CYBER RESILIENCE FRAMEWORK

V1.2

Please send all comments, questions or feedback to cyberresilience@gov.scot

CONTENTS

INTRODUCTION AND CONTEXT

1. This document sets out the Scottish Public Sector Cyber Resilience Framework. The Framework is intended for all Scottish public sector organisations, to support them to improve their cyber resilience and to comply with a range of legislative, regulatory, policy and audit requirements in respect of cyber security.

2. The requirements set out in the Framework are expected to be formally incorporated into the Scottish Public Finance Manual and/or supporting guidance.

3. Public sector organisations are encouraged to familiarise themselves and begin working to the Framework. Timescales for implementation and attainment of the Target or Advanced Stages will depend on organisational priorities and external regulatory requirements, but organisations are encouraged to aim to achieve implementation that best aligns with their risk appetites and organisational circumstances as soon as practicable.

4. The Public Sector Action Plan on Cyber Resilience 2017 included a commitment to develop the Framework and the Strategic Framework for a Cyber Resilient Scotland builds on this with a commitment to review this document every two years. Requests from the Scottish Government for monitoring and evaluation information should be expected annually.

Aims

5. The Scottish Public Sector Action Plan on Cyber Resilience 2017 set out a commitment to develop a **Scottish Public Sector Cyber Resilience Framework**. The key aim of this Framework is to:

   - Provide a **common, effective way** for Scottish public sector organisations to assess their cyber resilience arrangements, identify areas of strength and weakness, gain reasonable confidence that they are adhering to minimum cyber resilience requirements, and take decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.

6. In doing so, the Framework seeks to:

   - Align with key wider cyber-related requirements under the General Data Protection Regulation (GDPR), the Security of Network and Information Systems (NIS) Directive and other standards;

   - As far as possible, minimise any additional burdens on Scottish public sector organisations, including by making clear how the Framework relates to existing standards or requirements, and taking account of these when providing guidance on compliance;

   - Provide a clear basis for internal and external audit and inspection activity, promoting greater consistency in the areas and issues covered by audit and inspection bodies when assessing Scottish public sector organisations; and

- Help to provide clarity and assurance to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place across the Scottish public sector and its individual subsectors.

Relationship to individual standards and requirements

7. A key feature of the framework is its development on the basis of, and mapping to, existing "core" standards and requirements that generally apply to the Scottish public sector. **Annex A** provides a detailed mapping of the different standards that have been analysed to produce this framework. **Annex B** collates the key reference standards, to facilitate easy lookup by practitioners.

8. The framework is effectively intended to represent the entirety of the various requirements encompassed in these diverse standards in a single source document. If an organisation is already required to comply with these diverse requirements (or opts to do so as a matter of good practice), **there should be nothing new or additional in the Framework** – the main difference is that they may now rely on a single source document to gain reasonable confidence that they are achieving compliance across the piece.

9. The Framework, in combination with **Annexes A and B**, facilitates direct reference to individual standards where organisations wish or need to verify with greater confidence that they are in compliance with those individual standards. This document includes hyperlinks that can be used to jump from the framework requirements to the wording in the original source standards/guidance.

10. The development process for the Framework was designed not to take a single standard as its primary reference point. This has the benefit of increasing the Framework's flexibility, permitting further development and incorporation of other standards based on feedback from Scottish public sector organisations over time.

11. In respect of the security categories identified under the Framework, while common phrases and terms are employed across the categories of many of the core individual standards and guidelines, these do not always necessarily correspond to the same meaning or control requirement. Where individual standards are highly prescriptive, the binary compliant/non-compliant analysis is straightforward. However, most standards are written generically, requiring a level of interpretation by the organisation as to the applicability of the criteria and the appropriateness of any solution. A level of interpretation when mapping equivalency has thus had to be employed.

12. The Framework and concept self-assessment tool have benefited from feedback from a range of UK Government and Scottish public sector partners, including NIS Competent Authorities and the Cyber Catalyst organisations. Officials in the UK Cabinet Office PSN team have confirmed that relevant Scottish public sector organisations adhering to the framework, and applying it to appropriately scoped network arrangements, can have reasonable confidence that they are likely to be in compliance with the **Public Services Network (PSN) Code of Connection**. By also working towards compliance with the HMG Minimum Cyber Security Standard [1](which forms part of the Target stage of the Framework),

[1] https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

relevant organisations will be putting themselves in a strong position to progress away from PSN requirements when there is a need to do so.

13. Ultimately, compliance with individual standards will often be subject to individual assessments and audit. However, having a single source framework that provides reasonable confidence across a range of compliance requirements has been welcomed by Scottish public sector organisations as a positive step forward, and is expected to assist with discussions around future convergence and alignment of different standards (which is a key goal of the Scottish Government).

14. The implementation of the NIS Directive for Operators of Essential Services necessitated separate requirements for public sector organisations operating in the devolved **health** and **water** sectors. Organisations in these sectors should contact their relevant competent authority for further information on the requirements for them. From 2022/2023 onwards the health sector in Scotland will adopt the Scottish Public Sector Cyber Resilience Framework as a direct replacement for the current Information Security Policy Framework.

Keeping the Framework up to date

15. Cyber Resilience is a fast-moving area, and standards are frequently updated or amended. The Framework will be reviewed periodically in response to any significant developments with the core cyber standards. This will be reflected in version control for the document and communicated to relevant public sector organisations.

Concept self-assessment tool

16. This Framework is accompanied by a concept self-assessment tool, available here. This concept tool is intended for use by public sector organisations in combination with the Framework, to help them identify key areas of strength and weakness in their current cyber resilience arrangements, communicate these to senior decision-makers, and take action to address them accordingly. The tool has been designed to produce a "dashboard" that can be shared with senior decision-makers, audit bodies, etc. to assist decision-making around cyber resilience issues.

17. The separate user guide (available here[2]) provides further information on how to use the concept self-assessment tool in combination with this framework document.

18. This is intended as a first step towards the provision of a tool that will meet the needs of Scottish public sector organisations. In line with feedback received, it is intended that future iterations of the tool will incorporate greater automation and burden-reduction measures.

Who are the Framework and Self-assessment Tool intended for?

19. The Framework and concept self-assessment tool are intended for use by a range of key individuals within Scottish public sector organisations, including (but not limited to):

[2] https://www.gov.scot/publications/cyber-resilience-framework

- **Cyber security practitioners** – in particular, the framework document and reference lookup document are intended to assist them to ensure they have covered all key requirements from core standards, without the requirement to examine every source document or standard in detail (unless specific reporting requirements attach to those source standards, in which case the framework reference document facilitates direct read across to the specific requirements of the source standards). The concept self-assessment tool should assist them in presenting to senior levels on areas of strength and concern, engaging in benchmarking discussions, and highlighting areas where additional investment or resource are required.

- **Senior Risk Owners and Boards** – both the framework document and the concept self-assessment tool are intended to help senior risk owners with responsibility for cyber risks to identify areas of potential compliance/non-compliance against a range of different standards or requirements, identify areas of strength and weakness in organisational cyber resilience, benchmark against other organisations within and across parts of the Scottish public sector, and highlight areas where greater investment or resource may be required.

- **Audit and inspection bodies** – we are in discussion with Scottish public sector audit and inspection bodies about the potential for them to align their cyber audit and inspection activities with the final framework. Individual organisations contracting with private sector audit organisations may also wish to ask that they align their approach with the framework. This is intended to help promote greater consistency in the audit demands made of Scottish public sector organisations.

