved...

Expected Evidence: The certifications and reports demonstrating the effectiveness of your security.

1206 - Internal Controls Assurance

Control Requirement

The Applicant shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed time frames.

Jargon Buster

This control wants to know how you are reviewing your security measures to make sure they're still working well. This is about reviews against a standard or compliance framework and **not** business as usual security dashboards, log checking or periodic policy changes etc.

1206.1 - (MOD 000371) - (L2-L3)

How often does your organisation internally assess the effectiveness of its information security controls?

Available answers (choose one):

- ☐ At least once a year
- ☐ Ad-hoc
- ☐ No assessment carried out

Example: We do this annually as detailed in…

Expected Evidence: Documentation or evidence showing the frequency of assessments.

1206.2 - (MOD 000372) - (L2-L3)

Which of the following activities are included in the assessment?
Please select all that apply to your organisation:

- ☐ Assessing control effectiveness against information security policies
- ☐ Identifying deficiencies
- ☐ Reporting assessment results to leadership
- ☐ None of the above

Example: Our Risk Management policy details the assessment requirements and distribution of results. (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: A document to show the scope and methodology of review or a findings report showing the methodology and distribution.

13XX Family – Asset Management

In order to manage security risks to the network and information systems supporting essential functions, organisations require a clear understanding of what needs to be protected including service dependencies. This understanding might include physical assets, software, data, essential staff and utilities. These should all be clearly identified and recorded so that it is possible to understand what things are important to the delivery of the essential function and why.

Whichever risk management method your organisation uses, asset management will play a key role as you cannot effectively manage risks without understanding what assets are part of the essential function. Your asset management regime should consider all relevant assets, and dependencies between them. Dependencies may be identified between assets under your organisation's control (including IT and OT domains), elements of the supply chain (including power), and key staff who are critical to operations. Assets in an operational technology environment may need a more tailored approach than the corporate IT assets.

For asset management to be effective, up to date knowledge of your assets must be maintained throughout their lifecycle.[3]

There are two controls in the 13xx family. Put simply, they are:
1300 (L1-3) – Do you manage your assets in a reasonable way?
1301 (L2-3) – Do you use some form of automation to keep your asset inventory accurate and up to date?

[3] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a3-asset-management

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

This control is about conducting basic asset management. Your organisation needs to understand what it relies on to deliver its Functions and protect Data.

You should be able to demonstrate an effective way to identify and record key assets, and to keep that information current as things change. Assets can include the people you work with (e.g. staff, contractors, students, and volunteers), the systems and technology you rely on (hardware, software, and services you own, lease, or use), and supporting infrastructure (such as power or cooling).

Organisations can define and select the system components they include in their inventory on a proportionate basis. Many organisations find it helpful to start with what matters most; the components that store, process, transmit, or control access to organisational data, or that are critical to delivering functions. From there, consider which components would cause real impact if they failed or were compromised, and scale the level of detail based on the risk.

For example, most organisations should inventory items such as servers, laptops, user accounts, key cloud services, and network/security devices. You would not normally need to inventory low risk peripherals such as headphones, keyboards or mice unless they were genuinely critical to your operation.

Further guidance for asset management can be found on the NCSC site https://www.ncsc.gov.uk/guidance/asset-management.

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.

1301 - Automated asset inventory management

Control Requirement

The Applicant shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support functions and protect data.

Jargon Buster

Control 1301 applies to Levels 2 and 3 and builds on the asset management expectations set out in Control 1300. From Level 2 onwards, your asset inventory is expected to be more current, and some form of automation is expected to achieve this.

Automation does not necessarily require an expensive enterprise system. For many organisations, appropriate automation can be achieved using commonly available tools. A combination of automated and manual steps is acceptable, provided it reliably produces an accurate, up-to-date inventory. Cost-effective approaches include using existing tools and data sources to collect asset information and using those outputs to keep the asset register current.

For example, you might export lists from the systems you already use to manage devices, accounts, and cloud services; use built in reporting from security or endpoint tools to capture device and software details; and run regular automated checks (discovery scans) to identify new or changed assets where appropriate. You can then bring these outputs together in a single asset register (which may be a dedicated tool or a spreadsheet) and use manual updates for items that cannot be discovered automatically. The solution must be appropriate for the Applicant's organisation. The more dynamic and complex the Applicant's environment, the more automated and scalable the process needs to be.

For further advice, see NCSC guidance on asset management and maintaining asset inventories (https://www.ncsc.gov.uk/guidance/asset-management).

1301.1 - (MOD 000374) - (L2-L3)

Does the organisation use automated tools for asset discovery and management to maintain an up-to-date asset inventory?
You should use an automated tool to find and record all assets on your network, even those in remote or off-site locations. This tool should gather details such as:

- The type of device,
- The IP and MAC addresses,
- The Operating system,
- The Software versions,
- The Last user login,
- And other important information.

Scans should be performed regularly to maintain an up-to-date inventory.
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have implemented [tool] which [explain what it does]

Expected Evidence: A screenshot of the tool followed up with a live demonstration.

14XX Family – Supplier Management

If an organisation relies on third parties (such as outsourced or cloud-based technology services) it remains accountable for the protection of any essential function. This means that there should be confidence that all relevant security requirements are met regardless of whether the owning organisation or a third party operates the function.

For many organisations, it may make good sense to use third party technologies and services. Where these are used, it is important that contractual agreements provide provisions for the protection of things upon which the essential function depends.

Organisations responsible for essential functions need to ensure that when third party suppliers are used, all relevant security requirements are met. This means that a number of specific supply chain related security considerations should be addressed where relevant to the provision of the essential function. NPSA and NCSC provide guidance on understanding and managing supply chain risks.[4]

[4] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a4-supply-chain

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.

Third party suppliers are often necessary for providing specialised services. However, attackers may target suppliers to gain access to your systems or data. You should therefore consider the risk of a supplier being compromised and how you will reduce and mitigate that risk.

Supply chain attacks are a common cause of security breaches and data loss. Even if you maintain strong security controls internally, your overall risk may still be affected by the security posture of your suppliers. Attackers understand this and may target suppliers as a route into your organisation.

The NCSC[5] and NPSA[6] have produced guidance to help organisations establish effective control and oversight of their supply chain. Where possible, Applicants should be familiar with the Software Security Code of Practice[7], which will give greater assurance that third-party software and services are resilient to cyber attack. Applicants may use alternative assurance approaches, but the method chosen must be suitable and effective for the Applicant, including risk tiering where appropriate.

---

[5] https://www.ncsc.gov.uk/collection/supply-chain-security, https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

[6] https://www.npsa.gov.uk/security-best-practices/supply-chain-guidance

[7] https://www.ncsc.gov.uk/section/software-security-code-of-practice/overview

Note: This control does not assess DEFCON 658 obligations flowed down to subcontractors (which may be a subset of your suppliers). Instead, it assesses how you manage the risks associated with all suppliers.

You are not obliged to direct your own suppliers to get DCC as some may not be part of the MOD supply chain. But you may wish to request your suppliers achieve a certification that provides a suitable level of assurance (e.g. CE, DCC or a suitable ISO standard).

Applicants wishing to know more about DEFCON 658 and contractual flow down should contact the MOD.

Where an Applicant wishes to certify under DCC and has a parent organisation that provides services to the Applicant (child organisation), these services may be assessed as if provided by an external organisation. This allows the Applicant's DCC scope to exclude the parent organisation for the assessment, but the services provided by the parent to the Applicant will be assessed. This results in the DCC scope being smaller but places greater emphasis on the supplier checks as the Applicant is more reliant on externally provided services.

Where a control is met by the third-party service or product, this must still be evidenced to show how the control is met.

The Applicant is expected to perform due diligence on all externally provided services, whether they are from the parent or a genuine external service provider. The level of due diligence should be appropriate and proportionate to the products and services being consumed and the risks faced by the Applicant and the supplier. This may involve, but is not limited to, measures such as:

- legal/contractual assurance
- Service Level Agreements (SLAs)
- a supplier holding Cyber Essentials or other suitable certification
- a supplier conforming to the Software Security Code of Practice
- independent testing of services/products (e.g. penetration testing or security audits)

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: For each answer your assessor will expect corresponding evidence.

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.

15XX Family - Physical management

Physical security predates cybersecurity and already plays a role in most people's lives, as such many organisations have will already have a mature approach to physical security.

Your organisation's approach to physical security needs to be an appropriate fit for your organisation. Good security governance is integrated with your business's usual decision making structures and processes, this should be reflected in the measures your organisation takes to secure it's premises. Like cybersecurity, physical security should be layered in order to increase it's effectiveness.

Management of physical security underpins cybersecurity. Many cybersecurity controls may be undermined, or even completely bypassed by being able to physically access a device.

The 15XX controls are concerned with controlling physical access to sites or premises where work is carried out. These controls do not apply to occasions when you are working on a third-party site such as a customer site as this would be covered by other controls (e.g. 2311 and 2312 amongst others) but they do apply to sites where you have some control over the security arrangements, such as working from home (WFH), a rented space or your own premises.

Applicants should understand the locations they work from and what steps they can take to minimise any risks whilst working from that location. Almost all Applicants are expected to have some form of physical premises where they perform their work.

For example, a sole trader may only work from their home office and customer sites, this would make the home office their physical premises. It is not expected that a residential property has security guards, swipe cards or photographic ID cards, however there should still be an adequate level of mechanisms in place to prevent unauthorised access. The way the control is applied will be taken into account by the Assessor to ensure it is adequately met given the circumstances.

The NPSA (https://www.npsa.gov.uk/) have multiple guidance documents on physical access controls. You should decide which are appropriate for your organisation for the risks you face, and implement proportionate and appropriate measures.

The Applicant is not expected to attempt to control physical access to a third-party data centre; this would fall under the Supplier Chain controls 1400 and 1401.

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

The physical access control is about ensuring only authorised people enter the places where your data is stored or processed. The simple test is: could someone get in who isn't supposed to?

Physical access is a real cyber security concern. An attacker with in-person access to your devices and equipment can bypass many of the online protections you have in place. Effective physical controls reduce this risk by preventing, deterring, or detecting unauthorised access in the first place.

The examples listed in the control are not a checklist. They are prompts to help you consider what is already in place and what may be needed. What is adequate depends on your organisation and context, and your Assessor will take your circumstances into account. If your organisation is FSC accredited, this can be used as evidence of how you meet the control. However, if FSC does not apply across your whole organisation, you must demonstrate how non-FSC areas meet the control.

Applicants must implement this control in a proportionate way, taking account of risk, the type of work being carried out, and the types of location involved. The measures must be sufficient to prevent unauthorised access, and what is appropriate will vary by role and site. For example, a sole trader working from home is unlikely to use smart card access systems, whereas an Applicant with dedicated premises would be expected to implement stronger measures.

For further guidance on physical security, home working and third-party sites, refer to NCSC and NPSA guidance.

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 focuses on recording who has access to your physical premises and how you manage the devices used to grant access, such as keys or access cards. In cases where an Applicant has no control over the premises where they work, this must be clearly explained and demonstrated to the Assessors satisfaction. The approach to meeting this control will vary depending upon the Applicant's circumstances. For example, a sole trader working from a home office will require a different inventory solution compared to a large company operating from a dedicated office space.

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

Does the organisation perform any Functions or process Data from its own physical premises?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We have a rented office space for our CEO and sales, all other staff work from home. Office and home workers must follow our policies regarding document and device usage and storage.

Expected Evidence: Policy detailing security in the workplace, acceptable use policy.

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 any location where significant damage could occur if a malicious actor were to gain access. Whether it involves critical equipment or essential functions, any compromise in these areas could have a detrimental impact on the organisation's ability to operate effectively.

The definition of a sensitive area will vary depending on the nature of the organisation but typically includes locations where confidential work is conducted or where sensitive information is stored and/or processed. Other examples may include workshops housing Operational Technology (OT), product storage areas, server rooms, and even HVAC/plant rooms. Unlike public spaces such a reception area or lobby, access to sensitive areas must be restricted to authorised individuals with official permission.

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.

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. For example, a company may allow all staff to access a kitchen area, but not all staff should have access to the server room, or other areas where key systems are housed.

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.

Jargon Buster

This control exists so you know who is on your premises and can account for them at any given time.

Recording entry and exit times helps you establish who was where if an incident occurs. ID badges make it easier to see to see who should be on site and who should not. Escorting visitors allows you to supervise where they go and what they do. Collecting badges at the end of a visit reduces the risk of them being reused to gain access later.

How you meet these requirements will depend on your environment. For example, a sole trader may only need a simple visitors' book, while a larger organisation may need a more formal system. Similarly, in a micro organisation where everyone on site is already known to all staff members, a formal ID badge may not be necessary. The purpose of an ID badge is identification, if people can already be reliably identified, the intent of the control is still met.

If you have no visitors, or you do not have office premises, you must discuss this with your Assessor.

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 visitors 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.

21XX Family – Planning for Resilience

The organisation's approach to securing network and information systems that support essential functions should be defined in a set of comprehensive security policies with associated processes and procedures. It is essential that these policies, processes and procedures are more than just a paper exercise and steps must be taken to ensure that they are well described, communicated and effectively implemented.

Policies, processes and procedures should be written with the intended recipient community in mind. For example, the message or direction communicated to IT staff will be different from that communicated to senior managers. There should be mechanisms in place to validate the implementation and effectiveness of the policies, processes and procedures where these are relied upon for the security of the essential function. Such mechanisms should also support an organisational ability to enforce compliance when necessary.

To be effective, cyber security and resilience policies, processes and procedures need to be realistic, i.e. based on a clear understanding of the way people act and make decisions in the workplace, particularly in relation to security. If they are developed without this understanding there is a significant risk that service protection policies, processes and procedures will be routinely circumvented as people use work-arounds and shortcuts to achieve their work objectives. [8]

[8] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b1-service-protection-policies-processes-and-procedures

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.

2101 - Policy and process implementation

Control Requirement

The Applicant shall implement security policies and processes that demonstrate the continuing security benefits to functions and data.

2101.1 - (MOD 000385) - (L2-L3)

Does the organisation update its cyber security and cyber resilience policies and processes in response to:

Available answers (choose all that apply):

- ☐ Relevant organisational changes
- ☐ Evolving cyber security and resilience risks
- ☐ Changes in applicable laws and regulations
- ☐ Changes in contractual obligations
- ☐ None of the above

Example: Yes, our last policies and processes review was completed on [insert date], with the next scheduled review set for [insert date]. During the review, we updated... (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: The Assessor will be looking at the history of revisions for your policies and will want to see how often they are updated or whether there is any indication that the above answers prompted a review or update.

22XX Family – Identity and Access

It is important that the organisation is clear about who (or what in the case of automated functions) has authorisation to interact with the network and information systems supporting an essential function in any way or access associated sensitive data. Access rights granted should be carefully controlled, especially where those rights provide an ability to materially affect the operation of the essential function. Access rights granted should be periodically reviewed and technically removed when no longer required such as when an individual changes role or leaves the organisation.

Users, devices and systems should be appropriately verified, authenticated and authorised before access to data or services is granted. Verification of a user's identity (they are who they say they are) is a prerequisite for issuing credentials, authentication and access management. For highly privileged access it might be appropriate to include approaches such as multi-factor or hardware authentication.

Unauthorised individuals should be prevented from accessing data or services at all points within the system. This includes system users without the appropriate permissions, unauthorised individuals attempting to interact with any online service or individuals with unauthorised access to user devices (for example if a user device were lost or stolen).

NCSC provide guidance that sets out security fundamentals that operators should consider in designing and managing identity and access management systems.

In addition to technical security, organisations should protect physical access to networks and information systems supporting the essential function, to prevent unauthorised access, tampering or data deletion. Some organisations may already have physical security measures in place

to comply with non-cyber regulatory frameworks. See NCSC guidance[9] on Control Access and also NPSA guidance[10]

[9] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b2-identity-and-access-control

[10] https://www.npsa.gov.uk/security-best-practices/passport-good-security/control-access

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.

2201 - Access control - Multi-Factor Authentication

Term

Multi-factor authentication (MFA) means using more than one type of check to confirm a person's identity before granting access. These checks usually come from different categories, such as something you know (e.g. a password or PIN), something you have (e.g. a smart card, token, or security key), and something you are (e.g. a fingerprint or other biometric).

Control Requirement

The Applicant shall implement Multi-Factor Authentication mechanisms to control access to critical or sensitive systems, and organisational operations. Factors can include:

- Something you know (e.g. password/Personal Identification Number (PIN))
- Something you have (e.g., cryptographic identification device, token)
- Something you are (e.g., biometric).