- **Central coordinating bodies, competent authorities, etc.** – the framework and the concept self-assessment tool are intended to help generate the types of common "dashboard" reports that could be requested by the Scottish Government, competent authorities and other central coordinating or representative/membership bodies (such as the Local Government Digital Office, APUC, HEFESTIS, NSS, etc.) with an interest in understanding areas of strength and weakness in cyber resilience in the Scottish public sector, with a view to targeting central support and activity appropriately.

SECTION 1 – FRAMEWORK OVERVIEW

This section provides information about the cyber resilience guidance and standards that make up the Framework, and an explanation of how the Framework has been developed. It is most likely to be of use to readers with specialist cyber resilience knowledge. Board/executive-level individuals with responsibility for cyber resilience are also encouraged to use this section to develop their understanding of the Framework and the various standards that can be used to measure their organisational progress.

Core standards

1. The contents of the Scottish Public Sector Cyber Resilience Framework are drawn from or aligned with the following "core" requirements that currently apply to Scottish public sector organisations:

   - The Scottish Public Sector Action Plan (including Cyber Essentials/Plus (CE/+)
   - The NCSC's 10 Steps to Cyber Security
   - NCSC and ICO guidance on technical security outcomes under the General Data Protection Regulations (GDPR)[3]
   - UK Cabinet Office Public Sector Network Code of Connection requirements and IT Health Check (PSN – ITHC)
   - Payment Card Industry Data Security Standards (PCI-DSS)
   - HMG Security Policy Framework Minimum Cyber Security Standard (HMG-SPF)
   - Security of Network and Information Systems (NIS) Directive – NCSC Cyber Assurance Framework (NIS-CAF)
   - ISO 27001:2013[4] (alignment with requirements)

   These standards were selected on the basis of criteria including how widespread their use is currently in the Scottish public sector, whether their application is required by law or regulation, and/or whether they have been endorsed or produced by the NCSC. The fact that many of these standards are in

[3] As implemented in the UK Data Protection Act 2018.

[4] Note that BS EN ISO/IEC 27001:2017 is a modest revision restricted to Clause 6.1.3 and Annex A clause 8.1. Clause 6.1.3 was a formatting adjustment, separating the required content for a Statement of Applicability from the main paragraph into separated bullets. A.8.1.1 (Inventory of Assets) replaces the control's objective text from: *"Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained."* to: *"Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained."* Neither impact upon the CRF categories. Moreover, certification against the 2017 revision is not possible; all certifications remain against 27001:2013. To quote BSI *"This is not a change from ISO/IEC, it is a regional update that just reflects the acceptance by CEN/Cenelec and has no other modifications requiring your actions. We therefore have no current plans to update certificates to the 2017 version so you will continue to receive an ISO/IEC 27001:2013 certificate at this stage."*

widespread use in the private and third sectors is also expected to help with broader efforts to align cyber resilience practice across these sectors in Scotland.

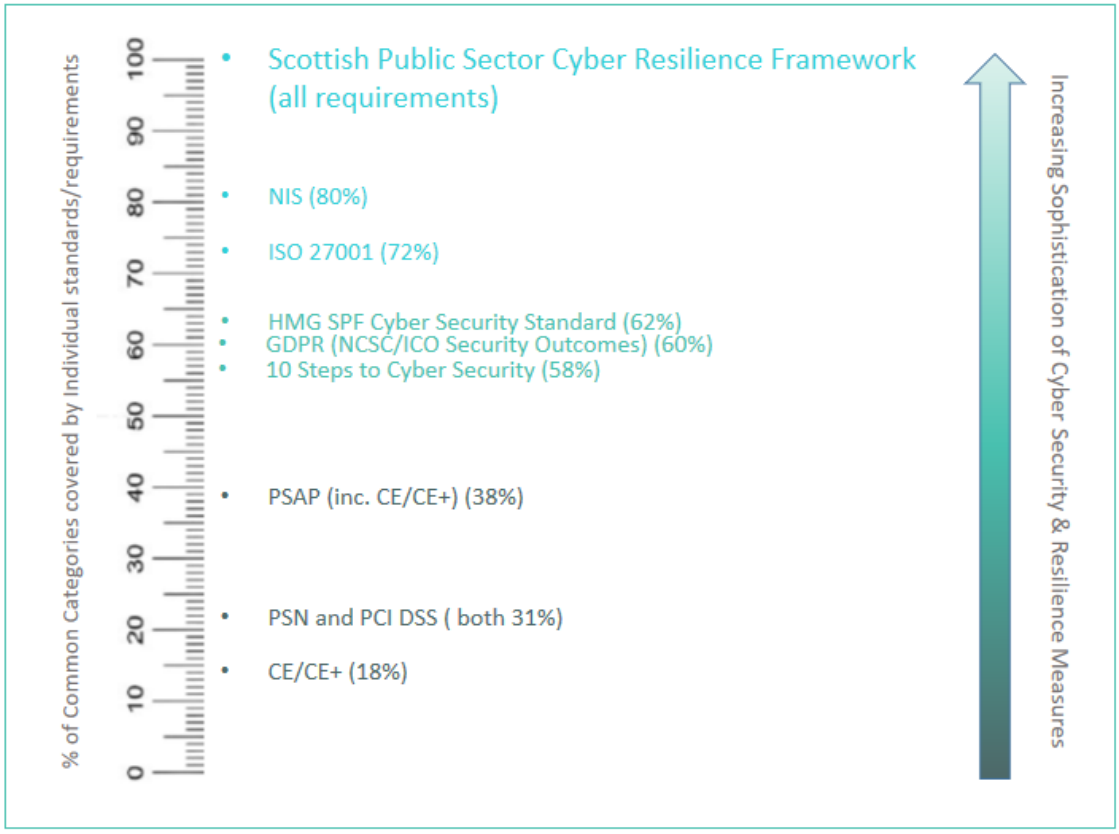
The relevant requirements of the Digital First standard have also been included in the mapping at Annex A.

2. No specific standard was favoured when undertaking the analysis to develop the Framework. This approach was intended to avoid distorting the resultant model towards a particular framework or standard, to ensure the creation of a flexible model that can be developed in the future (as standards change over time or new frameworks become the preferred option for public sector organisations).

3. The resulting Framework effectively represents "100%" of the requirements that apply to Scottish public sector organisations under these combined "core" standards or requirements. It is important to note that, while some individual standards (e.g. NIS and ISO27001) are more comprehensive than others, no single standard incorporates the full 100% of requirements represented by the Framework. This is because the various standards were developed at different times and for a range of purposes – this should not be taken as meaning that individual standards are not fit for the purposes for which they have been developed.

4. It is also important to understand that there is no expectation that an organisation will meet 100% of the requirements of the Framework, or achieve an "end state". This is because cyber resilience is a process of continuous improvement based on evolving risks and responses.

5. The figure below sets out the extent to which individual standards encompass the full body of requirements represented by the Framework.



Domains, Categories and Sub-Categories

6. The Framework has extracted **4 overarching domains** and **17 common categories of security controls and requirements** from the core standards. The 4 overarching domains align closely with those under frameworks such as the NCSC's NIS Technical Guidance and the US NIST cybersecurity framework.

7. The 4 overarching domains and their related categories are:

- **Domain 1: MANAGE Security Risk**: This domain covers the organisational structures, policies and processes necessary to understand, assess and systematically manage security risks to Scottish public sector organisations' network and information systems and essential services. The security control categories under this domain cover:
  - Organisational Governance
  - Risk Management
  - Supplier Management
  - Asset Management
- **Domain 2: PROTECT against cyber-attack**: This domain covers the requirement for proportionate security measures to be in place to protect Scottish public sector organisations (and their essential services and systems) from cyber-attack. The security control categories under this domain cover:

- Information security management
- Physical/building security
- Operational security
- Environmental Security
- System Management
- Services Resilience
- Media Management
- Access Control
- People
- Network Security

- **Domain 3: DETECT cyber security events**: This domain covers measures to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, Scottish public sector organisations (and their essential services and systems). The security control categories under this domain cover:

  - Incident detection

- **Domain 4: RESPOND and RECOVER**: This domain covers measures to minimise the impact of a cyber security incident on Scottish public sector organisations (and their essential services and systems), including the restoration of services where necessary. The security control categories under this domain cover:

  - Incident management
  - Business continuity

8. Brigaded under each domain and security category there are specific sub-categories of control. The tables on the following pages summarise the contents of the Framework.

MANAGE		
ORGANISATIONAL GOVERNANCE	**RISK MANAGEMENT**	**ASSET MANAGEMENT**
• Governance framework • Leadership & responsibility: - SMT - Board • Adoption of assurance standards • Information Asset Register • Audit/assurance compliance	• Risk management policy & process • Cyber/Information Risk Assessment • Risk treatment & tolerance • Risk governance: - Risk assurance & management - Risk register review - Board responsibility - Risk training & culture	• Hardware assets register & management • Software assets register & management • Infrastructure management
SUPPLIER MANAGEMENT		
• Supply chain security assurance & management • Roles & responsibilities defined • Access control • Security in system procurements		

PROTECT

INFORMATION SECURITY MANAGEMENT

- Security policy & processes
- Lifecycle management
- Storage:
  - cloud/3rd party
  - on premise
- Information/data classification
- Information assets register
- Information/data transfer controls

SERVICES RESILIENCE

ACCESS CONTROL

- Account management
- Identity authentication
  - Password policy
  - Multi factor authentication
- Privilege management
- Administrator account management

MEDIA MANAGEMENT

- Storage media management:
  - Mobile media/devices
- Cryptography
- Remote wipe capability

ENVIRONMENTAL SECURITY

- Equipment location
- Power resilience

PHYSICAL/BUILDING SECURITY

- Access control
- Internal security

SYSTEM MANAGEMENT

- Secure configuration
- Secure design/development
- Change control procedures
- System Testing

PEOPLE

- Prior to employment:
  - Security screening
  - T&C
- During employment:
  - induction
  - security roles & responsibilities
  - acceptable use policy
  - disciplinary procedures
- Staff training & awareness culture
- Staff skills assessment:
  - Board
  - SMT
  - Staff
  - Interim & contractor

OPERATIONAL SECURITY

- Malware policies & protection:
  - AV screening
  - Media scanning
  - File scanning
- Email security
- Application security
- Vulnerability management & scanning:
  - Executables prevention
  - Peripheral device management
- Data exfiltration monitoring
- Software supported & updated
- Web site screening
- Browser management
- Monitor/audit user activity
- Disabled auto-run

NETWORK SECURITY

- Patch management
- Device management
- Content screening
- Internal segregation
- Wireless security
- Boundary/Firewall management
- Administrator control
- Error message management
- Penetration testing
- IP & DNS management

DETECT		
INCIDENT DETECTION		
• Detection capability • Security Monitoring		

RESPOND & RECOVER		
INCIDENT MANAGEMENT	**BUSINESS CONTINUITY**	
• Incident response protocol • Incident reporting procedure • Staff training & testing • Post-incident review & learning	• Data recovery capability • Back up policies & procedures • Disaster recovery policies & procedures • BC/DR testing policies & procedures • Data Loss impact assessments • BC contingency plan	

Progression stages

9. Within and across these 4 domains and 17 categories, the framework sets out **3 progression stages**. These represent progressive levels of sophistication so that, within each domain and category, public sector organisations are either required (e.g. by legislation) or can opt to implement basic, intermediate and more advanced sets of controls according to their sector, risk appetite, etc.

10. The progression stages have been designed to encompass the requirements of a range of core standards so that, by working to a specific progression stage, public sector organisations can achieve reasonable confidence that their cyber resilience arrangements are aligned with the requirements of those individual core standards.

11. The progression stages, and the core standards they encompass, are as follows:

- **Initial baseline**: This is the progression stage that **all Scottish public sector organisations should have achieved by end October 2018**. It encompasses the requirements of the **Scottish Public Sector Action Plan on Cyber Resilience** (representing 35% of the full Framework requirements), which itself encompasses a requirement to have independent assurance of the critical technical controls set out in the **Cyber Essentials** standard (representing 12% of the full Framework requirements).

  If implemented appropriately, the requirements set out at the Initial Baseline stage should help mitigate against many of the most common internet-borne cyber threats.

- **Target:** This is the progression stage beyond the initial baseline stage that **all Scottish public sector organisations** will be required or encouraged to achieve, on a risk-based and proportionate basis. It is effectively intended to be the new "baseline" for public sector organisations. It encompasses the combined additional (i.e. beyond the initial baseline stage) requirements of:

  - **PSN and IT Health Check requirements** (representing 31% of the full Framework requirements), which the Scottish Government, local authorities and other public sector organisations are required to comply with in respect of those parts of their networks that connect to the UK Public Service Network;

  - **GDPR Security Outcomes** (representing 60% of the full Framework requirements). All public sector organisations processing personal data are legally required to comply with GDPR, and the Security Outcomes represent authoritative guidance from the NCSC and ICO on what technical protections should apply to personal data;

    It is important to note that GDPR requirements go wider than those covered by the NCSC/ICO Guidance, which focus only on the technical security outcomes that should apply to personal data.

  - **10 Steps to Cyber Security** (representing 58% of the full Framework requirements). These guidelines from the NCSC represent a more holistic approach to Cyber Security, intended for larger organisations or those likely to be at greater risk from cyber crime.

  - **HMG Minimum Cyber Security Standard** (representing 62% of the full Framework requirements). This standard published by the UK Government sets out the minimum standards that UK Government Departments are expected to adhere to and exceed wherever possible. While it does not currently have direct applicability to Scottish public sector organisations, it represents a standard of good practice for the public sector that Scottish public sector organisations should have regard to, including in view of the potential for its applicability to be extended in the future.

  - **Payment Card Industry Data Security Standards (PCI DSS)** (representing 31% of the full Framework requirements). These are information security standards that apply to the processing of payment card data. They set the operational and technical requirements for organizations accepting or processing payment transactions, which include Scottish public sector organisations that transact with the public.

  The requirements set out at the Target stage, if met, should generally help Scottish public sector organisations mitigate against more technically capable cyber attacks.

- **Advanced:** This is the progression stage that **Scottish public sector organisations facing the most advanced cyber or network and information security threats**, or **those providing the most essential public services**, will be required or encouraged to meet on a risk-based and proportionate basis.

The advanced stage also represents a pathway "beyond compliance" for those public bodies that wish to move beyond the requirements of the target progression stage in specific areas, making clear what more can be done by Scottish public sector organisations that wish to become exemplars in the area of cyber resilience, or that wish to strengthen specific aspects of their cyber resilience arrangements.

It is intended to encompass the combined additional (i.e. beyond the initial baseline and target stages) requirements of:

- **The Security of Network and Information Systems Directive - Cyber Assessment Framework (NIS-CAF)** (representing 80% of the full Framework requirements). The NIS Technical Guidance and Cyber Assessment Framework, published by the NCSC, constitute a framework for all organisations deemed by the NIS Competent Authorities to be 'Operators of Essential Services'. These bodies are legally required to comply with the EU NIS Directive (as enacted in regulations by the UK Government). Scotland's devolved health and water sectors are legally required to comply with the NIS Directive.