Jargon Buster

The intent of this control is to protect access to critical systems and operations by ensuring access does not rely on a single check. Multi-factor authentication (MFA) strengthens access control by requiring more than one check before access is granted.

MFA can be implemented in different ways depending on the system and how access is managed. Typical methods include:

- a password plus an authenticator app
- a password plus a hardware token or security key
- a smart card plus a PIN
- or a biometric check plus another factor

Where no person is signing in (e.g. non-interactive or machine-to-machine access), you should refer to the wider 22xx family of controls to show how access is verified, authenticated, and authorised.

If people access in-scope OT or safety-critical systems, this control still applies. In some environment, standard interactive MFA may not be practical or may introduce operational or safety risks. Where this is the case, you should explain why and demonstrate how access is still protected so that it does not rely on a single check.

If standard interactive MFA is not practical or safe, your explanation should explain why and show how access is still protected. This may include:

- why MFA cannot be applied in the usual way
- who can access the system or operation
- how access is controlled in practice
- what checks, restrictions, or safeguards are used to protect access
- how those measures reduce the risk of unauthorised access
- any limits on where, when, or how access is permitted (e.g. limits on location, device, network, or role)

Example 1: standard user access
A member of staff accesses a sensitive business system using a password and an authenticator app. This uses more than one check before access is granted and is a typical way of meeting this control.

Example 2: OT or safety-critical environment
A person accesses an in-scope OT or safety-critical system in an environment where standard interactive MFA would create operational or safety issues. In this case, the Applicant should explain why standard MFA is not suitable and show how access is protected by other controls, such as tightly controlled physical and/or network access, so that access does not rely on a single check.

2201.1 - (MOD 000387) - (L2-L3)

Does the organisation implement multi-factor authentication (MFA) to control access to:
Available answers (choose all that apply):

- ☐ All systems deemed critical
- ☐ All systems processing sensitive information
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will expect a screenshot of the security settings for each system where MFA has been implemented.

2201.2 - (MOD 000388) - (L2-L3)

For these systems, is MFA mandatory before access is granted:
Available answers (choose all that apply):

- ☐ From remote locations
- ☐ To privileged/administrator functions
- ☐ To sensitive information
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: our Assessor will expect to review screenshots or policy documents demonstrating the implementation of MFA for the selected options.

2202 - Device management

Control Requirement

The Applicant shall fully understand and trust the devices that are used to access the network, and information systems that support functions and process data.

Jargon Buster

This control is about making sure that only known, vetted, and authorised devices can access your network and systems. It sits within a wider family of controls focused on identity and access, but this is the control that focuses specifically on devices.

The control asks you to "fully understand and trust" the devices on your network. In practice, this means having a managed approach to how devices are recognised, approved, protected, monitored, and handled throughout their time in use. The word "fully" sets a high bar, but it does not require perfect knowledge of every technical detail of every device. What it does require is a clear, managed, proportionate approach that covers the whole device lifecycle, from the moment a device is approved for use through removal or decommissioning.

The measures in question 2202.1 set out what good device management looks like in practice. Taken together, they cover the full lifecycle of a device's authorisation: establishing its identity, approving it for use, maintaining appropriate security, reviewing it regularly, and removing access when it's no longer needed or is suspected to be compromised.

Modern Equivalent Approach;

Some organisations use continuous or dynamic trust models, such as Zero Trust architectures and Conditional Access. These approaches reassess device trust on an ongoing basis, rather than relying on a one-time approval decision. This aligns with the intent of this control (maintaining appropriate, risk-based device trust throughout the device lifecycle), and these approaches are acceptable.

If you use a modern implementation that meets or exceeds the control intent but does not map neatly to the control questions, explain your approach to your Assessor so that it can be considered appropriately in the scoring.

2202.1 - (MOD 000389) - (L2-L3)

How does the organisation ensure only trusted devices access trusted networks and systems?
Available answers (choose all that apply):

- ☐ Establish identities for endpoint devices
- ☐ Explicitly authorise identified endpoints
- ☐ Only authorise devices with a business need
- ☐ Configure endpoint security software to enforce security policies
- ☐ Deauthorise trusted endpoints when no longer required
- ☐ Deny unauthorised endpoints access to trusted resources
- ☐ Revoke authorisation for compromised endpoints
- ☐ Regularly review justification for trusted endpoints
- ☐ Monitor endpoint configuration and usage
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will expect evidence to correspond with your selected answers, such as an endpoint device management policy or a screenshot demonstrating security software enforcing the specified policies.

2203 - Privileged user management

Term

A privileged user is someone who has special permissions that go beyond those of a regular user. They can make significant changes to the system or access sensitive information.

Control Requirement

The Applicant shall closely manage privileged user access and actions to networks and information systems supporting functions and that protect data.

Jargon Buster

This control looks at how you control and monitor the access and activities of privileged users.

2203.1 - (MOD 0000390) - (L2-L3)

Which of the following actions does the organisation take to manage privileged user access and actions?

Available answers (choose all that apply):

- ☐ Maintain records of privileged accounts.
- ☐ Review justification for privileged accounts at least quarterly.
- ☐ Review justification for privileged accounts upon transfer or termination.
- ☐ Log privileged user actions.
- ☐ Review privileged user actions at least quarterly to confirm legitimate use.
- ☐ None of the above.

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: You could include documentation of privileged accounts, meeting minutes from reviews, change or version histories, and activity logs.

2203.2 - (MOD 000391) - (L2-L3)

What privileged user actions are logged by the organisation?
Available answers (choose all that apply):

- ☐ Login attempts
- ☐ Command executions
- ☐ System changes
- ☐ Access to sensitive resources
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: The Assessor will expect to review logs that demonstrate the selected actions are being recorded.

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.

Malware operates with the same privileges as the user it infects. By limiting account privileges, you can significantly reduce the potential impact of an attack. Users with internet access should not have administrative rights. If administrative privileges are required, internet access should be restricted or tightly controlled to minimise risk. This ensures that, even if a phishing link is clicked, the malware will be unable to execute or cause significant harm.

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 - 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.

2206.1 - (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.

2207 - 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.

Separation of duties also refers to the difference between standard user accounts and administrator accounts. Account separation is required for all administrator accounts. This includes local administrators, domain administrators and cloud administrators. Accounts with admin privileges should not be used for day-to-day work. An attacker who gains admin credentials on any of these systems can easily change configurations, install malware and carry out other damaging activities.

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.

2207.1 - (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.

2207.2 - (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.

2208 - Identity and Access Management (IdAM)

Terms

- Identity and access management, often called IdAM, IAM or just identity management, is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources.
- An entity is a user, administrator or system. Each entity needs an identity.
- Authentication is the verification of the entity's identification.
- Authorisation is the process of checking what access the entity should have.
- A role is a set of permissions that can be assigned to users, groups, or other entities.
- Service accounts are accounts not associated with a human; they are used by applications, systems, or services to access resources and perform tasks

Control Requirement

The Applicant shall closely manage and maintain identity and access control for users/admins, devices and systems accessing their networks and information systems supporting business functions and protecting all data.

Jargon Buster

Without good identity and access management, even a well-managed network with patched systems and firewalls will not prevent an attacker with valid credentials from accessing your systems. This control is about how your identities and their accesses are managed.

When answering these questions, have in mind your life cycle for identity and access.

2208.1 - (MOD 000398) - (L2-L3)

Which of the following does the organisation use to manage identity and access controls for users, administrators, devices and systems accessing its non-public networks and information systems?
Available answers (Choose all that apply):

- ☐ Authentication of entities
- ☐ Authorisation of access
- ☐ Accounting of activities
- ☐ None of the above

Example: Our IAM life cycle covers... (For each selected answer, clearly explain how you are doing what you say you are doing. For authentication, consider who you are authenticating, i.e. business to business, business to customer and business to employee and how i.e. Single Sign-On. For authorisations, consider how access is authorised (e.g. role-based access control). For accounting of activities, think about how activities are tracked and logged (e.g., audit logs, SIEM tools).)

Expected Evidence: Your Assessor will want examples of tools, policies, or processes used for each selected answer.

2208.2 - (MOD 000074) - (L2-L3)

Does the organisation maintain an inventory of all service accounts?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Think about how service accounts are created and documented during provisioning, and how they are deprovisioned when no longer needed.)

Expected Evidence: Your Assessor will want to see the inventory of service accounts.

2208.3 - (MOD 000399) - (L2-L3)

Has the organisation implemented automated mechanisms within its critical or sensitive systems that:
Available answers (Choose all that apply):

- ☐ Notify administrators of account changes
- ☐ Notify administrators of unusual system account use
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will want to review a sample notification and the configuration that shows the automated mechanism setup.

2208.4 - (MOD 000400) - (L2-L3)

Has the organisation implemented automated mechanisms to:
Available answers (Choose all that apply):

- ☐ Notify relevant stakeholders of staff terminations and transfers
- ☐ Provision accounts on sensitive or critical systems
- ☐ Deprovision accounts on sensitive or critical systems
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will want to see the tools or systems in use, example notifications and configuration details or workflows.

2209 - Limit access to authorised entities

Control Requirement

The Applicant shall implement automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users.

The Applicant must use automated systems to manage and monitor, through their lifecycle, both system accounts and processes acting on behalf of authorised users. This refers to automated system accounts and the management of them.

Jargon Buster

This refers to automated system accounts and the management of them. An automated system account is a type of account that operates on a device with specific permissions or access rights, without requiring any direct user interaction. These accounts are not intended for real users to log in as; instead, they are designed to perform automated tasks or processes.

The purpose of system accounts is to eliminate the need for manually increasing permissions or access rights, which can introduce security risks. However, if not properly managed, these accounts can become a vulnerability, as they may be exploited for unauthorised activities.

This control aims to assess the maturity of your organisation's management of automated system accounts. Effective management includes implementing mechanisms to monitor and alert on any misuse or unauthorised modification of system account activities.

2209.1 - (MOD 000648) - (L3)

Does the organisation have automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use a software product to deliver this capability. Or, we have configured all relevant systems to alert when system account conducts certain activities. This is then investigated manually.

Expected Evidence: Screenshot or configuration log of the tool of the mechanism, example of tool in operation and documentation showing how it is managed.

2210 - Limit to authorised transactions

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 its 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).

Control Requirement

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

Jargon Buster

This control requires a documented process for managing the lifecycle of accounts, be it a user or system/process, limiting system access to the types of transactions and functions that authorised accounts are permitted to execute. Control 2209 is about limiting access to authorised entities and 2210 covers how those authorised entities are managed.
It is important to note that Applicants must prevent the reuse of identifiers (e.g. reusing an old username for a new user) for a defined period after an account is deactivated. Failure to do this may result in the new user inheriting permissions assigned to the previous user along with access to files or systems they should not have.

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.

2212 - Automated password management

Control Requirement

The Applicant shall employ automated mechanisms for the generation, protection, storage, rotation, transmission, cryptographic protection and management of passwords for staff and systems.

Jargon Buster

The control is about **automated mechanisms** for managing password lifecycle end-to-end so think about what automation your users and systems have to protect passwords.

You should follow NCSC's current guidance for password management.

Where possible, automate password management through technical controls (e.g. platform/system settings) as relying on policy alone can introduce weaknesses.

However, it may not be possible to implement these technical controls on OT or legacy systems. Where this is the case, the Applicant must explain why and set out what alternative steps or mechanisms are in place to mitigate the associated risk.

Controls 2212 and 2213 should be considered together where possible. Although 2213 applies to Level 1 and above, and 2212 applies to Levels 2 and 3, an Applicant may (but is not obliged to) implement both controls to strengthen their security posture, even if they intend to certify at Level 1.

2212.1 - (MOD 000470) - (L2-L3)

Which of the following does the organisation use to automate the protection of passwords?
Available answers (choose all that apply):

- ☐ Password hashing
- ☐ Password policy compliance check
- ☐ Account lockout policies
- ☐ Password manager tools
- ☐ Password generators
- ☐ None of the above

Example: We use all of the above (for each selected answer, clearly explain how you are doing what you say you are doing)

Expected Evidence: Password or account management policy/process, password management tool configuration screenshot, logs of checks carried out

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 assess the strength of passwords. It wants to confirm you are making sure passwords meet certain quality standards or best practices.

The password requirements below are a minimum; they should be exceeded if systems allow it. Assessors will be expecting to see the latest NCSC guidance is being followed unless there is a technical reason why this is not possible, such as legacy technology that does not allow more than 8 characters.

Applicants may use passwordless, phishing resistant methods (e.g. passkeys) to meet this control. It is not expected that Applicants will reduce their password requirements to match those listed in the control or its questions.

Applicants may have different password policies for different account or user types, while still aligning with NCSC guidance. For example, human-remembered passwords should be memorable and should not be routinely rotated. This should be distinguished from other credential types, such as machine accounts or vaulted secrets, which may require different controls (e.g. different length, complexity, storage, and rotation requirements).

Controls 2212 and 2213 should be considered together where possible. Although 2213 applies to Level 1 and above, and 2212 applies to Levels 2 and 3, an Applicant may (but is not obliged to) implement both controls to strengthen their security posture even if they intend to certify at Level 1.

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 by using throttling and lockouts.

NCSC provides up-to-date guidance on password administration, which should be consulted for the latest best practices. If NCSC guidance conflicts with the wording of this control you should follow the NCSC guidance and inform the Assessor who will take this into consideration.

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. (as defined by NIST)

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.

2216 - Privilege failure handling

Control Requirement

The Applicant shall prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Jargon Buster

A privileged function is an action on a computer system that's reserved for users with the necessary permissions. If someone without these permissions attempts the function, the computer simply won't execute it. All actions and attempted privileged functions should be recorded, regardless of the user's privilege level.

2216.1 - (MOD 000091) - (L2-L3)

Does the organisation restrict standard users from executing privileged functions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the controls include (describe how standard users are restricted from executing privileged functions).

Expected Evidence: Your Assessor will want to see the tools or settings used to prevent the above actions.

2216.2 - (MOD 000467) - (L2-L3)

Does the organisation log attempts by non-privileged users to access privileged functions?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is fed into our SIEM.

Expected Evidence: Your Assessor will expect to see example logs.

2217 - Service accounts

Term

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

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.

Jargon Buster

The intent of this control is to confirm that your organisation is implementing effective account management practices to generic service and system accounts. You should be able to demonstrate that you track these accounts with clear ownership and accountability for their management.

It must be noted that this control applies to all three account types: generic, service, and system accounts. When answering 2217.1 and 2217.2, you must address each of these types, even though 2217.2 only explicitly mentions two. If additional account types are introduced through newer technologies, they should also be considered where relevant.

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.

Not everything interacting with your system will be a person using a standard user account. In OT environments, such as a factory floor, you may have engineer workstations, SCADA machines, jump boxes, programmable logic controllers (PLCs), and scheduled jobs running automatically. Each of these should be uniquely identifiable whether that's by device name, network address, location on the network, or the account or service that owns it. The key question is simple: if something is active on your system, can you clearly identify what it is, and who (or what) it belongs to?

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.

23XX Family – Data Security

The protection in place for data that supports the operation of essential functions must be matched to the risks associated with that data.

As a minimum, unauthorised access to important and critical data should be prevented (protecting data confidentiality). This may mean, for example, protecting data stored on mobile devices which could be lost or stolen.

Data protection may also need to include measures such as the sanitisation of data storage devices and/or media before sending for maintenance or disposal.

Protect data in accordance with the risks to essential functions posed by compromises of data integrity and/or availability. In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date, isolated (e.g. offline) back-up copies of data, combined with the ability to detect data integrity failures where necessary. Software and/or hardware used to access critical data may also require protection.

It is important to ensure that data supporting the operation of essential functions is protected in transit. This could be by physically protecting the network infrastructure, or using cryptographic means to ensure data is not inappropriately viewed or interfered with. Duplicating network infrastructure to prevent data flows being easily blocked provides data availability.

Some types of information managed by an organisation responsible for an essential function would, if acquired by an attacker, significantly assist in the planning and execution of a serious attack. Such information could be, for example, detailed network and system designs, security measures, or certain staff details. These should be identified and appropriately

protected. Networks and information systems should be designed to protect important data.[11]

[11] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b3-data-security

2300 - Data security

Control Requirement

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.

2301 - Understanding data

Control Requirement

The Applicant shall have a good understanding and classification of the data important to the operation of functions and protection of data, including where it is stored, where it travels, the application of protective markings to media. The Applicant shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of functions and protection of all data.

Jargon Buster

Understanding your data is the foundation of protecting it. If you don't know what data you hold, how sensitive it is, or where it is stored, shared, or processed, you can't make informed decisions about how to handle it safely. Poor data handling can have serious consequences for your organisation, far beyond the commercial risks a typical business might consider. Data classification is how your organisation sets clear rules for handling different types of data. It helps protect confidentiality, integrity and availability by ensuring that appropriate controls are applied to the right information.