- **ISO 27001** (representing 72% of the full Framework requirements). ISO27001 is an international information security standard, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. A number of Scottish public sector organisations already align their information security arrangements with the requirements of ISO27001.

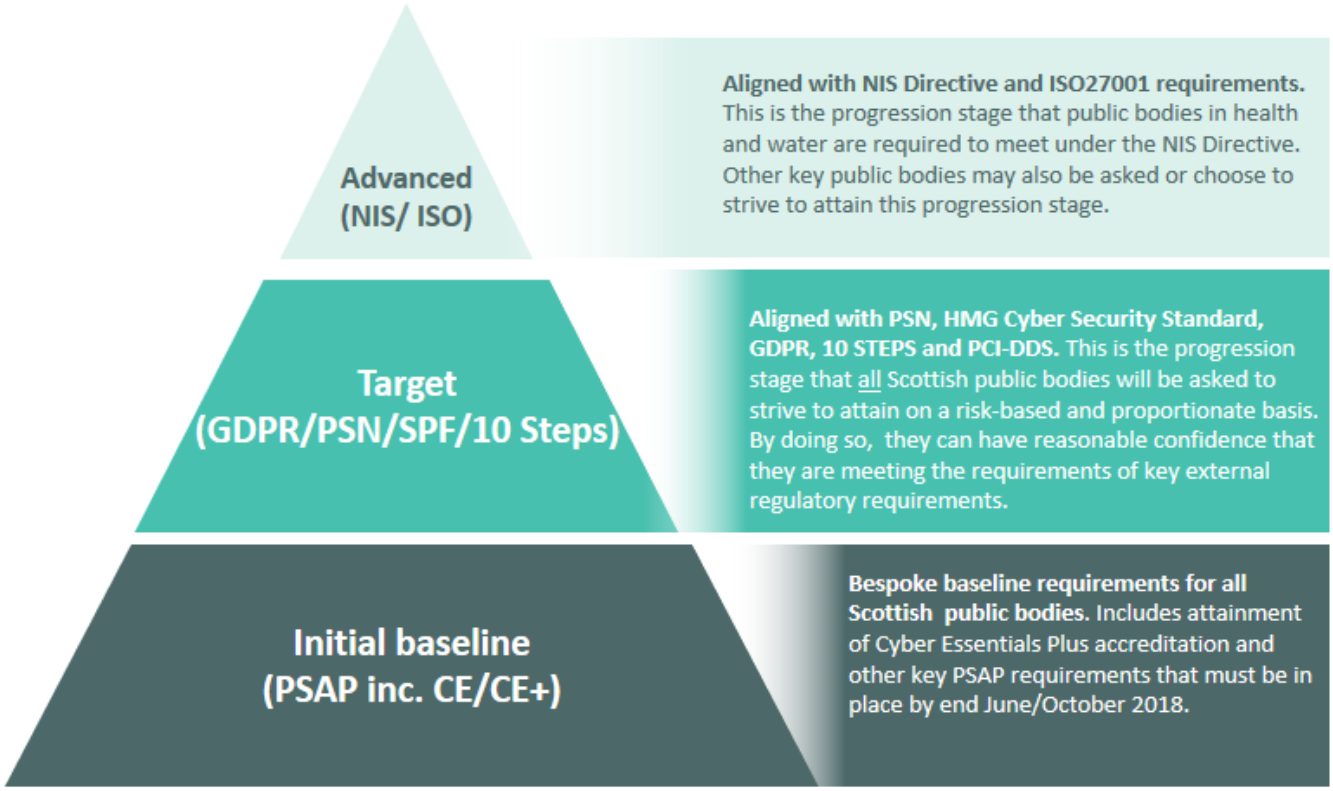
The requirements set out at the Advanced stage, if met, should generally help mitigate against more advanced persistent threats of the type that Scottish public sector organisations delivering the most essential services, or processing the most sensitive or valuable data, might reasonably be expected to face.

12. It should be noted that specific elements of the individual standards that form the target and advanced stages may be covered off at lower progression stages. For example, by meeting the target stage, a public sector organisation will already have met some of the specific requirements of the NIS Directive or ISO27001. The Advanced stage sets out the additional requirements in order to comply with all of the requirements of the NIS Directive or ISO27001.

13. Different progression stages of the framework represent less "sophisticated" or extensive coverage of the 4 domains. For example, a public body operating to the target stage of the framework will be doing less, to less sophisticated standards, than a public body working to the advanced stage.

Framework diagrams

14. The following figures represent the overarching "shape" of the Framework.


Advanced
(NIS/ ISO)
Aligned with NIS Directive and ISO27001 requirements. This is the progression stage that public bodies in health and water are required to meet under the NIS Directive. Other key public bodies may also be asked or choose to strive to attain this progression stage.
Target
(GDPR/PSN/SPF/10 Steps)
Aligned with PSN, HMG Cyber Security Standard, GDPR, 10 STEPS and PCI-DDS. This is the progression stage that all Scottish public bodies will be asked to strive to attain on a risk-based and proportionate basis. By doing so, they can have reasonable confidence that they are meeting the requirements of key external regulatory requirements.
Initial baseline
(PSAP inc. CE/CE+)
Bespoke baseline requirements for all Scottish public bodies. Includes attainment of Cyber Essentials Plus accreditation and other key PSAP requirements that must be in place by end June/October 2018.

	Manage				Detect									Respond	Recover	
	Organisational Governance	Risk Management	Supplier Management	Asset Management	Information Security Mgt.	People	Service resilience	Access control	Media management	Environmental security	Physical security	System management	Operational security	Network security	Incident detection	Incident management	Business continuity
Advanced (NIS/ ISO)	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓
Target (GDPR/PSN /SPF/10 Steps/PCI)	✓✓✓	✓✓✓	✓	✓	✓✓✓	✓		✓✓✓	✓✓			✓✓	✓✓	✓✓✓	✓✓	✓✓✓	✓✓
Initial baseline (PSAP inc. CE/CE+)	✓✓✓	✓✓✓	✓	✓		✓		✓✓✓				✓	✓✓	✓		✓✓	

Legend: ✓ = <50% ✓✓ = 50-75% ✓✓✓ = >75% of full requirements of Framework

Approach to risk and proportionality

15. The Scottish Government is clear that the Framework should be implemented by public sector organisations on a **risk-based and proportionate basis**. In practice this means:

- Where organisations are legally or otherwise required to comply with elements of the framework (e.g. because they are Operators of Essential Services under the NIS Directive, because they handle personal data, or because they connect to the PSN), they must continue to do so.

- In that context, organisations should consider selecting and working to the progression stage of the Framework that is likely to offer reasonable confidence that:

    - legal or other obligatory requirements are met; and

    - the threats and risks they are likely to face in view of their sector, their profile, the data they handle and the services they offer are appropriately mitigated.

- It is open to organisations to take a decision that they will not meet the requirements of specific control categories under the progression stages they are working to, e.g. because they judge it to be unnecessary or disproportionate to do so. In these cases, organisations should ensure they document clearly why they have taken this decision. This will be particularly important given the intention to align Scottish public sector audit and inspection activity with the framework, and to incorporate compliance with the Framework into the Scottish Public Finance Manual and other key mechanisms.

SECTION 2 – HOW TO USE THE FRAMEWORK

This section provides simple advice on how to use the Framework in conjunction with the concept self-assessment tool and other available support products. It is for use by any person with responsibility for implementing the Framework in a public sector organisation.

Step 1: Board buy-in and use of NCSC Board Toolkit

1. The Framework and the outputs of the concept self-assessment tool have been designed to help ensure that senior decision-makers in public sector organisations can identify areas of strength and weakness in organisational cyber resilience, benchmark against other organisations within and across parts of the Scottish public sector, and highlight areas where greater focus, investment or resource may be required. The Framework contains key requirements around **organisational governance**, which are fundamental to effective management of cyber risks. As a first step, **ensure that these basic arrangements are in place to allow you to use the Framework effectively.**

2. It is vital that Boards/executive teams understand that the cyber risk is a business risk – it has the potential to have a significant impact on an organisation's ability to deliver its duties and objectives in respect of public services, and fulfil to its obligations to staff and citizens. Cyber resilience is not purely an IT issue.

3. Officials responsible for cyber resilience should ensure that Boards/executive teams are briefed on the Framework, and receive regular updates on progress against its implementation. Boards/executive teams should actively seek such updates, and give appropriate priority to discussion of their contents.

4. Boards/executive teams are encouraged to use the Framework in conjunction with the NCSC Board Toolkit. The Framework and the Board Toolkit are mutually reinforcing. The Framework can help Boards implement key aspects of the advice contained in the Board Toolkit, such as identifying a cyber security baseline (see Q3, page 13) and reviewing defensive measures against suitable frameworks (see Q1, page 32).

5. **For smaller organisations**: Some smaller organisations (including some that are on the SCOTS network) may not have a "Board" or "Executive Team". However, where they have formal responsibility for risk management and the delivery of organisational objectives, they should still assure themselves that appropriate arrangements are in place for cyber resilience. For those organisations that are on SCOTS, a **bespoke SCOTS annex** is available, setting out the split of responsibilities between SG iTECS (which delivers SCOTS) and customer organisations. Please contact the SG Cyber Resilience Unit (cyberresilience@gov.scot) for a copy of this annex.

Step 2: Identify the scope of your assessment(s) under the Framework

6. You should identify which networks/systems you intend to assess under the Framework – i.e. the scope of the assessment. This decision may be informed by your initial and ongoing assessment of which of your assets must be protected from cyber threats. The NCSC Board Toolkit advises you to work out what your organisation's "crown jewels" are – i.e. the things most valuable to your organisation – and prioritise their protection accordingly. Related to his, the Framework includes requirements around Information Asset Registers, as well as Hardware and Software Asset Registers.

7. Your organisation may decide to work to different progression stages (or different profiles within progression stages) for different parts of your segmented networks (see "Select your progression stage" below). You should be clear about the scope of any self-assessment undertaken, and ensure that any decision-making is documented. You may, for example, use separate copies of the concept self-assessment tool for relevant segments of your networks, to help understand the sophistication of approach for those different parts.

8. Note that where network or other ICT arrangements are delivered by external suppliers, these can be treated as supply chain issues. The Framework states that "Organisations shall adopt a proportionate, risk-based policy in respect of supply chain cyber security. Specifically, they shall implement the Scottish Public Sector Guidance Note on Supplier Cyber Security from Financial Year 2019-20." The Scottish Government's Cyber Security Procurement Support Tool (CSPST) supports implementation of the Guidance Note and decision-making around the cyber security of suppliers. CSPST is accessible here. The Guidance Note is available here.

Step 3: Identify the Framework progression stage and individual standards you wish to assess against

9. Select a progression stage to assess the relevant arrangements against:

    - All Scottish public sector organisations should already have achieved the initial baseline stage as a result of implementing the Public Sector Action Plan. No additional requirements have been included in the Initial Baseline stage of the Framework.

    - For the majority of public sector organisations, the most appropriate progression stage to aim for is expected to be the Target Stage – in effect, this will become the new "baseline" for the Scottish public sector.

    - For some public sector organisations, it will be appropriate to aim for the Advanced Stage. This is particularly the case for Scottish Health Boards and Scottish Water (which are legally required to achieve the standards of the NIS CAF), but it may also be appropriate for other high profile organisations dealing with very sensitive information, critical services or other assets.

10. The judgement around which progression stage to work to should be informed by your organisation's assessment of things such as the sensitivity of the assets on a network, the potential impact of a breach, etc.

11. By selecting and working towards a Framework progression stage, you will be giving your organisation reasonable confidence that you are working towards the requirements of the individual standards embedded in those progression stages (see the explanation of "Progression Stages" in Section 1, above). You should also consider whether there are **individual standards** that you will particularly wish to have confidence you are meeting. These may include, for example, PSN requirements or NCSC/ICO Guidance on GDPR security outcomes, where there may be particular audit/compliance requirements that you will need to report against. In these circumstances, you should ensure that:

    - The outputs of the concept self-assessment tool relating to those individual standards are correct and are brought to the attention of appropriate people in the organisation; and

    - Appropriate consideration is given to the requirements of the specific individual standards in question – this can be supported by the mapping matrix at **Annex A**, which will aid your understanding of which Framework controls correspond to which specific controls in individual standards.

12. You may also wish to consider which parts of the Framework you will be required, or wish, to get independent assurance against. For some aspects, e.g. those aligned with PSN or Cyber Essentials Plus, independent assurance is an inherent requirement.

Step 4: Conduct an initial self-assessment

13. Undertake an initial self-assessment of the relevant systems/networks using the Framework document and the concept self-assessment tool. Guidance on how to assign appropriate scores using the concept tool can be found in the separate User Guide, available here.

14. **For smaller organisations on SCOTS**: For those organisations that are on SCOTS, a **bespoke SCOTS annex** is available, setting out the split of responsibilities between SG iTECS (which delivers SCOTS) and customer organisations. Please contact the SG Cyber Resilience Unit (cyberresilience@gov.scot) for a copy of this annex.

Step 5: Identify areas of risk acceptance and priority areas for improvement

15. The concept self-assessment tool supports you to identify areas of strength and weakness in your cyber resilience arrangements. You should complete the tool in line with the advice in the separate User Guide, in order to identify those control areas where you may wish to prioritise action to address weaknesses.

16. As noted in Section 1, above, the Scottish Government is clear that the Framework should be implemented by public sector organisations on a **risk-based and proportionate basis**. In order to do this effectively, it will be important to understand your organisation's risk appetite in respect of specific risks arising from non-implementation of specific controls. If you do not currently have a clear understanding of organisational risk appetite, you can use this process to draw this to your Board's attention, and encourage the development of a better defined risk appetite statement (a requirement of the Scottish Public Finance Manual).

Step 6: Report internally against progress and consider the need for improvements

17. You can use the outputs of the concept self-assessment tool dashboard to provide information to your Board/Executive Team about progress against the Framework and (where appropriate) individual standards, and areas of strength and weakness. You should ensure that your senior decision-makers understand that not all controls at a progression stage need to be in place – depending on your organisation's circumstances or risk appetite, it may be perfectly acceptable not to have specific controls in place. However, in such circumstances it is important to document for audit purposes any mitigation measures and the decision-making rationale.

18. Boards/Executive Teams can use the outputs of the self-assessment to help them answer some of the key questions set out in the NCSC Board Toolkit, and take decisions on whether there is a need for improvements (and if so, how these should be achieved).

Step 7: Undertake improvements and repeat self-assessment and reporting at regular intervals

19. After making any improvements required by the Board/Executive Team, you should repeat the self-assessment and reporting progress at regular intervals. The time period for reporting may depend on things such as your organisation's risk appetite, how important cyber resilience is in comparison to other key business risk issues for your organisation, etc.