There is no single classification scheme you must use. Your classification system should reflect your organisation and be proportionate to the data you hold. As a starting point, common categories include:

- Contractually protected data (e.g. information covered by a non-disclosure agreement)
- Commercially sensitive data (e.g. pricing, intellectual property, or business plans)
- UK Government Security Classifications (where you handle information on behalf of, or released by, a government customer)

Your data may not map neatly to an existing scheme and that is acceptable. What matters is that your organisation has identified the data it holds, agreed the level of protection each type requires, and made sure everyone who handles it understands the rules.

Classification applies wherever your data lives and wherever it goes. This includes physical media (such as USB drives or printed documents) and digital environments (such as cloud services, email databases, and third-party applications). Your handling rules should follow the data across storage, transfer, and processing.

This also includes data you share externally. If you share data with suppliers, subcontractors, or partners, you should understand what you are sharing, why you are sharing it, and what protections are in place to ensure it is handled appropriately outside your organisation.

Applicants should be aware of their responsibility to report incidents relating to Defence-related classified material to the UK MOD (for example, via MOD Defence Industry WARP).

2301.1 - (MOD 000412) - (L2-L3)

Does the organisation identify and understand the data critical to its functions?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes (provide details on how this was achieved, such as through data mapping exercises, stakeholder consultations, or risk assessments).

Expected Evidence: Your Assessor will expect to see documentation of the data identification process, reports, risk assessments, meeting minutes or records showing discussions about critical data.

2301.2 - (MOD 000413) - (L2-L3)

Does the organisation have a data classification approach that considers the impact from:
Available answers (Choose all that apply):

- ☐ Unauthorised access
- ☐ Unauthorised modification
- ☐ Loss of availability
- ☐ None of the above

Example: (For each selected answer, clearly explain how the organisation's data classification approach addresses the specific impact.)

Expected Evidence: Your Assessor will expect to see a documented data classification policy or framework.

2301.3 - (MOD 000414) - (L2-L3)

Does the organisation maintain an inventory of where data is stored?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we keep a comprehensive inventory of data storage locations, including info such as…

Expected Evidence: Your Assessor will expect to see a data inventory document or database.

2301.4 - (MOD 000415) - (L2-L3)

Does the organisation maintain an understanding of where data moves, including internally and to third parties?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we track data flows by…

Expected Evidence: Your Assessor will expect to see data flow diagrams or maps and sharing agreements with third parties.

2302 - Data in transit

Control Requirement

The Applicant shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the functions and all data. This includes the transfer of data to third parties.

Jargon Buster

This control is about ensuring that data being transferred (or "in transit") is protected from unauthorised access, interception, or tampering. This includes using encryption where necessary, whether the data is being sent over the internet, within internal networks, or to third parties. It also covers protecting physical storage media (such as USB drives or hard drives) when they are being moved.

The final version of TLS 1.3 was released in 2018 and has since become widely adopted. While TLS 1.2 is still in use, using the latest version offers enhanced security.

2302.1 - (MOD 000416) - (L2-L3)

Has the organisation assessed and identified the encryption requirements for all data in transit?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: yes, our evaluation included... (how you came to your decision on encryption requirements).

Expected Evidence: Your Assessor might expect to see the assessment of the requirements, as well as any resulting policies or procedures developed from it.

2302.2 - (MOD 000422) - (L2-L3)

Has the organisation's assessment of encryption requirements covered all data in transit, including the following?
Available answers (Choose all that apply):

- ☐ Over the internet
- ☐ Within your networks and systems
- ☐ Via removable media
- ☐ None of the above

Example: all (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will want to see the above considerations addressed in your assessment.

2302.3 - (MOD 000423) - (L2-L3)

Does the organisation use Transport Layer Security (TLS) version 1.1 or earlier for protecting any sensitive data in transit?
Available answers (choose one):

- ☐ Yes
- ☐ No
- ☐ Not applicable

Example: No, we use… (TLS1.2 or higher).

Expected Evidence: Your Assessor will want to see configuration settings or logs showing the use of the latest supported version of TLS

2302.4 - (MOD 000104) - (L2-L3)

Does the organisation protect storage media and equipment containing data when physically moved?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: yes, we use…

Expected Evidence: Your Assessor will want to see what measures you are using to protect physically moved data - for example, documented processes for secure media transportation or examples of secure storage devices.

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)

Terms

In this context, 'data' refers to any information generated, stored, or handled by the organisation in support of its Functions. These terms are defined by the MOD.

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

Remote access is any method staff use to connect to your organisation's systems or data when they are not connected to your normal managed work network (e.g. working from home or from another location). This includes accessing third-party cloud services that you do not host, such as web-based email.

This control sets the security expectations for remote access. Although it refers specifically to VPNs, you may meet the intent of the control using other remote access methods, provided they deliver equivalent protection.

Split tunnelling is a networking technique that routes some traffic through the VPN while allowing other traffic to go directly to the internet.

A full tunnel VPN routes all traffic through the organisation's network. This can provide stronger protection for remote workers and increase organisational visibility, monitoring, and control. However, it can also place greater demand on infrastructure due to increased bandwidth, processing, and logging requirements.

Applicants should take relevant NCSC guidance into account, including guidance on VPNs and Zero Trust. Regardless of the mechanism chosen, it must provide security that is equivalent to, or exceeding, that of a full-tunnel VPN

- https://www.ncsc.gov.uk/collection/zero-trust
- https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks.

Controls 2305 and 2306 overlap and may be easier to address together. Control 2305 focusses on staff connecting to the organisation, while 2306 requires all remote sessions (human and non-human) to be encrypted. You may also wish to consider control 2307 (Managed access control points) as part of your approach to meeting 2305 and 2306.

Before answering the questions, consider what "remote access" looks like in your organisation. For example, how might staff connect when they are:

- working anywhere other than your office
- using remote desktop
- signing into cloud services (e.g. email, file storage, business apps)
- carrying out sensitive work that faces higher threats, or where contractual requirements apply

If staff do not need remote access to an internal network, you may not need a VPN. You should not install a VPN just to pass the control if it is not suitable for your organisation. An incorrectly configured VPN can introduce new security risks. A simple check is:

- What are staff trying to access remotely?
- Is there already a secure way to access it (for example, a cloud service or secure web portal using MFA and encryption)?

Whatever method you choose, you must ensure it:

- uses MFA as a minimum before access is granted or Data is transferred between the remote device and organisation's networks and systems

- protects data in transit using encryption (e.g. HTTPS/TLS or encryption within a VPN)
- Only transmits Data via channels controlled by the organisation

You should also consider how you:

- mitigate threats such as captive portals, WiFi evil twin/fake access points, DNS poisoning, and similar threats
- force traffic between a device and external services through internal, protective monitoring tools
- enable the organisation to monitor, filter and detect suspicious traffic that may indicate a device has been compromised or is acting suspiciously

For organisations using cloud-based Remote Monitoring and Management (RMM) tools, the connections between the cloud service and the organisation's networks and devices should be via VPN or other suitable alternative technologies, where it is deemed appropriate for the risk/threats faced.

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

Control Requirement

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 all of your remote access sessions and keep them private. Your solution to controls 2305 and 2307 may overlap with this control.

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. Your solution to controls 2305 and 2306 may overlap with this control.

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.

2308 - Stored data

Control Requirement

The Applicant shall appropriately protect the confidentiality of soft and hard copies of data being stored for all functions.

Jargon Buster

This control focuses on the disposal of hard copies.

2308.1 - (MOD 000439) - (L2-L3)

Has your organisation implemented appropriate controls to protect stored confidential data from the following threats?

Available answers (Choose all that apply):

- ☐ Intruders
- ☐ Bystanders
- ☐ Insider threat
- ☐ None of the above

Example: (For each selected answer, provide a clear explanation of what you have implemented. Be sure to address both physical formats, such as confidential data printed on paper or other physical medium, and digital formats, stored electronically as digital files.)

Expected Evidence: Your Assessor will expect to review the implemented controls, whether they involve documentation, technology, or tools.

2308.2 - (MOD 000440) - (L2-L3)

Does the organisation require personnel to store confidential data only in approved locations?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, … (specify where, such as in a secure room, a designated storage area, etc. This can be generalised if necessary).

Expected Evidence: Your Assessor will request a list of approved locations and might also conduct a site visit.

2308.3 - (MOD 000442) - (L2-L3)

Does the organisation label assets to help personnel track those containing confidential data?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our labelling system includes… (details of what is included on the labels for tracking assets containing confidential data).

Expected Evidence: Your Assessor will want to see a sample of the labels.

2308.4 - (MOD 000441) - (L2-L3)

Does the organisation ensure adequate secure data storage facilities are provided to staff who are required to store confidential information?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, (Describe the facilities you provide. For instance, in an office environment, do you provide secure safes, locked filing cabinets, or restricted-access storage rooms for physical documents?)

Expected Evidence: Evidence may include a list of secure storage facilities (e.g., safes, locked cabinets, restricted-access rooms), policies for remote staff on secure storage, photos of storage solutions or even records of staff training. Your Assessor may request a site visit.

2308.5 - (MOD 000438) - (L2-L3)

Has the organisation implemented full disk encryption on data storage where necessary to protect the confidentiality of data at rest?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is detailed in our build process

Expected Evidence: Your Assessor will prefer practical evidence demonstrating that full disk encryption is in place, such as details of the encryption software used, screenshots or reports. They may also accept policy documentation outlining your approach to encrypting data at rest.

2308.6 - (MOD 000443) - (L2-L3)

Has the organisation trained its staff on how to manage the storage of confidential data?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our training is part of... (explain how the training is incorporated into the overall staff training program).

Expected Evidence: Your Assessor will want to see how training is being delivered and see records of completion.

2309 - Mobile data

Control Requirement

The Applicant shall protect, such as through encryption, data important to the operation of functions and all data on mobile devices.

Jargon Buster

This control should really be called encryption of mobile devices because it's essentially about ensuring that mobile devices are encrypted to protect sensitive data.

2309.1 - (MOD 000430) - (L2-L3)

Does the organisation ensure that all mobile devices processing Data have full device encryption?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is configured in our MDM

Expected Evidence: Your Assessor will want to see proof that all mobile devices used to process sensitive data are encrypted. This could include a policy document that requires encryption, reports from mobile device management (MDM) software showing encryption is enabled, or a list of devices with confirmation that encryption is active. There will likely be crossover with the following question.

2309.2 - (MOD 000464) - (L2-L3)

Does the organisation remotely configure and manage mobile devices accessing its secure environment or data, ensuring it can:
Available answers (Choose all that apply):

- ☐ Restrict Data access to authorised users and applications
- ☐ Require passcodes and biometrics to access Data
- ☐ Securely remove Data
- ☐ Maintain a minimum standard of device and application patching
- ☐ Confirm device security features have not been bypassed (e.g. jailbreaking/rooting)
- ☐ Manage applications containing Data
- ☐ Monitor application compliance with organisational policy
- ☐ Verify full device encryption is enabled
- ☐ Require minimum application and device inactivity locks
- ☐ None of the above

Example: (For each selected answer, clearly explain how you are doing what you say you are doing.)

Expected Evidence: Your Assessor will expect evidence for each selected answer, demonstrating how mobile devices are managed and secured. For example: If you select "Require passcodes and biometrics to access data," you could explain how mobile devices are configured, then show a device being unlocked using these methods.

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)?
It should be noted that FIPS-140-2 has been superseded by a newer version. Wherever possible, Applicants should utilise the latest supported version or, at a minimum, ensure the use of AES 256 encryption. Organisations should be aware of the lifespan of the products used and plan to update the products without interruption, or reduction, in the level of security.

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

Control Requirement

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 focuses on defining the locations, beyond your company's main office, where your staff and contractors are permitted to work. Your organisation must establish a clear list of approved working location types, based on what is appropriate for your structure, operating environment, and risk. Applicants are not required to list every individual address where staff may work. A list of approved location types is sufficient. Approved locations may vary between organisations, departments, and roles, and may include (for example) home working, customer sites, or public spaces. Restrictions may also be driven by contractual obligations, data classification requirements or other relevant considerations.

Controls 2311 (Authorised working locations) and 2312 (Security at alternate working locations) should be considered together.[12]Control 2311 defines which types of locations are permitted, while control 2312 sets out the security measures to consider for each location type. Different location types may require different security measures and may also restrict the work that can be carried out. Applicants should take relevant NCSC[13] and NPSA[14] guidance on remote working into account.

[13] https://www.ncsc.gov.uk/section/advice-guidance/all-topics/remote-working
[14] https://www.npsa.gov.uk/specialised-guidance/insider-risk-guidance/remote-working-0

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.

The actions listed in the control text are examples, not a checklist. Your approach should be proportionate to the risks you face, and you should be able to explain how your chosen measures mitigate those risks.

For example, disabling USB and other ports by default may be a sensible starting point, but this is not a requirement. You should decide whether ports need to be restricted, disabled or physically removed based on the risks to your organisation and your business needs. Where there is a legitimate business requirement for an exception, such as penetration

testing or other approved specialist activities, this should be documented, authorised and subject to appropriate safeguards.

You can meet this control using a combination of physical and technical controls. For example, you might physically remove a USB port, or disable it through software. It is not expected that a single product or action will meet the entire control; it may be achieved through multiple mechanisms working together to meet the overall intent.

Security measures may also vary by location and the type of work being performed. For example, an Applicant might:

- not use an always-on VPN when working from a trusted location (e.g. home),
- not carrying out sensitive work in higher-risk locations (e.g. a café), and/or
- use measures to ensure the Wi-Fi they connect to is trusted.

Where sensitive work is being carried out and the risk is higher, additional controls may be appropriate for example, using a VPN to provide greater protection. For more information on VPNs and alternative technologies, see control 2305.

Applicants should understand the threats associated with alternate working locations and respond proportionately (for example, the risks posed by captive portals or rogue access points). User awareness and technical controls should be used together to reduce overall risk; you should not rely on only one of them.

Controls 2311 (Authorised working locations) and 2312 (Security at alternate working locations) should be considered together. Control 2311 defines which location types are permitted, while control 2312 sets out the security measures to consider for each type of site. Different location types may require different security measures and may also restrict the work that is permitted. Applicants should take relevant NCSC and NPSA guidance on remote working into account (as referenced in control 2311).

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

2313 - Media/equipment sanitisation

Control Requirement

The Applicant shall appropriately sanitise before reuse and / or disposal of the devices, equipment, and removable storage media & devices holding data important to the operation of business functions and that protect all data.

Jargon Buster

This control is about wiping your equipment of data -for example, preparing a laptop for reissue if an employee leaves or clearing data from a hard drive before disposal.

2313.1 - (MOD 000132) - (L2-L3)

Does the organisation sanitise devices, equipment, and removable storage media before reusing or disposing of them?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: The next two questions will expand on the administrative side of decommissioning, destruction and disposal, so for this question, focus your answer and evidence on the practical aspects of sanitisation. Your Assessor will specifically look for evidence such as sanitisation logs, certificates, or reports that demonstrate the process was successfully carried out.

2313.2 - (MOD 000133) - (L2-L3)

Which of the following are included in the organisation's decommissioning and destruction policy, standards, and procedures?
Available answers (choose all that apply):

- ☐ Secure removal and destruction of information based on sensitivity of data
- ☐ Type of medium (e.g. paper, tapes, disks, etc.)
- ☐ None

Example: This is addressed in..., which 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: A copy of the policy, standard or procedure.

2313.3 - (MOD 000444) - (L2-L3)

Does the organisation's disposal process for assets containing confidential information ensure the following?
Available answers (choose all that apply):

- ☐ Assets awaiting disposal are appropriately labelled.
- ☐ Evidence of sanitisation or destruction is obtained.
- ☐ Identifying labels are removed on disposal.
- ☐ Records of disposal are maintained.
- ☐ None of the above.

Example: The process for disposal is documented in...

Expected Evidence: For each of the selected answers, your Assessor would expect to see a piece of evidence for confirmation. While policies and processes are acceptable, they must be accompanied by proof of implementation - for example, a photo of a labelled asset awaiting disposal or certificates of destruction from third-party disposal vendors.

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).

Jargon Buster

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 Data or Personally Identifiable Information (PII) and government information. Whilst the control directly references PII (a predominantly US centric term for direct identifiers) it also means Personal Data as defined within the UK GDPR.

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.

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

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

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.

Encryption – Understanding Approved, Validated and Compliant terminology

When looking at the next few controls, you may come across three terms that are easy to confuse: approved, validated, and compliant. Getting this right matters, because holding a certificate is not the same as being secure.

Approved means a cryptographic standard or method has been recognised by a national or departmental authority(for example, NCSC, NIST, NATO, or MOD) as acceptable for protecting data.

Validated means a specific product or cryptographic module has been independently tested and confirmed to meet an approved standard. For example, NIST operates the Cryptographic Module Validation Program (CMVP) for this purpose. A validated product has a certificate showing it meets the standard-but the certificate applies to the product/module, not to how it is implemented or configured in your environment.

Compliant means you are using the validated product correctly, with the required settings enabled. A product can be validated and still fail to protect you if it is not configured or used properly.

A useful analogy: a fire extinguisher may be certified to a safety standard, but if it is sitting uncharged in a cupboard, it will not save you in a fire. The validation certificate only has value when the extinguisher is on the wall, charged, and ready to use.

For guidance on cryptographic methods that are currently acceptable, refer to:

- NCSC: Cryptography guidance
- NIST: Cryptographic standards and guidelines

These sources are maintained by national bodies and updated over time to reflect current preferred practice.

2317 - Endpoint encryption

Term

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...

FIPS-140-2 has been superseded. Where possible, you should use a newer version of FIPS-140 or equivalent AES 256.

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.

Jargon Buster

This control requires full disk encryption on all endpoints, using an approved encryption standard. Devices can be lost or stolen, and this risk applies to organisations of any size. Full disk encryption helps ensure that if a device falls into the wrong hands, the data stored on it remains unreadable. Without full disk encryption, an attacker with physical access to a device may be able to remove the drive or otherwise extract data directly from storage.

This control is specifically concerned with protecting data at rest on endpoints (i.e. data stored on the device).

How you implement and evidence full disc encryption will depend on your size and operating model. For example:

- A small organisation may verify full disc encryption on each device individually, confirming that encryption is enabled and that the full drive is covered.
- A larger organisation will typically manage full disc encryption centrally through endpoint management tools, enabling consistent

configuration and providing a single view of encryption status across all devices.

In all cases, you should be able to demonstrate that encryption is enabled on all in-scope endpoints and that the encryption method used meets an approved standard. For guidance on approved cryptographic methods, refer to the NCSC and NIST links above.

It must be noted that some devices may not be able to meet the encryption required for this control, e.g. Operational Technology or legacy devices which do not have the technical capacity to meet the control. For such devices, you must take alternative measures to compensate and demonstrate these measures to the Assessor.

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

Control Requirement

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

This control requires that wherever cryptography is used to protect data, the methods used are recognised, supported and appropriate.

Cryptography protects data in two important ways. It keeps data confidential, meaning only the right people can read it. It also protects integrity, meaning you can trust that data has not been altered by someone who should not have access to it. This applies wherever data is being protected, whether that is in your communications, files, or data stored on your systems (at rest or in transit). If the cryptographic methods you use are weak or unrecognised, that protection may be worthless, even if it appears to be working.

A small business might demonstrate good practice by showing that the services they use, such as their email provider or file sharing platform, use approved cryptographic methods by default, and that they have a simple policy or document that records this. You do not need to be a cryptography expert, you just need to know what you are using and why it is appropriate.

A larger organisation might go further, with a formal cryptographic policy that defines approved methods for use across the business, supported by configuration evidence showing those methods are implemented and active.

For guidance on approved cryptographic methods, refer to the NCSC and NIST links in the above Encryption – Understanding Approved, Validated and Compliant section.

What if you can't use approved cryptographic methods?

In some cases, using approved cryptographic methods may not be possible. This is most likely where you are running older or specialist systems that do not support modern cryptography.

If this applies to your organisation you should:

- Seek advice from your certification body or retained security consultancy for guidance and next steps.
- Refer to MOD (Industry Security Notices) or NCSC guidance for alternative methods of achieving the control intent.

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 focuses on cryptography, specifically the management of cryptographic keys. Keys are what make encryption work. Without proper key management, even strong encryption can be undermined. If keys are lost, you may permanently lose access to your own data. If keys are exposed or shared too widely, unauthorised parties may be able to access that data.

How you manage keys will depend on your size and operating model. For example:

- A small organisation may manage keys using a reputable password manager (where appropriate) or a dedicated key management service, such as those provided by major cloud providers. The key requirements are that keys are stored securely, access is restricted to those who need it, and there is a process for updating or revoking keys when required.
- A larger organisation will typically use a centralised key management solution to manage key creation, storage, rotation, revocation, and deletion across the business, supported by configuration evidence demonstrating that it meets an approved standard.

For guidance on approved standards, refer to the NCSC and NIST links above.

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.

2320 - Data Loss Prevention (DLP)

Term

DLP: Data Loss Prevention is all about detecting and preventing certain data types from being lost, stolen, or improperly shared or transferred. It typically includes a mixture of strategies, processes and technology to prevent data leaks. This is typically done through known methods of extraction which should have been identified during a discovery phase, but may also include elements from threat intelligence or penetration testing.

Data types: A data type is a specific kind of sensitive information your DLP system is configured to look for and protect. Defining your data types tells the system what to watch out for. Example data types include; Personal information, financial information, health information, confidential business information and custom data. For defence suppliers, custom data, such as proprietary technical drawings, is often the most critical category.

Channels are routes through which data can travel out of your organisation via.

Appropriate DLP tooling: This is tooling that proactively monitors, detects, and prevents data loss across your channels in scope. It enforces your DLP policies automatically and generates evidence of that enforcement: alerts, logs, and reports that show the system is working. A tool is appropriate if it:

- Monitors the channels your policy covers
- Enforces the rules you've defined for your data types
- Generates alerts when a rule is triggered
- Provides logs or reports you can use as evidence

<u>Control Requirement</u>

The Applicant shall implement and maintain appropriate tooling to monitor and restrict the access and use of:

- Removable storage media and devices.
- External websites.
- Email.

Jargon Buster

This control expects two things:

- A clear policy that defines what sensitive data you're protecting and where/how it could leave your organisation.
- Technical controls (DLP tooling) that enforce that policy by monitoring and preventing data loss in real time.

Policy is not box ticking: it sets the rules your tooling must apply. But policy on its own isn't enough at this level you must also be able to show active enforcement through tools, not just guidance or training.

At its core, DLP (Data Loss Prevention) is about prevention. Training and policy tell people what they should do; DLP tooling provides oversight of what is actually happening and can stop sensitive data leaving when it should not. Without technical controls, you may not detect data loss until after the damage is done.

Applicants should consider the data types they handle and identify what information would cause harm if disclosed. They should also define which data types and channels they will monitor. As a minimum, this must include the following:

Channels in scope

- Removable storage: e.g. USB drives, external hard drives, memory cards.
- External websites: any web destination outside your organisation, including file-sharing sites, social media, and public forums (for example, posting sensitive project details on a hobbyist forum).
- External email: messages sent to recipients outside your organisation, including attachments

Though not listed above, AI tools, including public chatbots, AI assistants and features that send prompts to external services, should also be considered as potential data exfiltration channels where their use could allow organisational information to be sent to external websites or services.

Appropriate DLP measures should be considered where relevant to the risks and scope of the control.

Appropriate tooling
You don't need a single standalone DLP product. Many organisations use DLP features built into existing tools; others, especially smaller organisations, outsource to a managed DLP provider. Either approach is acceptable, as long as coverage is appropriate and the tooling is actively configured and maintained.

Expectations are proportionate to your risk. A ten-person firm and a large enterprise will implement DLP differently, but both must achieve the same outcome: active monitoring, enforcement, and evidence.

Common pitfalls

- Incomplete coverage, e.g. protecting one channel but not others
- Data types defined too loosely for tooling to enforce meaningfully
- Data types not defined at all

Ensure your tooling covers every channel identified in your policy. Review the channels you monitor regularly, and define data types that are specific enough to be detected and acted on in practice.

Monitoring and penetration testing should provide a continuous input to DLP for potential new sources of data exfiltration.

If you use a managed provider, you must still be able to demonstrate that the service is configured to reflect your policy, covers the required channels, and produces evidence that you can access and review.

This control is complementary to 2403 (Penetration testing) and 4105 (Exfiltration tests) which may overlap to some extent and show the effectiveness of DLP being tested.

2320.1 - (MOD 000469) - (L2-L3)

Does the organisation have a Data Loss Prevention (DLP) policy in place that covers:
Available answers (choose all that apply):

- ☐ What information may be released
- ☐ How the flow of data must be controlled
- ☐ How attempted unauthorised release is to be detected
- ☐ None of the above

Example: Yes, this appears in …, it covers …, and defines… It was last updated [date]

Expected Evidence: The policy or policies that would cover data loss prevention topics.

2320.2 - (MOD 000461) - (L2-L3)

Does the organisation have a Data Loss Prevention (DLP) policy in place that addresses data loss through the following channels?
Available answers (choose all that apply):

- ☐ Removable storage media and devices
- ☐ External websites
- ☐ Email
- ☐ None of the above

Example: Yes, … covers …, and defines… It was last updated [date]

Expected Evidence: The policy or policies that would cover data loss prevention for the selected topic.

2320.3 - (MOD 000462) - (L2-L3)

Does the organisation implement systems to enforce its Data Loss Prevention (DLP) rules and to generate alerts?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use... which enforces our data protection policies and...

Expected Evidence: Your Certification Body Assessor may expect to see a screenshot of the data loss prevention settings in the system, a recent example of an alert or a summary report from the system showing enforcement action.

2320.4 - (MOD 000159) - (L2-L3)

Are automated search tools used to identify data in unauthorised network drives or online/cloud storage locations?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use automated search tools such as... that...

Expected Evidence: Your Certification Body Assessor may expect to see screenshots or logs from the search tools demonstrating what it searches for or a sample report or log showing the detection of this type of activity.

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 may include press releases, social media updates, product information and published road maps etc. Non-public information includes any data your organisation has classified, labelled, or otherwise designated as non-public.

The Applicant should review non-public(including classified) information as defined by their own classification scheme, and in a way that is proportionate to their public footprint. This control may not be not limited to defence-related information: it could also covers sensitive information about the Applicant (e.g. commercially sensitive material) that the Applicant does not intend to be publicly available.

Applicants are not expected to review all general business content. Instead, they should have mechanisms in place to prevent non-public information from being published, and to remove or remediate any non-public information that is made 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?
Before making content available on a public system, does your organisation conduct a review to make sure information you have classified as private 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?
Is your organisation reviewing the content on its public systems to make sure that information that your organisation has classified as non-public 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)

Terms

Bring Your Own Device (BYOD): When an individual uses their own personal device for work purposes. This is different from your organisation providing a device that staff are also allowed to use personally.

Corporate environment: Your organisation's systems, networks, applications, and data. This includes email, file storage, internal tools, and any other business system your staff connect to.

Mobile Device Management (MDM): A type of software that lets your organisation remotely configure, monitor, and manage mobile devices. MDM is one way to meet this control, but it is not the only way.

Equivalent solutions: Other tools or approaches that achieve similar outcomes. These include:

- Mobile Application Management (MAM): manages specific apps on a device rather than the whole device
- Containerisation: separates work data and apps from personal ones on the same device
- Virtual Desktop Infrastructure (VDI): lets users access a secure virtual desktop from their device, so corporate data never actually sits on the device itself

Remote wipe: The ability to delete all data from a device remotely, without physically having it. Useful when a device is lost or stolen and corporate data is stored on it.

Disabling access: Revoking a user's ability to connect to your systems. Where no corporate data is stored on the device itself, this can achieve the same protective outcome as a remote wipe.

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.

Jargon Buster

When a device can access your business systems or stores copies of your data, it must be appropriately protected. Mobile devices are particularly vulnerable because they travel with their users, which increases the likelihood of loss, theft, or damage.

Allowing employees to use personal devices for work adds complexity, making it harder to manage and secure your corporate environment and data.

This control is designed to make sure that Bring Your Own Devices connecting to your systems meet a minimum-security standard.

Although the control refers to "industry recognised solutions such as…", it is not prescribing a specific product. It is seeking an outcome: that mobile devices are appropriately configured and managed, and that you have a clear, rehearsed process so that if a device is lost or stolen you can respond quickly and limit harm to the organisation.

The example solutions listed in the control may help you decide which approach is appropriate for your organisation. Applicants should also consider relevant NCSC guidance on the use and secure configuration of BYOD (Bring Your Own Device).

(https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device).

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?
Is a Mobile Device Management (MDM) system, or equivalent, 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?
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 once it is no longer needed, this includes data stored in electronic form on devices or hard/physical copies such as paper.

The Applicant is responsible for understanding the requirements outlined in documents such as contracts or Security Aspect Letters (SAL). It is also their duty to communicate these requirements clearly to the Assessor.

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.

24XX Family – System Security

There are a range of protective security measures that an organisation can use to minimise the opportunities for an attacker to compromise the security of networks and information systems supporting essential functions. Not all such measures will necessarily be applicable in all circumstances – each organisation should determine and implement the protective security measures that are most effective in limiting those opportunities for attackers associated with the greatest risks to essential functions.

Opportunities for attackers to compromise networks and information systems, also known as vulnerabilities, arise through flaws, features and user error. Organisations should ensure that all three types of vulnerability are considered when selecting and implementing protective security measures.

Organisations should protect networks and information systems from attacks that seek to exploit software vulnerabilities (flaws in software). For example, software should be supported and up-to-date with security patches applied. Where this is not possible, other security measures should be in place to fully mitigate the software vulnerability risk.

Limiting functionality (e.g. disabling services that are not required) and careful configuration will contribute to managing potential vulnerabilities arising from features in hardware and software.

Some common user errors, such as leaving an organisation-issued laptop unattended in a public place, inadvertently revealing security-related information to an attacker (possibly as a result of social engineering) etc. can provide opportunities for attackers. Staff training and awareness on cyber security should be designed to minimise such occurrences.

The majority of cyber security incidents can be traced to common cyber attack vectors. The opportunity for successful attacks can be minimised by

managing the known vulnerabilities which these attacks exploit. Many opportunities for user error can be reduced by technical means.[15]

[15] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b4-system-security

2400 - System security

Control Requirement

The Applicant 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

The NCSC provides guides which detail how to securely configure platforms commonly used.

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.

Controls 2402 and 2405 are similar and overlap to some extent, but 2405 has a narrower focus of patch management. You may have a policy or approach that will cover both controls.

Organisations must develop a strategy that is appropriate to their structure, environments, risks, and any other relevant factors.

Organisations may have technology that cannot fully meet this control. Where this is the case, it should be clearly documented and justified. The Applicant must also demonstrate how the associated risk is mitigated through alternative controls or measures. For example, if Operational Technology (OT) or legacy systems are excluded from the standard patch management programme, the Applicant must show what alternative steps are in place to protect those systems from the relevant threats.

Such measures may include (but are not limited to) network segmentation, restricted and monitored access, and privileged access checks before connecting to OT environments.

Although CVSS v3 is referenced as one way to prioritise remediation, it is not always the best measure of the impact a vulnerability may have on your organisation. Some vulnerabilities may not have a CVSS v3 score, and others may be low impact in your specific context.

DCC allows flexibility in how this control is met. The Assessor must be satisfied that the Applicant's approach is suitable and adequate for their organisation. Applicants should follow good practice and risk-based decision-making, rather than aiming only for compliance with a particular scoring scheme.
Applicants should also be aware that vulnerabilities are being exploited increasingly quickly. Vulnerabilities should therefore be remediated as soon as practicable, rather than routinely waiting up to 14 days.

It is recommended Applicants follow NCSC guidance (https://www.ncsc.gov.uk/collection/vulnerability-management) and regularly check for updates to this guidance.

Most organisations are familiar with the Cyber Essentials requirement to apply patches within 14 days of an update being made available by the vendor. However, this does not mean an Applicant is protected during that 14-day window. For business critical systems NCSC provides the following table for business -as-usual updates:

Type of estate	**Rollout**	**Update completed within**
Internet-facing services and software	Install on test environment or backup first. Test and rollout (a phased rollout can be used if applicable).	5 days
Operating system and applications	These updates should be applied automatically, as soon as an update is published. Phased rollout, for example 10% of the estate updated per day. Pause/rollback if issues encountered.	7 days
Internal/air-gapped service and software	Install on test environment or backup first. Test and rollout.	14 days

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

Control Requirement

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

A penetration test is an authorised, simulated cyber attack on your networks, systems, or applications to identify weaknesses that a real attacker could exploit. This control focusses on externally facing systems, because they are typically the easiest for attackers to discover, probe and exploit.