Step 8: Respond to audit and monitoring requests

20. Audit and inspection bodies for public sector organisations in Scotland are being encouraged to align their audit approach with the Framework. They may ask for evidence as an initial step in their analysis of your organisation's cyber resilience.

21. Where external bodies require reporting in a specific format, you will currently be required to complete those requirements separately. This is likely to be the case for, e.g. PSN and Cyber Essentials certification. However, the Scottish Government Cyber Resilience Unit is aiming to develop the next generation of the self-assessment tool to produce reporting in different formats that will be acceptable to a wider range of external bodies.

22. The Scottish Government does not currently expect to ask for sight of self-assessments using the concept tool. However, when the next generation of the tool is in place, it may seek reports to help identify areas where greater central support or guidance is required for the Scottish public sector.

3. The Framework

SECTION 3 – THE FRAMEWORK

1. The following tables set out the Initial Baseline, Target and Advanced progression stage requirements under the Scottish Public Sector Cyber Resilience Framework. The tables include **links to key resources** that can support you to implement the Framework controls. They also include **links to mappings against individual standards** in Annex A, to support you to gain reasonable confidence that the Framework controls are appropriately aligned with any specific requirements you wish to assess your organisation against.

2. Users will note that there is some **repetition** of requirements across different domains, security categories and sub-categories of control. This has been done intentionally, to ensure security categories are self-contained and to minimise the need for cross-referencing within the document.

3. The Framework is not intended to be technically prescriptive – for example, no requirements are set out on the type of firewall that must be chosen for a particular risk environment. This must be a judgement of the organisation, informed by its own expertise and risk appetite.

MANAGE: Category 1: Organisational Governance

ORGANISATIONAL GOVERNANCE	Appropriate organisational structures, policies, and are processes in place to understand, assess and systematically manage security risks to the organisation's network and information systems.	
RESOURCES: NCSC Board Toolkit; NCSC Staff Training Guide; Scottish Government Training Guide.		
1.1 GOVERNANCE FRAMEWORK: **You have effective organisational security management led at board level and articulated clearly in corresponding policies.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. There is a Board/Senior Management-level commitment to manage the risks arising from the cyber threat.	
TARGET	1. There are appropriate data protection and information security policies and processes in place to direct the organisation's overall approach to cyber security.	
	2. Personal data processed is catalogued and the purpose for processing it is defined and described.	
	3. There are clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services.	

	4. Senior accountable individuals have received appropriate training and guidance on cyber security and risk management.	
	5. There is a culture of awareness and education about cyber security across the organisation.	
ADVANCED	1. Significant risks to sensitive information and key operational services have been identified and are managed.	
	2. The security issues that arise because of dependencies on external suppliers or through the supply chain are detailed, organised and managed.	
1.2 LEADERSHIP & RESPONSIBILITY: There is a board-level individual who has overall accountability for the security of networks and information systems. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. A named Board and Senior Management member of staff have been identified as responsible for organisational cyber resilience arrangements.	
	2. There are clear lines of responsibility and accountability to named individuals for the cyber resilience of sensitive information and key operational services, which have been defined and understood.	
	3. There is a written information security policy in place, which is championed by senior management.	
	4. There is regular staff training in cyber security and information risk management.	
TARGET	1. Senior accountable individuals have received appropriate training and guidance on cyber security and risk management.	
	2. There is a culture of awareness and education about cyber security across the organisation.	
ADVANCED	1. Direction set at board level is translated into effective organisational practices that direct and control the security of the organisation's networks and information systems.	
	2. The board shall ensure that the organisation has planned and budgeted for adequate resources for the delivery, maintenance and improvement of cyber	

	resilience and network and information security, and that these activities are supported by senior management.	
	3. The organisation has established roles and responsibilities for the security of networks and information systems at all levels.	
	4. There are clear and well-understood channels for communicating and escalating risks.	
	5. There is senior-level accountability for the security of networks and information systems with delegated decision-making authority.	
1.3 ADOPTION OF ASSURANCE STANDARDS: There is demonstrable confidence in the effectiveness of the security of the organisations technology, people and processes. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. There is demonstrable and appropriate independent assurance that the five critical network controls of Cyber Essentials are in place: a) firewalls b) secure configuration c) user access control d) malware protection e) patch management	
TARGET	1. The organisation has obtained assurance that suppliers of 3rd party services have appropriate, proportionate and adequate cyber security policies and practices that are certified or aligned with recognised standards or their equivalent. (e.g. HMG Cyber Security Standard, Cyber Essentials, ISO 27001).	
ADVANCED	1. Security as it relates to technology, people, and processes can be demonstrated and verified by a third party audit.	
	2. There are procedures to ensure security measures that are in place to protect the networks and information systems are effective, and remain effective for the service lifetime.	
	3. The assurance methods available are recognised and appropriate methods to gain confidence in the security of essential services are adopted and implemented.	
1.4 INFORMATION ASSET REGISTER: There is a catalogue of sensitive information and data, stored with appropriate management procedures. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	1. Key information assets have been identified and recorded.	
	2. Key information assets have been assessed for their vulnerability to cyber-attack.	
TARGET	1. Organisations shall know and record: a) What sensitive information they hold or process b) Why they hold or process that information c) Where the information is held d) Which computer systems or services process it e) The impact of its loss, compromise or disclosure	
ADVANCED	1. Assets associated with information and information processing have been identified	
	2. An inventory of these assets has been established and is maintained through recognised process.	
	3. Assets maintained in the inventory have ascribed owners.	
1.5 AUDIT/ASSURANCE COMPLIANCE: There are in place procedures to provide assurance on the security of systems and services. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. There is demonstrable and appropriate independent assurance that the five critical network controls of Cyber Essentials are in place: a) firewalls b) secure configuration c) user access control d) malware protection e) patch management	
TARGET	1. The organisation has obtained assurance that suppliers of 3rd party services have appropriate, proportionate and adequate cyber security policies and practices that are certified or aligned with recognised standards or their equivalent. (e.g. HMG Cyber Security Standard, Cyber Essentials, ISO 27001).	
	In addition for PSN: You must implement regular IT Health Checks and ensure the IA conditions of the PSN Code of Connection are met.	
ADVANCED	1. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	

	2. The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	
	3. Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	

MANAGE: Category 2: Risk Management

RISK MANAGEMENT	Appropriate steps are in place to identify, assess and understand security risks to the network and information systems. This includes an overall organisational approach to risk management.	
RESOURCES: NCSC Board Toolkit: Risk Management; NCSC Risk Management Guidance; NCSC Cyber Security Information Sharing Partnership		
2.1 POLICY & PROCESSES: **Your organisation has effective internal processes that manage and mitigate risks to the security of network and information systems and services.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. There are information risk management policies and assessment procedures in place.	
TARGET	1. Organisations shall identify and manage the significant risks to sensitive information and key operational services.	
	2. Senior management and boards regularly review the organisational cyber risks and threats.	
ADVANCED	1. The organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.	
	2. Risk owners are identified.	
	3. The output from the risk management process is a clear set of security requirements that will address the risks in line with the organisational approach to security.	
	4. Significant conclusions reached in the course of the risk management process are communicated to key security decision-makers and accountable individuals.	
	5. The effectiveness of the risk management process is reviewed periodically and improvements made as required.	