The intent of this control is to confirm that your organisation undergoes at least annual penetration testing carried out by an approved and suitably qualified tester using an appropriate, recognised testing methodology. The control does not mandate a single standard, as methodologies and scopes can vary. Instead, Applicants should select an approach that achieves the intended outcome and is appropriate, proportionate, and risk-based. For example, higher-risk or business-critical systems may warrant broader scope and/or more frequent testing, while lower-risk systems may justify a narrower scope.

Penetration testing may also include activities that overlap with other controls (for example, Data Exfiltration (4105) and Data Loss Prevention (2320)). Even where those controls are at a higher level than the Applicant is seeking (e.g. a Level 1 Applicant is not assessed against Level 2–3

controls), Applicants should not treat this as a reason to exclude exfiltration paths or data-loss scenarios from testing if they are relevant to the risks faced. The penetration test should be tailored to the Applicant's environment and threat model.

Testing should take place at least once every 12 months. Applicants should define and apply "timely" remediation based on risk: critical findings require faster action than lower-risk issues. The penetration test report should clearly describe what was tested (and how), the findings and their severity, any key assumptions or constraints, and recommended remediation actions.

Where an Applicant has no externally reachable systems, this may be demonstrated, and adequately proven, to the Assessor in order to show the control cannot be met. If the Applicant only uses systems provided by a third party, such as a Managed Service Provider (MSP), then the 14XX controls should show how this control is met on the Applicant's behalf.

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.

Jargon Buster

Out-of-band patching refers to patches released outside of the normal update cycle. These patches are often issued to address newly discovered critical vulnerabilities, particularly where active exploitation has been observed. In these circumstances, Applicants should apply the patch, or implement an effective mitigation, as soon as practicable, rather than waiting for the next scheduled patching window.

If you do not carry out the control requirement as written, document what you do instead and how it achieves the same security outcome. Explain how your approach manages the risk, and provide evidence that it is in place. Your assessor will review this evidence against the control's intent.

This control overlaps with 2402, Applicants should follow the NCSC guidance (https://www.ncsc.gov.uk/collection/vulnerability-management).

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....
xpected 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.

2406 - Privacy warning notices - prior to access

Control Requirement

The Applicant shall ensure that mechanisms are in place to ensure users accept appropriate warning notices prior to information system access. At a minimum, users must be warned that:

- Use of the information system is monitored, recorded and subject to audit.
- Unauthorised usage of the information system is prohibited.
- Unauthorised usage of the information system use is subject to criminal and civil penalties.
- In continuing, the user affirms consent to monitoring and recording of their activities.

Jargon Buster

This is about the alerts you may have set up on endpoints for users to read and agree to before they're allowed to access the endpoint.

2406.1 - (MOD 000650) - (L2-L3)

Does the organisation ensure users acknowledge appropriate warning notices before gaining system access?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: Your Assessor will want to see screenshots of the warning notices.

2406.2 - (MOD 000203) - (L2-L3)

Which of the following are included in the warning notices?
Available answers (Choose all that apply):

- ☐ Use of the information system is monitored, recorded and subject to audit.
- ☐ Unauthorised usage of the information system is prohibited.
- ☐ Unauthorised usage of the information system use is subject to criminal and civil penalties.
- ☐ By continuing, the user affirms consent to monitoring and recording of their activities.
- ☐ None of the above.

Example: We use all of these, they are added when devices/systems are onboarded and configured.

Expected Evidence: Your Assessor will want to see screenshots of the warning notices and any policy/process showing how/when the warnings are configured.

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.

Jargon Buster

This control is intended to prevent unauthorised viewing of information displayed on unattended screens. This includes content shown in notifications (e.g. an email title/sender or preview of a message) which could inadvertently expose sensitive information.

If an OT or safety-critical system cannot lock automatically without creating a safety risk, you should explain why. You should then demonstrate how unauthorised viewing is prevented through other controls and layered defences. This may include physical access controls, restricted areas, privacy screens, or other measures that limit who can see the screen.

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 5 minutes 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

You should be able to demonstrate how you manage the software that can run on your systems. Your responses should explain:

- how you decide which applications are permitted to run, and
- how all other software is blocked by default.

If you allow exceptions (for example, temporarily permitting software that would otherwise be blocked), describe how those exceptions are requested, reviewed, approved, and recorded.

Control 2410 is closely related, but focuses on the periodic review and ongoing management of the authorised software list. For control 2409, focus on how you identify and control which software is permitted to run.

A corporate environment is the infrastructure, software, and hardware an organisation uses to process, store, and manage data. It may be cloud-based, on premises, or a hybrid of both.

In most cases OT would not form part of the corporate environment, However, there may be occasions where legacy technology or OT is connected to, or forms part of the corporate environment. In these circumstances it is preferable to segregate it from the main corporate environment and implement suitable controls to limit and manage access to and from the corporate network.

Block-by-default (allow listing) typically provides stronger assurance and is often easier to manage over time than a denylist-based approach. Applicants must demonstrate how unauthorised software is prevented

from running. This may be achieved in a number of ways including(but not limited to):

- Built in OS controls
- Restricting what users or system accounts can do through privileges and permissions
- MDM/MAM controls (where applicable)

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 to 2410 but focuses on how you identify and manage which software is permitted to run. For control 2410, focus on how you periodically review and manage your authorised software list.

Organisations may review and manage the list of authorised software in a manner suitable for their organisation. This may be an annual full review alongside a more frequent addition/removal of programs as the business requirements change. The Applicant must show the Assessor that the list of approved software is being managed and maintained in a structured and organised manner rather than a rubber stamp/compliance led tick box exercise.

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.)

Jargon Buster

Within this control, the requirement is to intercept or prevent harmful downloads before they can affect the host. This may be achieved through sandboxing, or through existing security controls such as endpoint anti-malware that scans and blocks malicious content at download time.

Sandboxing is one way to meet this requirement, but it is not the only way. A sandbox is an isolated environment used to analyse files safely (for example, testing an email attachment) without exposing the host device or wider network. Other solutions that detect and block malicious files or content before use, without sandboxing, are also acceptable, provided they achieve the same outcome.

Not all networks or devices can support these types of solutions. In such cases, Applicants are expected to take a proportionate approach and implement appropriate mitigations. For example, in some Operational Technology (OT) environments it may not be reasonable to run anti-malware or similar tooling. Where this applies, Applicants should document and evidence the compensating controls in place, with a proportionate interpretation agreed with the Certification Body.

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.

2412 - Voice over Internet Protocol (VoIP)

Terms

Voice over Internet Protocol has been expanded to include common remote working tools that include Teams, Google Meet, Cisco Webex, Zoom, and WhatsApp. Technology has evolved from VoIP desk phones to include technologies such as:

- Virtual meeting platforms
- Collaboration tools/software
- Unified communication platforms

For more information, NCSC provides guidance to help you assess the security of voice, video and messaging communication services. https://www.ncsc.gov.uk/guidance/secure-communication-principles

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.

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

Does the organisation have a documented policy in place for the use of Voice over IP (VoIP) type 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: Our policy covers which roles and devices are allowed to use Teams, only certain roles are allowed this app and installation/use is restricted by MDM. Any attempted use of unapproved apps or by roles/users unauthorised to have the apps are blocked by device policy. Teams usage is monitored and controlled by the IT department to detect malicious usage.

Expected Evidence: Your Assessor will want to see how this is done, such as screen shots, policies and logs showing unauthorised attempts to install/use apps.

2413 - Mobile code management

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. Some examples of software technologies that provide the mechanisms for the production/use of mobile code include Java, JavaScript, ActiveX, VBScript, WebGL, Flash, malicious PDFs, scripts or macros, applets, plugins etc.
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, be it via the internet or internal networks. 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.
Mobile code may be controlled by deploying relevant security configuration settings to browsers as well as other applications such as Adobe Acrobat and Java. This may be accomplished via group policy settings or other methods.

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.

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, SSLv3, SNMPv1 and other weak protocols.

Expected Evidence: Configuration policy/processes, configuration screenshots, Security Policy, hardening guides.

2415 - Automatically identify and address misconfigurations and unauthorised components

Control Requirement

The Applicant shall employ automated mechanisms to detect misconfigured or unauthorised system components.

Jargon Buster

What does this mean? Well, you are required to implement automated tools or systems that can detect:

1. Misconfigured components: i.e. things that are not set up properly. Examples include incorrect settings, missing updates or patches, or configurations that differ from the approved standards.
2. Unauthorised components: i.e. things that are not permitted to be part of the network. This could include unapproved devices or rogue devices, unauthorised software, or equipment running outdated firmware.

In both cases, we are treating system components as hardware, software, and firmware components within the information system.

It's important to note that you don't need to rely on a single tool to meet this requirement. You can use a combination of tools to achieve compliance.

2415.1 - (MOD 000220) - (L3)

Does the organisation use automated mechanisms to detect misconfigured system components?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, misconfigured system components are detected by… (the tool that handles this).
Expected Evidence: Your Assessor will look for policy or processes that explain how your organisation identifies automatically misconfigured components. Tool configuration policy or screenshots, logs, or reports of findings that show tool is in use and running as expected.

2415.2 - (MOD 000651) - (L3)

Does the organisation address detected misconfigured system components through its vulnerability management process?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, once detected, an alert is automatically raised with detailed information about the affected system components. Appropriate actions are then automatically taken- e.g., removing or isolating the components in a quarantine or remediation network to enable patching, reconfiguration, or other corrective measures.

Expected Evidence: Policy or process showing actions to be taken, logs or reports showing detected misconfigured components and how they were addressed including follow up to show remediation and compliance.

2415.3 - (MOD 000221) - (L3)

Does the organisation have automated mechanisms to detect unauthorised system components?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, unauthorised system components are detected by… (the tool that handles this such as SIEM or MDM).

Expected Evidence: Policy or process defining how unauthorised system components are detected, tool configuration evidence, evidence automated mechanisms are in place and working.

2415.4 - (MOD 000503) - (L3)

Does the organisation address detected unauthorised system components through its incident management and change control processes?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, once detected, system components are automatically… (the actions take i.e. removed or isolated in a quarantine or remediation network to enable patching, reconfiguration, or other corrective actions.)

Expected Evidence: Policy or process defining how unauthorised system components are handled once detected. Incident response reports or change management logs will show how the organisation has responded to unauthorised system components.

2416 - Shared system resources

Terms

- Registers: Small storage locations within the CPU used for quick data access.
- Cache Memory: High-speed memory used to store frequently accessed data.
- Main Memory (RAM): The primary memory where active processes and data are stored.
- Hard Disks: Persistent storage devices that may hold sensitive data.

Control Requirement

The Applicant shall prevent unauthorised and unintended information transfer via shared system resources (e.g. registers, cache memory, main memory, hard disks).

Jargon Buster

Without proper controls, the above shared resources can become a vector for data leakage or unauthorised access. This control requires you to implement technical and procedural controls to mitigate these risks and protect sensitive information.

This control can be largely met through standard good practice that is already covered elsewhere in the framework (for example, keeping operating systems patched, using process isolation, applying encryption, and enforcing appropriate access controls).

2416.1 - (MOD 000504) - (L2-L3)

Has the organisation implemented system controls to prevent unauthorised or unintended information transfer via shared system resources?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: (Consider both unauthorised access and unintended information transfer in your answer. There are a variety of technical and procedural controls you could be using to answer this question. Think about your access control mechanisms, process isolation, encryption and monitoring. You may find that other controls already help demonstrate compliance with this requirement.)

Expected Evidence: The evidence will vary based on your response. You might demonstrate compliance through policies or technical configurations, in which case, your Assessor may request screenshots of system settings, virtualisation, or containerisation setups. Training records could also serve as evidence, showing how staff are equipped to prevent unintended information transfers.

2417 - Authorise remote execution of privileged commands

Control Requirement

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.

2418 - Baseline configurations and inventories

Terms

Baseline configuration: A documented, agreed set of security settings for your devices and systems. It defines how each system should be set up and what it should and should not be allowed to do.

System hardening: The process of reviewing and tightening default settings as part of building your baseline, turning off what isn't needed and locking down what is. New devices and software often ship with default settings designed for ease of use rather than security, and some features or services may be enabled that you don't need.

Unsupported software or hardware: Software or hardware that the developer or manufacturer no longer maintains, updates, or releases security fixes for.

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

This control requires you to build, document, and maintain baseline configurations for all your systems and devices. Applying consistent baselines across your organisation ensures each device meets an agreed security standard, reducing the risk that one misconfigured or overlooked system becomes a weak point. Your baselines must also restrict what users can do and address any unsupported software or hardware in your environment.

Unsupported software and hardware

Over time, security vulnerabilities will be discovered in unsupported software but will not be fixed, leaving systems exposed. The same applies to unsupported hardware where the manufacturer no longer provides firmware or security updates. Where possible, you should replace it or migrate to supported alternatives.

Where replacement is genuinely not possible, for example where software is tied to a specific piece of equipment or a contractual obligation, your baseline must document why it remains in use, the risk it introduces, and the steps you are taking to reduce that risk. This is not a general opt-out. The expectation is that unsupported software and hardware is identified, actively managed, and accounted for.

User actions

Your baselines should also restrict what users can do on your systems. This means preventing users from changing security settings, installing unapproved software, or otherwise deviating from the agreed security settings. In practice this is enforced through access controls and device policies. These are covered in more detail in other controls but must be reflected in your baseline configurations.

Example 1: standard IT environment

A small business defines a baseline configuration as part of onboarding new laptops. The baseline specifies which features are enabled or disabled, how updates are applied, and what users can and cannot do on the device. Each new laptop is configured to match the baseline before it is issued for use. The business reviews its baselines annually and updates them when new software is rolled out or a security issue is identified. One device was found to be running software no longer supported by the developer. The business documented this, assessed the risk, and restricted network access for that device while sourcing a replacement.

Example 2: OT environment

A large organisation operates a range of Operational Technology (OT) including different types of machinery and control systems. Because device types vary in function and firmware, the organisation maintains separate baseline configurations for each type. Shared elements, such as network settings and access controls, are covered by a common baseline that applies across the OT environment. Some systems rely on software that is no longer supported and cannot be replaced without unacceptable operational or safety risk. For these systems, the baseline documents why the software remains in use, the risk it introduces, and the compensating controls in place to contain that risk (for example, network segmentation and tightly restricted access). The organisation reviews its baselines at least annually.

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

Control Requirement

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.

Jargon Buster

This control is not looking at components such as resistors and capacitors, rather it focuses on ensuring that the hardware, software and firmware, you use are obtained from official trusted sources, 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.

Where possible Applicants should be familiar with the Software Security Code of Practice (https://www.ncsc.gov.uk/section/software-security-code-of-practice/overview) which will give greater assurance that the software and services used are resilient to cyber attacks.

This control links to 1300 (Asset Management) and 1400 (Supply Chain), which underpin control 2423. Applicants must be able to demonstrate that suppliers providing system components or support (such as updates) have been subject to appropriate due diligence and verification before being used.

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

2424 - Implement audit for stored credentials outside policy

Control Requirement

The Applicant shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/location/tools etc.) and quarterly audits are performed to ensure the control is consistently applied and functions appropriately.

Jargon Buster

There are a few key terms to break down when thinking about this control requirement:

Approved Storage: This refers to storing credentials in a manner that meets industry standards or guidelines - essentially, an authorised method of storage.

Secured Storage: The chosen method, whether it's a process, location, or tool, must ensure security. Think about the steps you are taking to protect the storage and ensure its security.

The second part is Audits. Routine audits should be conducted to verify that the storage method complies with the industry approved standards. These audits are essential to make sure that security measures are properly implemented and effectively protect the credentials.

2424.1 - (MOD 000514) - (L2-L3)

Does the organisation ensure that administrator credentials are stored using an approved and secure storage mechanism?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use...

Expected Evidence: Evidence for this question may overlap with that provided for other more specific controls. It could include documentation of the approved storage mechanism (e.g., compliance with recognised standards), configuration settings or screenshots of secure storage tools (e.g., password vaults, hardware security modules, encrypted databases), and policies or procedures detailing the secure storage of administrator credentials.

2424.2 - (MOD 000515) - (L2-L3)

Does the organisation audit its systems at least quarterly to ensure that controls enforcing the secure storage of administrator credentials are applied and effective?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last audit was [date]

Expected Evidence: Evidence could include audit reports or logs from the past year confirming quarterly reviews of the secure storage mechanism.

2425 - Use integrity verification tools

Control Requirement

The Applicant shall implement an integrity verification tool to detect unauthorised changes to web facing, critical software and firmware. Upon discovering discrepancies, the tool should automatically trigger the incident response process.

Jargon Buster

The control requires you to use a tool or tools to monitor your software, web systems, and firmware for any unauthorised changes. It uses a known good state (or trusted baseline) as a reference point for comparison. If the tool detects something unusual, it should automatically generate an alert and activate your process for handling security incidents.

2425.1 - (MOD 000516) - (L3)

Has the organisation implemented integrity verification tooling to detect unauthorised changes to web-facing, critical software and firmware?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use... (the name of the tool or tools, and a brief description of how the tool works or how you are using it.)

Expected Evidence: Your Assessor will want to see the scope of monitoring, so present something that shows how it's configured to monitor Web-facing software (e.g., website files, web application code), Critical software (e.g., operating system files, application binaries) and Firmware (e.g., BIOS/UEFI integrity checks).

2425.2 - (MOD 000517) - (L3)

Does the integrity verification tooling automatically trigger the organisation's incident response process on detection of unauthorised changes?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, ... (explain how briefly).

Expected Evidence: Your Assessor will need proof that the integrity verification tools are connected to the incident response process through automation. This could include a screenshot of an alert, logs showing past triggered responses (including incident response reports), or documentation explaining how the tool is set up to integrate with the process.

2426 - Anti-malware capabilities

Control Requirement
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

Control Requirement

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.

For controls 2427 and 2428 Applicants should be aware of NCSC guidance:

"In most commercial environments, standard architectural good practice is usually sufficient to manage data flows between these zones. However, when you believe that some of your systems may be subject to targeted attack, and the data is sensitive or critical, the risks increase significantly. In these higher-threat contexts, simple boundary controls are rarely enough. A cross domain approach can be used in these environments because it provides a deliberate, rigorous way to think about the risks of inter-zone data movement, and to design controls that remain effective even when an adversary is actively trying to subvert them.

Ultimately, cross domain is about enabling essential business functions in a safe, manageable and threat-aware way. It recognises that different parts of an architecture have different trust levels and that data flows between them must be carefully controlled when facing sophisticated or persistent threats."

More guidance is available from
https://www.ncsc.gov.uk/collection/cross-domain

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

Control Requirement

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.

2430 - External system connection review

Control Requirement

The Applicant shall promptly remove or disable unnecessary firewall rules when they are no longer required or fulfil no business need.

2430.1 - (MOD 000250) - (L2-L3)

Does the organisation remove or disable firewall allow rules when they are no longer required or serve a business need?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, the firewall rule management policy covers this in…

Expected Evidence: Your Assessor will probably request to review your firewall management policy. You may also be able to demonstrate compliance by providing evidence of past notifications or communications regarding changes, or in some cases, event logs.

2430.2 - (MOD 000524) - (L2-L3)

Does the organisation review and verify firewall rules at least annually?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last review was [date]

Expected Evidence: Your Assessor will expect to see something to show the review was conducted such as meeting minutes or a review report.

25XX Family – Network and System Resilience

The essential functions performed by an organisation should be resilient to cyber attack. Building upon the 24XX family of controls, organisations should ensure that not only is technology well built and maintained, but consideration is also given to how operation of the essential function can continue in the event of technology failure or compromise. In addition to technical means, this might include additional contingency capability such as manual processes to ensure functions can continue.

Organisations should ensure that systems are well maintained and administered through life. The devices and interfaces that are used for administration are frequently targeted, so should be well protected. Spear phishing remains a common method used to compromise accounts with privileged access. Preventing the use of these accounts for routine activities such as email and web browsing significantly limits the ability for a hacker to compromise them.

It's important to be prepared to respond to significant disruption by having business continuity and disaster recovery planning in place. This should include a definition of your most critical resources and an understanding of the order of actions needed to restore service(s). Test that these plans work, for example through manually triggering failover testing, carrying out table-top scenario walk-throughs, red-teaming or Cyber adversary simulation testing. You should be ready to adjust the security measures in place in response to changes in risk. For example, if threat intelligence indicates an increased likelihood of your organisation or sector being targeted you may decide to isolate operational networks until the threat has decreased. Alternatively, in the event of public disclosure of an unpatched vulnerability in equipment that you use, with reported use of exploits targeting the vulnerability, you may respond by elevating your protective monitoring, changing your configuration to avoid being susceptible, or taking other mitigating action in the period until a patch is made available and can be deployed.[16]

[16] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b5-resilient-networks-and-systems

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? 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? 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.

It is important to note that NCSC recommends that organisations maintain a copy of their response and recovery plans in a non-electronic format, such as paper. This ensures that the organisation can effectively respond to an attack even if the IT systems are unavailable and electronic versions of the plans cannot be accessed.

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.

2503 - Resilience preparation with testing

Control Requirement

The Applicant shall develop recovery plans for all systems that deliver Functions and protect Data. Recovery plans must also be tested at least annually with any deficiencies being recorded, risk assessed and resolved within defined timelines.

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 higher level, the emphasis is on validating your recovery plan is effective in practice.

It is important to note that NCSC recommends that organisations maintain a copy of their response and recovery plans in a non-electronic format, such as paper. This ensures that the organisation can effectively respond to an attack even if the IT systems are unavailable and electronic versions of the plans cannot be accessed.

2503.1 - (MOD 000529) - (L2-L3)

Does the organisation develop recovery plans for all systems to facilitate 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. Our process is covered in our risk assessment policy. 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 will be cross referenced to the 1200 control family which could have triggered the writing of plans.

2503.2 - (MOD 000530) - (L2-L3)

Does the organisation test its recovery plans at least annually?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last tests were conducted [date]and [date].

Expected Evidence: Your Assessor may expect to see dated proof of testing - for example, test results, reports, or communications - to show the recovery plan was practically demonstrated.

2503.3 - (MOD 000258) - (L2-L3)

Are issues identified during recovery plan testing recorded, risk-assessed, and addressed within organisationally defined timelines?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, issues from recovery plan testing are logged, risk-assessed, and resolved within [timeframe], with progress tracked and escalated if required.

Expected Evidence: An example issue/finding that shows you have recorded the issue, assessed the associated risk, addressed or resolved it, within a time frame that you can cross reference to a defined timeline, and validation of the fix. Updates to the recovery plan would also support this.

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.

2505 - Resilient 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
- Secure offsite storage supporting availability requirements
- Regular backup recovery testing

Jargon Buster

Both 2504 Backups and 2505 Resilient Backups emphasise the importance of maintaining data and information backups that are both secure and accessible. However, 2505 introduces additional requirements. It includes all the practices outlined in 2504, such as ensuring backups are accessible, secure, encrypted, and regularly checked for integrity to confirm they are not corrupted. But in addition, 2505 requires storing backups offsite in a secure location away from the primary site, which protects them from local risks such as fires, floods, theft, or other disasters that could compromise onsite backups. It also emphasises the importance of regularly testing the recovery process to ensure that backups can be successfully restored when needed.

2505.1 - (MOD 000534) - (L2-L3)

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, this is laid out in…
Expected Evidence: Your Assessor will want to see your backup policy and procedures. They may also want to see evidence of a backup schedule.

2505.2 - (MOD 000535) - (L2-L3)

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 use...

Expected Evidence: Your Assessor will expect documentation of encryption standards in your policies and evidence of encryption applied to backups (e.g., configuration screenshots or logs).

2505.3 - (MOD 000536) - (L2-L3)

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, this is done with...

Expected Evidence: Your Assessor will want to see logs or reports showing results of integrity validation checks and documentation of the process or tools used for integrity validation.

2505.4 - (MOD 000537) - (L2-L3)

Does the organisation ensure that backups are stored securely off site, where necessary, to support system recovery and meet availability requirements?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have…

Expected Evidence: Your Assessor will want evidence of off-site storage arrangements (e.g., contracts or agreements with storage providers). Or documentation showing that backups are stored off site (e.g., storage location details).

2505.5 - (MOD 000265) - (L2-L3)

Does the organisation conduct regular backup recovery tests to ensure systems and services can be restored in the event of an incident?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last was on [date]

Expected Evidence: your Assessor will want to see recovery test results or reports and documentation of the recovery test process.

2505.6 - (MOD 000538) - (L2-L3)

Does the organisation ensure backup recovery testing is conducted for critical systems at least every 6 months?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our last was on [date]

Expected Evidence: Your Assessor will want to see a schedule of recovery tests showing they are conducted at least every 6 months. Reports or logs from the most recent recovery tests for critical systems will also support you.

2506 - Physical transport of backups

Control Requirement

The Applicant shall protect the physical movement of media containing Data in transit using the following methodologies:

- Store backup media within a secured and locked container prior to transport.
- Utilise a certified backup courier to transport backup drives/tapes.
- Maintain a full chain of custody record.
- Ensure that tracking information is recorded for all drives being transported.
- Implement appropriate cryptographic mechanisms to protect confidentiality.

Jargon Buster

Some organisations still need to move backup media physically, for example, to store backups offsite, support disaster recovery, maintain long-term archives, transfer large volumes of data during a migration, or keep an offline (air gapped) copy to reduce the impact of ransomware.

This control focuses on the security risks associated with physically transporting backup media (rather than the practical logistics). In particular, it considers what happens if the media is lost or stolen or accessed by an unauthorised person, or tampered with while in transit.

This control focuses on backup media being transported outside secure locations. It expects you to protect the transfer, for example, by using locked containers, using a courier contracted and assured to meet your transport security requirements, maintaining a chain-of-custody record, recording tracking information, and protecting confidentiality through encryption. You should also consider any contractual requirements that apply when deciding how to meet this control.

Even if you do not currently transport backup media, you should still have a documented policy or procedure that sets out how you will apply these requirements if physical transport becomes necessary during the certification period.

If your organisation transports other high risk data media (for example to move large datasets during a migration), the same principles represent good practice. However, they are not assessed under this control unless the media being transported is backup media. This control should be considered alongside 2310 (Encryption of removable data) and 2313 (Sanitisation before disposal).

2506.1 - (MOD 000539) - (L2-L3)

When backup media is physically transported outside of secure locations, does the organisation require personnel to:
Available answers (Choose all that apply):

- ☐ Store backup media in a secured and locked container prior to transport
- ☐ Utilise a certified courier for transportation
- ☐ Maintain a full chain of custody record
- ☐ Record tracking information
- ☐ Implement appropriate cryptography
- ☐ None of the above

Example: All of the above. This is covered in our Data Transport policy.

Expected Evidence: Data Transport or other policy showing the requirements applied to staff or external parties. Third parties should follow a Service Level Agreement (SLA) or contract, a certified courier that specifies secure transport requirements may have a log of all criteria for each transport trip made.

2507 - Deny traffic by default at interfaces

Term

Change Advisory Board (CAB)

A Change Advisory Board is a group of people with the right knowledge and experience who review proposed changes to an organisation's systems or processes. Their role is to make sure changes are properly considered and approved, reducing the risk to the business.

Not all organisations will be of sufficient size to have a Change Advisory Board, for those that don't it is expected that the change must be authorised by a sufficiently experienced/qualified appointed person, or persons.

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 your firewall blocks everything unless you have a good reason to allow it, and that someone with the right knowledge has signed off the decision to allow it. Depending on the size and complexity of your organisation you may have a single firewall on your perimeter, or multiple firewalls separating different parts of your network from each other. This control applies to both external and internal firewalls, for both inbound and outbound traffic.

A firewall is a security tool, either a physical device or software, that manages which network traffic is allowed into and out of your systems. Think of it as a security guard at the door. The question this control asks is: is your security guard letting people in by default and only turning away known troublemakers, or are they turning everyone away unless they are on the approved list? This control requires the second approach.

This matters because you cannot predict every threat. If you only block what you already know is bad, you will inevitably leave gaps. A block-by-default approach, opening only what you need, reduces the routes available to unknown threats.

This applies to outbound traffic as well as inbound. If an attacker gains access, unrestricted outbound connections give them a route to communicate back to their own systems or exfiltrate data.

For everyday devices like laptops and desktops, your starting point should be meeting the requirements set out in Cyber Essentials (Control 0001).

Servers are a different matter. A server hosting a business system typically has a fixed, predictable set of network connections it needs. For servers, you should apply strict deny-by-default rules for both inbound and outbound traffic, and allow only a tightly controlled set of required connections. There is rarely a good reason to leave unnecessary network paths open on a server, and doing so can significantly increase risk.

You do not necessarily need a formal Change Advisory Board. Not every organisation will one, and that is fine. The intent of this control is to ensure that an appropriately authorised person makes an informed decision to allow or block a connection, and that the decision is recorded.

In a small organisation, this may simply be the IT manager or the person responsible for your systems. What matters is that the decision is deliberate, based on sufficient understanding of the risk, and documented in a way that can be referenced later.

This simple record does not need to be complicated; An email exchange, a line in a spreadsheet, or a note in a helpdesk ticket are all acceptable ways of showing that a change was considered and approved. The record should capture what changed, why, and who approved it.

Any firewall rule that no longer has a clear business justification should be removed. Regularly reviewing your firewall rules and retiring those that are no longer needed is an important part of meeting this control.

Proportionality

The right approach will vary depending on the size and complexity of your organisation. A small office with a handful of staff and a single broadband router should ensure the firewall is configured to block traffic by default, that any exceptions are documented, and that changes are approved by a named, knowledgeable person. At this level, that may be an appropriate approach for a small or simple organisation.

Larger or more complex organisations should think beyond a single boundary firewall. They would typically be expected to implement network segmentation, potentially with multiple internal firewalls, to enforce the same block-by-default principles between different parts of the network.

This control also shares foundational principles with Zero Trust Architecture, an approach to security where no connection is trusted by default, regardless of where it comes from, even inside your own network. Rather than relying on a single perimeter to keep threats out, Zero Trust Architecture treats every access request as potentially hostile and requires it to be verified. If your organisation has already adopted a higher level of maturity like this approach, you are likely meeting or exceeding the intent of this control.

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

Control Requirement

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

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.

Control Requirement

The Applicant shall check all media containing diagnostic and/or test programs for malicious code prior to use on the organisational network.

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 media before use. (Clearly describe the tools or methods in place, such as antivirus software, endpoint protection tools, or sandboxing, and explain how they ensure the media is safe to use.)
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

Control Requirement

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.

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 - Awareness, Behaviours and Culture

Staff are central to any organisation's ability to operate securely. Therefore, organisations responsible for essential functions should ensure that their employees have the information, knowledge, and skills they need to support the security of networks and information systems.

To be effective any security awareness and training programme needs to recognise and be tailored to reflect the way people really work with security in an organisation, as part of creating a positive security culture.

The people who operate and support essential functions should be provided with all they need to carry out their job while supporting the organisation's cyber security. In line with the design of service protection and policies, you should apply the same people-focussed approach to staff awareness and training.

Training and awareness activities should provide appropriate cyber security skills for the job role based on an understanding of how people really work with the systems, with ongoing reminders and top-up training to maintain skills.

Using a range of approaches to training and awareness can improve understanding and information retention, from briefings, online courses and blogs to simulated cyber attack. You may achieve the widest uptake of training and awareness by accommodating different learning preferences and using various delivery methods.[17]

[17] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b6-staff-awareness-and-training

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.

2601 - Cyber security culture

Control Requirement

The Applicant shall develop and maintain a positive cyber security culture which encourages employees to make information security part of their day-to-day activities and incentivises them for doing so.

Jargon Buster

2601 - Cyber Security Culture is about creating an organisational environment where cyber security is a shared responsibility and part of everyday activities. Leadership plays a key role in fostering this culture by promoting secure behaviours, encouraging adherence to policies, and incentivising employees to prioritise information security in their roles. A positive cyber security culture ensures that employees feel supported and motivated to act securely.

2601.1 - (MOD 000286) - (L2-L3)

Does the organisation's leadership actively support and encourage positive cyber security behaviours, habits and adherence to cyber security policies and procedures?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe how leadership actively promotes and supports positive cyber security behaviours. Include examples of initiatives, recognition or rewards for secure behaviours, and leadership participation in cyber security awareness activities.)

Expected Evidence: Your Assessor will want to see evidence that leadership actively promotes and supports a positive cyber security culture. This may include examples such as leadership communications (e.g., emails, newsletters, or presentations) and incentive programmes that reward employees for demonstrating secure behaviours.

2602 - Cyber security training

Control Requirement

The Applicant shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Applicant shall conduct awareness training at least every 12 months to recognise and respond to the following topics:

- Social engineering and phishing
- Advanced persistent threats
- Suspected breaches
- Suspicious behaviours

A range of approaches to cyber security training, awareness and communications shall be employed and the Applicant shall update the training every 12 months or when there are significant changes to the threat.

Jargon Buster

2602 - Cyber Security Training is about making sure that employees are equipped with the necessary knowledge and skills to handle cyber security threats. This includes providing training on topics like phishing, advanced threats, and breach response.

Training must be conducted at least annually and updated regularly to reflect evolving threats. A variety of methods, such as workshops, e-learning, and simulations, should be used to ensure effective learning. Organisations that process MOD information must be aware of their obligation to report incidents to the Defence Industry Warning, Advisory and Reporting Point (Defence Industry WARP).