2.2 CYBER / INFORMATION RISK ASSESSMENT: The organisation has effective and robust risk assessment methodology and processes that identify and prioritise threats and vulnerabilities. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Key information and IT assets have been identified, risk assessed and prioritised for their vulnerability to cyber-attack.	
TARGET	1. Organisations should establish a process to identify security vulnerabilities and rank them according to their level of risk.	
	2. A systematic risk-based approach is taken to information security, data protection and the security of systems and services. This risk assessment takes into consideration: the technology available; cost of implementation; the nature, scope, context and purpose of any data processing; the probability and impact of the risk being realised.	
	3. The criteria for performing risk assessments are well defined to ensure risk assessments produce consistent, valid and comparable results.	
ADVANCED	1. The risk assessments are based on a clearly articulated set of threat assumptions; these are kept up-to-date through an understanding of changing security threats.	
	2. Risk assessments are conducted when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat.	
	3. The risk assessments are dynamic and are updated in the light of relevant changes, which may include technical changes to networks and information systems, change of use and new threat information.	
2.3 RISK TREATMENT & TOLERANCE: The organisation has risk treatment policies and procedures in place with defined risk appetite and mitigation controls documented. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Key information and IT assets have been identified, thoroughly risk assessed and prioritised for their vulnerability to cyber-attack.	

TARGET	1. The information and cyber risk that the organisation is prepared to tolerate is defined, understood and communicated.	
	2. A risk appetite statement shall be produced and used to guide risk management decisions.	
ADVANCED	1. The organization shall define and apply an information security risk treatment process that identifies appropriate risk treatment options and associated mitigation controls.	
	2. A risk treatment plan shall be produced	
	3. A Statement of Applicability shall be prepared to document the risk treatment and controls adopted.	
	4. The senior management shall assess and sign-off the risk treatment regime, policies and procedures.	
2.4 RISK GOVERNANCE: Risks to network and information systems are effectively managed, communicated, and regularly considered throughout the organisation and led by senior management. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Responsibility for cyber security risks has been allocated appropriately to named individuals.	
	2. Cyber security risks are on the organisational risk register.	
	3. Knowledge sharing of risk management through peer-networks and membership of CiSP is actively undertaken.	
TARGET	1. The board routinely reviews cyber risks which are a standing agenda item.	
	2. There is board-level accountability for cyber risk with a named individual.	
	3. Staff members are trained in cyber risk assessment and management relevant to their role.	
	4. An organisation-wide risk management culture is promoted by the senior management with demonstrable participation at all levels.	

ADVANCED	1. Senior accountable officers receive appropriate training and guidance on cyber security and risk management.	
	2. Senior management regularly reviews the resource allocations to ensure these are sufficient to permit prioritised information security and cyber risk mitigation measures to be implemented.	

MANAGE: Category 3: Supplier Management

SUPPLIER MANAGEMENT	The organisation understands and manages security risks that arise as a result of dependencies on external suppliers and third party services.	
RESOURCES: Scottish Public Sector Guidance Note on Supplier Cyber Security; Cyber Security Procurement Support Tool; NCSC Board Toolkit: Collaborating with Suppliers and Partners; NCSC Supply Chain Guidance.		
3.1 SUPPLY CHAIN ASSURANCE: **The organisation has a deep understanding of the security provisions and assurances around systems and services provided by third parties and their supply chain.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. Organisations shall adopt a proportionate, risk-based policy in respect of supply chain cyber security. Specifically, they shall implement the **Scottish Public Sector Guidance Note on Supplier Cyber Security** from Financial Year 2019-20.	
	2. Organisations that adopt cloud-based services shall ensure the NCSC 14 principles of cloud security are adopted from Financial year 2019-20.	
	3. The organisation has assessed, understands and has procedures in place to manage security risks that may arise as a result of dependencies on third party suppliers.	
	4. Documented and suitable assurances have been obtained from suppliers and their immediate supply chain that proportionate and appropriate security measures to protect systems, services, data and information are in place.	
	5. The security requirements and stipulations necessary to ensure GDPR and other regulatory compliance are incorporated into supplier contracts, are mutually agreed and understood..	
ADVANCED	No additional requirements	
3.2 ROLES AND RESPONSIBILITIES: **The organisation has defined the respective duties and responsibilities of third-party suppliers and the supply chain and these are understand and agreed by all parties.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	

TARGET	1. Where services are outsourced (for example by use of cloud infrastructure or services), you shall understand and accurately record which security related responsibilities remain with the organisation and which are the supplier's responsibility.	
	2. It is essential, where cloud services are employed (particularly with respect to IaaS and PaaS), that there is clarity (whether through contractual agreement or other arrangements) whether the responsibility to carry out certain actions (i.e. patching) lies with the organisation or the cloud supplier.	
ADVANCED	1. There is a clear and documented shared-responsibility model with suppliers for incident management.	
3.3 ACCESS CONTROL: There is visibility and control on third-party users (or automated functions) that can access organisational systems, services, data and information data and these are appropriately verified, authenticated and authorised. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	
TARGET	Not specified	
ADVANCED	1. Only individually authenticated and authorised users can connect to or access your networks or information systems.	
	2. Both electronic and physical access requires individual authentication and authorisation.	
	3. Where cloud-based services are employed, there is sufficient separation of the organisation's data and service from other users of the service.	
	4. Third party user access to all your networks and information systems is limited to the minimum necessary.	
	5. Additional authentication mechanisms, such as two-factor or hardware-backed certificates are employed, to individually authenticate and authorise all third party remote access to all networks and information systems that support essential services.	

	6. The list of external users with access to essential service networks and systems is reviewed on a regular basis, e.g. every 6 months.	
3.4 SECURITY IN PROCUREMENTS: The organisation has security embedded within procurement procedures. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	
TARGET	1. Ensure implementation of the **Scottish Public Sector Supplier Cyber Security Guidance Note** as part of procurement processes.	
ADVANCED	1. Cyber risk and information security related requirements shall be considered as an integral part of the procurement process and, where relevant, included in tender requirements for new systems, services or enhancements to existing provisions.	
	2. Organisations shall regularly monitor, review and audit supplier service delivery and associated security provisions.	
	3. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	

MANAGE: Category 4: Asset Management

ASSET MANAGEMENT	Everything required to deliver, maintain or support networks and information systems and services is determined and understood.	
RESOURCES: NCSC Board Toolkit: Establishing your baseline and identifying what you care about most; NCSC NIS Guidance on Asset Management; End User Device Security Principles; BYOD Guidance: Device Security Considerations.		
4.1 HARDWARE ASSETS: **The organisation has visibility and effective management of all hardware assets.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified	
TARGET	1. All hardware assets and their configuration are tracked and recorded, including end user devices and removable media.	
	2. End user devices are managed to enable organisational controls to be applied over software or applications	
	In addition for PSN: • The security of End User Devices (EUDs) meets the CESG guidance on End User Devices Security Principles and BYOD Guidance: Device Security Considerations.	
ADVANCED	1. All assets are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.	
	2. Assets are securely managed throughout their lifecycle, from creation through to eventual decommissioning or disposal.	
	3. All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	
	4. Assets are prioritised according to their importance to the delivery of the essential service.	
	5. Responsibility for managing the physical assets has been assigned	
	6. Assets management is in place; assets shall not be taken off-site without prior authorisation with associated documentation.	