2602.1 - (MOD 000287) - (L2-L3)

Does the organisation provide clear and accessible guidance to employees on how to recognise and report security breaches?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe how you provide guidance to employees, such as training materials, quick reference guides, or internal communications. Include details on how this guidance is made accessible, such as via an intranet, posters, or email campaigns.)

Expected Evidence: Your Assessor will want to see examples of the guidance provided to employees, such as training materials, quick reference guides, or screenshots of intranet pages. Evidence of internal communications, like emails or newsletters, may also be required.

2602.2 - (MOD 000546) - (L2-L3)

Does the organisation ensure those that support the operation of Functions and protection of data are appropriately trained in cyber security?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe the process for identifying staff who require training, the topics covered, and how the organisation ensures these individuals complete the training.)

Expected Evidence: Your Assessor will want to see training records for staff, including attendance logs, completion certificates, or reports from training platforms. Policies outlining the requirement for this training may also be requested.

2602.3 - (MOD 000547) - (L2-L3)

Does the organisation ensure staff receive cyber security awareness training upon appointment and at least annually thereafter?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Provide a clear explanation of the process for onboarding new employees with cyber security training, ensuring that all team members participate in annual refresher courses. Include details on how training completion is tracked.)

Expected Evidence: Your Assessor will want to see records of onboarding training for new hires and annual training for all staff. This could include attendance logs, completion certificates, or reports from training systems.

2602.4 - (MOD 000548) - (L2-L3)

Does the organisation's cyber security awareness training ensure relevant staff can recognise and respond to:
Available answers (choose all that apply):

- ☐ Social engineering and phishing
- ☐ Advanced persistent threats
- ☐ Suspected breaches
- ☐ Suspicious behaviours
- ☐ None of the above

Example: Yes, we... (Clearly describe how the organisation makes sure each of your selected topics is covered in training, such as through e-learning modules, workshops, or simulations.)

Expected Evidence: Your Assessor will want to see training materials or course outlines that show these topics are included.

2602.5 - (MOD 000549) - (L2-L3)

Does the organisation update its cyber security training, awareness and communications:

Available answers (Choose all that apply):

- ☐ At least annually
- ☐ When there are significant changes to the threat
- ☐ None of the above

Example: Yes, we... (Clearly describe the process for reviewing and updating training materials, including how the organisation monitors changes in the threat landscape and incorporates them into training.)

Expected Evidence: Your Assessor will want to see evidence of training updates, such as version histories of training materials, meeting minutes from review sessions, or records of updates made in response to new threats.

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.

The NCSC and NPSA have produced guidance on the use and risks of social media.

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.*

2605 - Annual threat focused training feedback

Control Requirement

The Applicant shall conduct practical exercises in awareness training for their organisation that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

Jargon Buster

2605 - Annual Threat-Focused Training Feedback is about ensuring that employees are prepared to handle real-world cyber threats through hands-on, practical exercises.

2605.1 - (MOD 000553) - (L2-L3)

Does the organisation include practical exercises as part of its cyber security awareness training?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we... (Clearly describe how practical exercises are included in your cyber security awareness training. For example, explain the types of exercises conducted, such as phishing simulations or incident response drills, and how they are delivered to staff.)

Expected Evidence: Your Assessor will want to see documentation of the practical exercises conducted, such as phishing simulation reports or incident response drill outlines. They may also request evidence of the planning process for these exercises, such as meeting minutes or email correspondence.

2605.2 - (MOD 000638) - (L2-L3)

Are the organisation's cyber security practical exercises:
Available answers (choose all that apply):

- ☐ Aligned with current organisational threat scenarios
- ☐ Undertaken by staff at least annually
- ☐ Assessed, with feedback provided to participants and supervisors
- ☐ None of the above

Example: Yes, we... (For each selected answer, clearly describe how your organisation ensures the practical exercises meet the stated criteria.)

Expected Evidence: Your Assessor will want to see documentation of exercises aligned with current threats, records of annual participation, and feedback reports provided to participants and supervisors.

27XX Family –Staff and Environment

This family is made up of three areas:
Checks before hiring Staff, whistleblowing and environmental control. Staff are one of the strengths of a business but may also be a point of weakness if the organisation hires a bad actor, it is important that the organisation performs adequate checks before employing staff. Staff moving within the organisation may require additional checks if their new role requires it. An organisation may have mechanisms in place to protect their Data and Function from external threats but these may not be effective against an internal threat. The checks you perform must be adequate for your organisation; they may vary according to the role or responsibility.

The lifecycle of an employee requires organisations to handle joining, moving within, or leaving the organisation. This may require changing their roles, permissions and access to follow least privilege rules, or revoking all access. As part of the security culture within your organisation staff should feel able to report concerns and the organisation should have a whistleblowing process.

The environment the staff work in must also be considered, The Workplace (Health, Safety and Welfare) Regulations mandate that employers ensure the health and safety of their staff. Your organisation must also consider which environmental controls are appropriate to support infrastructure, such as a server room, as well as mechanisms to support those functions like a backup power supply.

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

Control Requirement

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.

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

The DCC scheme is based on whole-organisation resilience, not just an anti-attack checklist. Environmental controls are included because fire, overheating, humidity and power loss can disrupt the same critical people, functions and equipment as a cyber-attack. Protecting the environment they operate in is therefore part of protecting the organisation itself.

This applies wherever your organisation houses staff, equipment or processes that your business-critical operations depend on. This could include a server room, a data centre, or a controlled environment such as a clean room used in manufacturing.

If none of your business-critical operations depend on an environments like these, you must explain your proportionate response to this control with your Assessor.

A note on JSPs. Not all organisations will be required to comply with Joint Service Publications (JSPs), or may even be aware of them. Some Joint Service Publications set requirements for physical environments such as data centres, and these may be included in contracts for certain services. Control 2704 concerns your own organisational resilience and applies regardless of whether any JSP is in your contract. Where separate contractual requirements do exist, they layer on top of this control rather than replace it.

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.

31XX Family –Security Monitoring

An effective monitoring strategy is required so that potential security incidents are discovered and there are appropriate processes in place to assist with a response. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that appropriate action can be taken.

One clear focus of your security monitoring should be the detection of incidents or activity that is likely to have an adverse impact on the network and information systems that support the operation of essential functions. Log data collection, secure storage, analysis tools, understanding your network and information systems that support your essential functions, threat intelligence and personnel skills should all be used to build an effective security monitoring capability.[18]

[18] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-c-detecting-cyber-security-events/principle-c1-security-monitoring

3100 - Security monitoring

Control Requirement

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.

This control does not explicitly require 24/7/365 monitoring however you should consider whether this level of continuous monitoring is appropriate for your organisation if deemed so by your risk assessments. Control 3101 is L1-2 and 3102 is L3, this does not mean you should not attempt to meet 3102 if it appropriate for the risks your organisation faces.

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.

3102 - Continuously monitor security controls

Control Requirement

The Applicant shall establish and document security event monitoring which at a minimum covers the following:

- 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments.
- Tools used for 24x7x365 monitoring and correlation.
- Security events covered.
- Frequency of monitoring.
- Clearly defined roles and responsibilities.
- Escalation matrix.

Jargon Buster

This is a level 3 control (the highest level), so the requirements and expectations are more stringent. Applicants must establish and document security event monitoring for identified information systems, including both production and non-production environments.

This does not mean you must monitor every system you own. Instead, you must identify which systems require monitoring and document the scope and rationale for that decision.

In simple terms you can think of:

- Production environments as your live systems used to deliver your functions day to day.
- Non-production environments as supporting systems used to build, test or maintain live systems.

When deciding what to include, non-production systems will normally be in scope where they contain real data, can connect to or affect production systems, or where compromise would have serious consequences.

For example, development or test environments that use real data, have connectivity to production, or can deploy changes into production would

typically be included. By contrast, a genuinely isolated sandbox with no real data and no route to production may not require the same level of monitoring.

Criticality of non-production

A practical way to judge criticality is to ask whether compromise could:

1. expose sensitive data
2. provide access to production systems (or other systems)
3. enable unauthorised changes to production systems or data

Once you've identified which systems need monitoring, you should also document how that monitoring will operate in practice. It is not enough to define a process, you must be able to demonstrate that it is followed, that alerts trigger correctly, and that relevant events are investigated where appropriate.

This control requires security event monitoring and correlation on a 24/7/365 basis, but it does not necessarily require a 24/7/365 staffed Security Operations Centre (SOC). For some Applicants, it may be sufficient for alerts to trigger and for affected devices to be automatically quarantined to limit the spread of infection or reduce harm.

Once a device has been quarantined and an alert raised, the Applicant may investigate on the next working day, or escalate to an on-call analyst to decide whether immediate investigation and incident response is required. This links to the 41XX incident management controls.

Your solution should be appropriate and proportionate to the risks you face. More critical systems may require faster escalation and a more intensive response, while lower-risk systems may be monitored with a standardised response process.

3102.1 - (MOD 000568) - (L3)

Does the organisation have documented policies, procedures and controls in place (i.e. implemented) for continuous security event monitoring?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is documented in our Security Event Monitoring Policy

Expected Evidence: Policy document(s) showing the policy, procedures and controls. Evidence of implementation may include screenshots of configurations, output of tools and test reports.

3102.2 - (MOD 000571) - (L3)

Does the organisation ensure security event monitoring of all identified systems includes both production and non-production environments?
How do you check that you are monitoring all of the appropriate systems and that monitoring is working?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, when onboarding a system, we determine if it needs to be monitored and the best way to do so. We review monitoring and coverage on a regularly scheduled basis and trigger test alerts to check the effectiveness. Our IT team notify us when a new device/system/network is added to our organisation.

Expected Evidence: Security Event Monitoring Policy, reports on monitoring and results of testing.

3102.3 - (MOD 000569) - (L3)

Which of the following are included in the organisation's security event monitoring procedures?
Available answers (choose multiple):

- ☐ Security events covered
- ☐ Frequency of monitoring
- ☐ Clearly defined roles and responsibilities
- ☐ Escalation matrix
- ☐ Tools used for 24x7x365 monitoring and correlation
- ☐ None of the above

Example: All of the above are included in our monitoring procedures.

Expected Evidence: Policy or process document defining and explaining the security event monitoring procedures, such as a Security Event Monitoring Policy.

3102.4 - (MOD 000570) - (L3)

Does the organisation ensure 24x7x365 security event monitoring of all identified systems?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. Our 24x7x365 SOC monitor alerts. This is detailed as a requirement in our Security Event Monitoring Policy.

Expected Evidence: Policy or process document, reviews of monitoring and assessments.

3102.5 - (MOD 000320) - (L3)

Does the organisation generate alerts for potential security events?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. This is detailed in our Security Event Monitoring Policy.

Expected Evidence: Policy or process document, reviews of monitoring and assessments.

3103 - Securing logs

Control Requirement

The Applicant shall hold logging data securely and grant read access only to accounts with business needs. The Applicant shall protect audit tools from unauthorised access, modification and deletion. Logging data shall be retained and protected from deletion to a documented retention period, after which it shall be deleted.

Jargon Buster

This control focuses on protecting the integrity, confidentiality, and availability of logging data. It's about securing logs to ensure they are tamper-proof and available for analysis.

3103.1 - (MOD 000572) - (L2-L3)

Does the organisation have documented policies, procedures and controls in place for securing logging data?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, requirements for securing logging data is covered in..., which was last updated [date]

Expected Evidence: A copy of the policies, procedures, or controls

3103.2 - (MOD 000573) - (L2-L3)

Does the organisation ensure only authorised individuals with a business need are granted read-only access to logs?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is granted to our SOC analysts.

Expected Evidence: Your Assessor will want to see an access control list and possibly a screenshot or screenshare demonstrating user permissions and the criteria used to determine access (e.g., role-based permissions).

3103.3 - (MOD 000324) - (L2-L3)

Does the organisation protect audit tools from unauthorised access, modification, and deletion?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is done by role-based permissions. Only our SOC analysts have permissions to access the audit tools and only our senior SOC analysts have permission to modify or remove them.

Expected Evidence: Your Assessor will want to see documentation and technical configurations showing access controls, permissions, and protective measures in place for your audit tools.

3103.4 - (MOD 000574) - (L2-L3)

Which of the following does the organisation require and enforce for stored logs?

Available answers (Choose all that apply):

- ☐ A retention period for logs is documented.
- ☐ Logs are protected from deletion during the retention period.
- ☐ Logs are deleted following the retention period.
- ☐ None of the above.

Example: Yes, all of the above. This is detailed in our Monitoring policy.

Expected Evidence: For each selected answer, your Assessor will expect evidence such as: A copy of your log retention policy or procedure. Technical configurations or screenshots showing protections against deletion during the retention period. Evidence of secure deletion processes, such as scripts, tools, or logs showing deletion activities after the retention period. Access control lists or permissions settings for log storage systems.

3104 - Security event triage

Control Requirement

The Applicant shall provide evidence from their monitoring tool of security incidents to verify the reliability of identified and triggered alerts for triage.

Jargon Buster

This control focuses on your triage process. Are you checking alerts to see if they're genuine and deciding which ones to deal with? How reliable are your alerts? Do you test your configuration by deliberately trying to trigger alerts?

This is a very wordy way of asking if you baseline your systems to reduce the false positives (which leads to alert fatigue) and ensure real events are not missed (false negatives) and how do you test it. Baselining involves setting up a clear idea of what "normal" behaviour looks like for a system. Alert fatigue happens when there are too many alerts, especially ones that aren't real issues, causing people to become overwhelmed or stop paying attention, which can lead to missing important alerts. False negatives occur when a monitoring tool fails to catch a real problem or threat, which means critical issues might go unnoticed and unaddressed. Testing your baseline may be done by performing actions which should trigger an alert or actions which should not trigger an alert.

3104.1 - (MOD 000627) - (L2-L3)

Which of the following does the organisation undertake as part of security event triage?

Available answers (Choose all that apply):

- ☐ Review of security alerts generated from events
- ☐ Verifying reliability of identified and triggered alerts
- ☐ Using monitoring tools to identify evidence of security incidents
- ☐ None of the above

Example: Our Security Monitoring policy and processes include all of the above. We baseline any onboarded system or device and review the baseline after system changes. When a false positive alert is identified and verified, we update the baseline.

Expected Evidence: For each selected answer, your Assessor will need to see it documented as a specific step in your event triage process

3105 - Identifying security incidents

Control Requirement

The Applicant shall contextualise alerts with knowledge of the threat and their systems and engage Incident Response when an incident (confirmed or otherwise) is identified.

Jargon Buster

The previous control, 3104, focuses on responding to alerts; 3105 asks for a documented process/technology to add context to those alerts and consider how they may affect your organisation. In order to do this, you should have a threat intelligence feed to provide information on the threats feeding into a centralised monitoring system. You then add context using your in-depth knowledge of your own systems to understand the relevance and potential impact upon your network and systems. Overall, this allows you to determine the relevant and potential impact of an alert which feeds into your incident response process.

3105.1 - (MOD 000575) - (L2-L3)

Does the organisation have documented plans and procedures in place for identifying security incidents?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, our plans and procedures are covered in… It was last updated [date]

Expected Evidence: A copy of the plan or procedure.

3105.2 - (MOD 000576) - (L2-L3)

Does the organisation contextualise alerts with knowledge of the threat and systems when identifying security incidents?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a threat intelligence feed which then allows us to prioritise alerts for threats to our most critical systems.

Expected Evidence: Documents showing process or technology used for adding context to alerts with threat intelligence, logs of ingesting threat intelligence, process document of how this is applied to system knowledge.

3105.3 - (MOD 000577) - (L2-L3)

Does the organisation engage incident response capabilities upon identification of an incident, whether confirmed or unconfirmed?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this is part of our escalation matrix within our SOC.

Expected Evidence: Incident response policy and incident response reports, correspondence or logs showing incident response engagement, configuration settings of threat intelligence feed.

3106 - Monitoring tools and skills

Control Requirement

The Applicant shall ensure that monitoring staff skills, tools and roles, including any that are outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have contextual knowledge of the Functions and requirements for the protection of Data.

Jargon Buster

This is about making sure that the people responsible for monitoring (whether they are in-house or outsourced) have the right skills, tools, knowledge and understanding to do their job effectively.

3106.1 - (MOD 000578) - (L2-L3)

Does the organisation ensure that security monitoring staff have appropriate skills, tools and assigned roles to meet the organisation's:
Available answers (Choose all that apply):

- ☐ Governance requirements
- ☐ Reporting requirements
- ☐ Expected threats
- ☐ Complexities of networks and systems
- ☐ None of the above

Example: Yes, we... (provide a description of the processes, measures, or practices you have in place to meet the selected requirements).

Expected Evidence: Your Assessor will expect to see sample job descriptions, training, policies, documentation showing network complexities and anticipated threats. If the monitoring is outsourced then you should provide details of service level agreements, contract requirements and the third party should provide you with details of how they meet this control.

3106.2 - (MOD 000579) - (L2-L3)

Does the organisation ensure that security monitoring staff possess the contextual knowledge of its Functions and the requirements for the protection of Data?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we provide training on the tooling and network/system complexities when they first start the role and then refresh their knowledge with regular updates.

Expected Evidence: Your Assessor will want to see how you brief your security monitoring staff. This might be covered by onboarding training, role specific training, collaborative workspaces or knowledge management tools.

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. If logs are stored in a cloud service, then the Applicant should configure the service in such a way that loss of the main system/service/tenant will not result in the loss of the audit 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.

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 18 months.

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.

3110 - Monitor alerts/advisories and take action

Control Requirement

The Applicant shall monitor system security alerts and advisories and act in response.

Jargon Buster

This is about monitoring external alerts and advisories (e.g., vendor notifications, threat intelligence) and taking appropriate action. For Level 3 Applicants, Control 1204: Threat Intelligence Capabilities has already addressed the requirement to have a threat intelligence capability. The emphasis of this control is now on the actions taken in response to the alerts.

3110.1 - (MOD 000595) - (L2-L3)

Does the organisation monitor for published alerts and advisories which pertain to the organisation's systems and act in response?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we monitor feeds/alerts/advisories from all of our suppliers. We maintain the list of suppliers and add/remove a supplier from the list when they are onboarded/offboarded.

Expected Evidence: List of feeds, subscription to supplier/vendor notifications.

32XX Family – Proactive Detection

Some cyber-attacks may evade your automated detections and alerting, particularly more sophisticated threats where their ability to evade detection is likely higher. Where this is the case, threat hunting should be leveraged to detect these threats. Threat hunting is the proactive, iterative and human-centric identification of Cyber threats that have evaded existing security controls

Your monitoring and detection teams should be able to proactively hunt for and detect the signs of adverse activity that may have evaded the detection of existing security controls. An organisation performing this at a cadence that matches the risks posed to them is best practice. However, if an organisation is unable to do this but can perform threat hunting on an ad hoc basis, for example in response to a tip off from a government organisation, risk will likely be reduced to some degree.

The exact steps an organisation should follow when performing threat hunting will likely vary between organisations. Threat hunts may also enable your organisation to create automated detections based on the procedure followed during the threat hunt. [19]

[19] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-c-detecting-cyber-security-events/principle-c2-threat-hunting

3200 - Proactive security event discovery

Control Requirement

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

Control Requirement

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.

3202 - Proactive attack discovery

Control Requirement

The Applicant shall implement reasonable and proportionate measures to detect malicious activity affecting, or with the potential to affect, the operation of Functions and protection of Data.

3202.1 - (MOD 000598) - (L2-L3)

Does the organisation ensure proactive detection of malicious attack activity by integrating its event detection, threat monitoring, and incident response capabilities?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we use SIEM and EDR to monitor for events which then feeds into our incident response capability.

Expected Evidence: Policy or process document, or network diagram, showing how the organisation performs threat detection and monitoring. Incident response plan may also show how the elements are integrated.

3202.2 - (MOD 000342) - (L2-L3)

Does the organisation use threat intelligence data to update and refine the scope of its monitoring and attack detection activities?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we ingest threat intelligence feeds to update our detection signatures and direct our detection methods/activities to account for new threats.

Expected Evidence: Policy or process showing how threat intelligence is ingested and used, examples of updating signatures and detection methods/activities.

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

Terms

In this control, "components" refers to hardware, software, and firmware. Applicants are not expected to inspect devices at the level of individual electronic parts (such as resistors or capacitors).

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.

Jargon Buster

Applicants must be able to detect unauthorised components within the scope being assessed for DCC. Detection outside the assessed scope is optional, but may strengthen the Applicant's overall security.

The Applicant must meet this control in a way that is appropriate for their organisation and proportionate to the risks they face. The approach will vary. For example, a small organisation may rely on endpoint management and a software inventory tool, while a larger organisation may combine network access control and asset discovery, with results integrated into a SIEM tool. These examples are not exhaustive-: Applicants should select an approach that is effective for their environment and be able to demonstrate its effectiveness to the Assessor.

This control relates to 1301 (Automated asset discovery), 2415 (Automatically identify and address misconfiguration and unauthorised components) and 2423 (Trusted source repository). This does not mean Applicants must meet all of these controls unless they are required for the level being sought. However, the same tooling and evidence may be

relevant across them. The Applicant should look for components that are unauthorised, unexpected, or present in the wrong environment. Where issues are detected, a proportionate response should be taken.

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.

41XX Family – Incident Response

Incidents will invariably happen. When they do, organisations should be prepared to deal with them, and as far as possible, have mechanisms in place that minimise the impact on the essential function.

The particular mechanisms required should be determined as part of the organisation's overall risk management approach. Examples might include things such as DDoS protection, protected power supply, critical system redundancy, rate-limiting access to data or service commands, critical data backup or manual fail-over processes, or threats to physical premises. Applicants should be aware of NPSA's guidance on Incident Management and NCSC's *The 10 Steps to Cyber Security* which includes a section on Incident Management.

Note: Some cyber-related regulations (e.g. the NIS Directive and DefCon 658) have mandatory reporting requirements around cyber security incidents that have the potential to affect essential functions. Organisations should make sure that they understand any mandatory incident reporting requirements that apply to them, be it regulatory or contractual, and include such requirements in their incident management planning.[20]

[20] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-d/principle-d1-response-and-recovery-planning

4100 - Response and recovery planning

Control Requirement

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.

It is important to note that NCSC recommend organisations maintain a copy of their response and recovery plans in a non-electronic format, such as paper. This ensures that the organisation can effectively respond to an attack even if IT systems are unavailable and electronic versions of the plans cannot be accessed.

NCSC also provide resources such as “exercise in a Box” which provide a range of scenarios to help evaluate and practice organisational response to incidents.

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.

4101 - Response plan

Control Requirement

The Applicant shall have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of business Functions and protection of Data and covers a range of incident scenarios.

It is important to note that NCSC recommend organisations maintain a copy of their response and recovery plans in a non-electronic format, such as paper. This ensures that the organisation can effectively respond to an attack even if IT systems are unavailable and electronic versions of the plans cannot be accessed.

4101.1 - (MOD 000605) - (L2-L3)

Does the organisation have a cyber security incident response plan in place?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have a documented incident response plan.

Expected Evidence: Incident response plan or supporting documentation.

4101.2 - (MOD 000606) - (L2-L3)

Is the organisation's cyber security incident response plan:
Available answers (choose all that apply):

- ☐ Based on risk assessments
- ☐ Maintained and up to date
- ☐ Suitable for a range of potential incident scenarios
- ☐ Tested
- ☐ None of the above

Example: Yes, we update it annually to incorporate updated risk assessments, or more frequently if organisational changes require it. After it has been updated, we test the plan to ensure it works.

Expected Evidence: Policy or documentation showing how the incident response plan is drawn up, maintained, updated and tested.

4101.3 - (MOD 000607) - (L2-L3)

Does the organisation have established procedures for incident response personnel to follow during each stage of its incident response plan?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have our incident response plan, policies and playbooks.

Expected Evidence: Examples of the response plan, policies and playbooks.

4101.4 - (MOD 000608) - (L2-L3)

Is the organisation's incident response plan reviewed at least annually?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We review it annually or if there has been a significant incident (or organisational change) that requires changes to be made.

Expected Evidence: Incident response plan showing version history and any other supporting documentation showing reviews and changes.

4102 - Response and recovery capability

Control Requirement

The Applicant shall have the capability to enact their incident response plan, including effective limitation of impact on the operation of Functions and protection of Data. During an incident, the Applicant shall enact processes and capabilities to provide access to information sources on which to base their response decisions to coordinate incident handling activities with contingency planning activities.

4102.1 - (MOD 000609) - (L2-L3)

Is the organisation's incident response plan endorsed by senior leadership to ensure it can be effectively enacted with the necessary authority during an incident?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. The incident response plan is signed off by the CTO. Authority is delegated to our SOC to raise an incident if certain criteria are met and these are detailed in our incident response policy.

Expected Evidence: Incident response plan or policy detailing authority to raise an incident or other documentation showing this. Senior leadership endorsement may be shown in the policy/process or meeting minutes.

4102.2 - (MOD 000351) - (L2-L3)

During an incident, does the organisation have processes in place to provide access to information needed for incident response decisions and coordination with contingency plans?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. These processes are detailed in our incident response process and associated playbooks.

Expected Evidence: Incident response policy/plan and any supporting evidence.

4103 - Testing and exercising

Control Requirement

The Applicant shall carry out exercises to test response plans at least every 12 months, using past incidents that affected their (and other's) organisation, and scenarios that draw on threat intelligence and risk assessments.

4103.1 - (MOD 000610) - (L2-L3)

Does the organisation conduct exercises at least annually to test its cyber security incident response plans?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We perform annual exercises to test the response plans. We incorporate the last incidents and threat intelligence knowledge of current tactics, techniques and procedures aimed at our industry. This is detailed in our testing policy.

Expected Evidence: Briefs and reports from the exercises and testing showing the history of testing.

4103.2 - (MOD 000611) - (L2-L3)

Does the organisation design its incident response exercises based on:
Available answers (choose all that apply):

- ☐ Past incidents of relevance to the organisation
- ☐ Threat intelligence
- ☐ Risk assessments
- ☐ None of the above

Example: Yes, we incorporate all of the above as detailed in our testing policy.

Expected Evidence: Policy or process showing how exercises scenarios are determined. Briefs and reports from the exercises and testing showing how they have been updated over time to incorporate past events, risk assessments and threat intelligence.

4104 - Incident handling capability

Control Requirement

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.

Organisations handling MOD information, classified data or MOD assets should be aware of their reporting responsibilities (either contractual obligation, or regulatory as detailed in DefCon 658) to MOD Defence Industry WARP, their Prime, or other entities.

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.

4105 - Exfiltration tests

Control Requirement

The Applicant shall conduct data exfiltration tests at the network boundaries at least every 12 months. These tests must be conducted against both authorised and covert channels.

Jargon Buster

Data exfiltration is commonly known as data theft. It is the intentional, unauthorised, usually covert transfer of data from a computer or other device. You should perform tests to see if unauthorised data can be sent from your company to the outside world. An authorised channel is one which is allowed (such as email, DNS or HTML) but is not intended to be used for that data. A covert channel is one by which you may not expect any data to be sent, or an authorised channel being used in a way it was not intended e.g. DNS data exfiltration, protocol header abuse or steganography. Data Loss Prevention (DLP) technology may detect some exfiltration attempts but if an attacker uses a covert channel that is not monitored by DLP then DLP will not detect it.

This control may overlap with 2320 (DLP) and 2403 (Penetration Testing), these controls serve different purposes and should be viewed as complimentary. Applicants should design exfiltration testing in a proportionate, risk-based way that reflects their environment and threat model.As technology and exfiltration methods evolve, Applicants should stay aware of emerging risks and update their testing accordingly. Penetration tests often include checks for data exfiltration and may highlight channels not covered by DLP. The intent of control 4105 is to provide assurance that your exfiltration defences can detect or prevent realistic exfiltration techniques in practice.

4105.1 - (MOD 000355) - (L2-L3)

Does the organisation conduct data exfiltration tests at the network boundaries at least annually?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we run our own tests twice a year, and our annual externally supplied penetration test also includes testing for data exfiltration.

Expected Evidence: Policy showing frequency of testing, reports showing testing process and results or other supporting documents.

4105.2 - (MOD 000614) - (L2-L3)

Do data exfiltration tests at network boundaries assess both authorised and covert channels?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we test both authorised and covert channels. The parameters of the testing are detailed in our testing policy.

Expected Evidence: Testing policy or other documentation showing parameters of how the testing is to be performed and channels chosen.

4105.3 - (MOD 000615) - (L2-L3)

Are data exfiltration tests at network boundaries used to test and train incident response procedures?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. If the testing finds a successful exfiltration technique, we then update our policies and procedures to take the technique into account. We also check our logs to see if the techniques have been used within our network.

Expected Evidence: Policy or process documentation showing version history and how changes have been implemented following data exfiltration tests.

4106 - Attempted unauthorised connections from staff

Control Requirement

The Applicant shall audit the identity of internal users associated with denied communications.

Jargon Buster

The intent of Control 4106 is to ensure you routinely record and review who (or what) is responsible for denied communication attempts, whether internal or external. Such communication attempts may originate from a device, process or service account, and may not initially map to a named user account.

For example, an internal user repeatedly attempting to access systems or data they are not authorised to access may indicate an insider threat (e.g. a payroll user attempting to access restricted information unrelated to their role). Similarly, unexpected activity from a device, process, or service account may indicate compromise, for example, a hijacked account attempting lateral movement, data exfiltration, or an infected device attempting to connect to an attacker-controlled command-and-control server.

In practice, your logging and review process should enable you to attribute each denied connection to a specific internal user account (where applicable). You should also review these records periodically to identify suspicious behaviour, policy breaches, misconfigurations, persistent malicious activity, or areas where additional training is needed.

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.

42XX Family – Recovery and Improvements

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those function(s) where necessary.

If an incident does occur, it is important your organisation learns lessons as to why it happened and, where appropriate, take steps to prevent the issue from reoccurring. The aim should be to address the root cause or to identify systemic problems, rather than to fix a very narrow issue. For example, to address the organisation's overall patch management process, rather than to just apply a single missing patch.[21]

[21] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-d/principle-d2-lessons-learned

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).

4201 - Business Continuity Risk Assessments

Term

A Business Continuity Plan (BCP) outlines a range of scenarios that could impact the business such as fire, flood, cyber attack and the steps the business will take in each scenario to maintain or restore normal operations. These plans should be prepared in advance and may also include precautionary measures to mitigate potential risks.

Control Requirement

The Applicant shall perform Business Continuity Risk Assessments to determine relevant risks, threats, and likelihood & impact of a service outage or Data Breach. The Applicant shall record the output of these Risk Assessments within a risk register along with the required controls and/or procedures to mitigate or remove the risk and/or threat.

4201.1 - (MOD 000619) - (L2-L3)

Does the organisation conduct Business Continuity Risk Assessments?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we perform annual risk assessments to identify changes to existing risks and how to mitigate their impact. If a new risk develops that is outside the annual cycle, then this is added to the risk register along with required mitigations.

Expected Evidence: Risk register/assessments, policy or process showing how risks are identified, assessed for likelihood and impact and any actions required to mitigate or remove the risk.

4201.2 - (MOD 000620) - (L2-L3)

Do the Business Continuity Risk Assessments include an assessment of:
Available answers (choose all that apply):

- ☐ Threats
- ☐ Impacts of service outage/breach
- ☐ Likelihood of service outage/breach
- ☐ Risks
- ☐ Suitability of existing recovery plans
- ☐ None of the above

Example: All of the above.

Expected Evidence: Risk register or other evidence of assessments.

4201.3 - (MOD 000621) - (L2-L3)

Does the organisation record business continuity risks in a risk register and monitor the improvements needed to mitigate those risks?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, these are recorded in our risk register.

Expected Evidence: Risk register or other document/evidence.

4202 - Operation resilience for equipment

Term

Redundant networking and telecommunication systems refers to systems you would use should your main systems be unavailable, be this from cyber-attacks or technical failures. These systems may refer to those within your control (e.g. servers with a fail over datacentre) or those outside your control such as external phone/internet lines.

Control Requirement

The Applicant shall assess the requirement for redundant networking and telecommunication systems to protect Functions and Data. Where required, the Applicant shall implement and protect these systems.

Jargon Buster

This control is about assessing what systems/policies you have in place to describe how you would react should a service or component fail. It is focussed on how you would be able to maintain your business operations should something go wrong.

4202.1 - (MOD 000623) - (L3)

Does the organisation assess the need for redundant networking and telecommunications systems to protect Functions and Data?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we assess the need as part of our annual review of risks. If new technology/networking equipment/devices are implemented, then we assess the risks and add it to the register as part of onboarding.

Expected Evidence: Risk register, or other evidence, showing the assessment of new risks

4202.2 - (MOD 000624) - (L3)

Does the organisation implement redundant networking and telecommunication systems where necessary?
Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we have redundant networking designed and implemented as per our network diagram. Our landline systems are backed up by mobile alternatives.

Expected Evidence: Network diagram or other evidence of implementation.