	7. Security is applied to all assets used off-site.	
4.2 SOFTWARE ASSETS: The organisation has visibility and effective management of all software assets. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. All software is maintained and up to date.	
	2. Software must: ➢ be licensed and supported ➢ be removed from devices when no longer supported ➢ be patched within 14 days of an update being released for critical or high risk vulnerabilities ➢ have other mitigating steps in place where patches cannot be applied	
TARGET	1. All software assets with licence and configuration details must be tracked and recorded	
	2. Software vulnerabilities monitoring, including using in-support software, must be implemented.	
ADVANCED	1. The installation of software shall be controlled and shall not be permitted by general users.	
4.3 INFRASTRUCTURE MANAGEMENT: The organisation recognises critical infrastructure assets and dependencies. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	
TARGET	1. Critical infrastructure assets are identified, threats evaluated and proportionate security measures are in place.	
ADVANCED	1. Network assets shall be regularly maintained to ensure service continuity.	
	2. Network assets shall be protected from power surges and failures.	
	3. Dependencies on supporting infrastructure (e.g. power, cooling etc.) shall be identified and recorded.	
	4. Equipment and devices on premise shall be sited to ensure protection from external and internal environmental risks (e.g. water ingress).	

PROTECT: Category 5: Information Security Management

INFORMATION SECURITY MANAGEMENT	Proportionate security measures are in place to protect information, data, services and systems from cyber attack.	
RESOURCES: Guidance on Departmental Information Risk Policy; The Role of Information Asset Owners in Government		
5.1 SECURITY POLICY & PROCESSES: **The organisation has developed and continues to improve a set of protection policies and processes that manage and mitigate the risk of security-related service disruption or data loss.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified	
TARGET	1. Appropriate policies and processes that direct the organisation's overall approach to securing systems are defined, implemented, communicated and enforced.	
	2. Security governance, risk assessment and technical security practices are documented.	
	3. Each organisation shall determine the boundaries and scope of its security policy. This should be defined to cover all relevant operations, which shall include interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations.	
	4. Information security shall be addressed in project management, regardless of the type of project.	
	5. Key security performance indicators are defined and reported to the executive management.	
	6. Acceptable usage policies that define the proper use of technology by all personnel are in place. (These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.)	
	7. The security policy and procedures clearly define information security responsibilities for all personnel.	

ADVANCED	1. Policies and processes are reviewed at suitably regular intervals to ensure they remain relevant to threats, business processes, accommodate lessons learned and remain appropriate and effective.	
	2. Security policies and processes are integrated with other organisational policies and processes.	
	3. All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date.	
5.2 LIFECYCLE MANAGEMENT: Information assets are managed throughout their lifecycle, from creation through to eventual decommissioning or disposal. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Information and data should be classified according to retention and disposal policies and legal requirements.	
	2. Where removable media is to be reused or destroyed then appropriate steps should be taken to ensure that previously stored information will not be accessible.	
	3. Personal data processed should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary.	
	4. The rationale for collecting, holding or processing personal information should be documented.	
	5. Technical controls are in place to prevent unauthorised or unlawful processing of personal data that might remain in memory when technology is sent for repair or disposal.	
	6. Information and data records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislation, regulatory, contractual or business requirements.	

	In addition for PCI compliance: • Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in the data retention policy. • Purge unnecessary stored cardholder data at least quarterly. • Do not store sensitive cardholder authentication data after authorisation (even if it is encrypted).	
ADVANCED	1. Information, data and media destruction and disposal processes should have assurance procedures and have an audit trail from collection to destruction.	
5.3 STORAGE: The organisation knows where data and information are stored and has security in place whether on premise, mobile, removable or cloud based storage is employed. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. There are suitable physical or technical means to protect stored data from unauthorised access, modification or deletion through unauthorised access to storage media.	
ADVANCED	1. There is a detailed understanding and mapping of data and information flows from creation, transit and storage.	
	2. The organisation has processes to remove or minimise unnecessary copies or unneeded historic records.	
	3. Where outsourced or third-party storage is employed, appropriate secured measures are in place and enforced, with appropriate assurance procedures consistent with data retention policies.	
	4. All data is sanitised from all devices, equipment or removable media before disposal.	

5.5 Information / Data Classification: Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification, to ensure it receives an appropriate level of protection in accordance with its importance to the organization. *[Click **here** to go to mappings]*		**Notes**
BASELINE	Not specified	
TARGET	1. Organisations shall know and record the information they hold or process.	
ADVANCED	1. All data and information assets have been identified and classified.	
	2. Information has been classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	
	3. An appropriate set of procedures for information labelling has been developed and implemented in accordance with the information classification scheme adopted by the organization	
5.6 Information Asset Register: Data and information assets are identified and an inventory of these assets is created and maintained. *[Click **here** to go to mappings]*		**Notes**
BASELINE	Not specified.	
TARGET	1. All data and information assets have been catalogued by type and classification and recorded in an information assets register.	
	2. The register records where the information/data are held and which computer systems or services process it.	
	3. The purpose for processing the personal data held by the organisation has been described and recorded.	
ADVANCED	1. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme.	
	2. The register maintains a current understanding of the location, quantity and quality of data and information stored.	
5.7 Information / Data Transfer Controls: The organisation has an understanding of information / data flows including the transfer of data to third parties and the associated security protocols that are in place. *[Click **here** to go to mappings]*		**Notes**

BASELINE	Not specified.	
TARGET	1. Data at rest on all devices is protected by appropriate measures including physical protection (when hosted within a secure data centre) and encryption.	
	2. There are technical controls in place (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest.	
	3. Data in transit accessed by remote workers and third parties is protected by encryption and the application of a virtual private network (VPN).	
	4. Protect data in transit using well-configured TLS v1.2.	
	In addition for PCI: • Strong cryptography and security protocols such as SSL/TLS, SSH or IPSec are employed to safeguard sensitive cardholder data during transmission over open, public networks. • Wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g. IEEE 802.11i) to implement strong encryption for authentication and transmission. • The use of WEP as a security control is prohibited. • Unprotected PANs are not sent by end user messaging technologies.	
ADVANCED	1. There is a current understanding and record of the data links and routes used to transmit data.	
	2. Appropriate physical or technical means are applied to protect data that travels over an untrusted carrier.	
	3. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	
	4. Agreements shall address the secure transfer of business information between the organization and external parties.	

PROTECT: Category 6: People

PEOPLE	The organisation has policies and procedures in place to ensure staff and contractors are screened, trained and know their security responsibilities.	
RESOURCES: Government Baseline Personnel Security Standard; Government Security: Roles and Responsibilities; NCSC Staff Training Guide; Scottish Government Training Guide.		
6.1 PRIOR TO EMPLOYMENT: **Employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified	
TARGET	**For PSN:** • For users who have administrative privileges, pre-employment checks which are aligned with the Baseline Personnel Security Standard (BPSS) should be implemented.	
ADVANCED	1. Pre-employment checks have been performed on all candidates proportional to the role and responsibilities, the classification of the information to be accessed and the perceived risks.	
	2. Employee and contractor contract terms and conditions shall state their responsibilities for information security.	
6.2 DURING EMPLOYMENT: **Staff and contractors are aware of and fulfil their information and cyber security responsibilities.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. A staff induction process is in place for new users (including contractors and third party users).	
	2. As part of the induction process staff are made aware of their personal responsibility and obligations to comply with the corporate security policies with regards to system security, data handling, and acceptable use.	
	3. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action.	

	4. Acceptable usage policies are in place that include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.	
	5. The security policy and procedures clearly define information security responsibilities for all personnel.	
ADVANCED	1. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	
	2. All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	
	3. There are established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	
	4. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	
	5. Users shall ensure that unattended equipment has appropriate protection.	
	6. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	
6.3 STAFF TRAINING & AWARENESS CULTURE: All employees and contractors receive appropriate awareness education and training with regular assessments and updates as relevant for their job function. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Appropriate staff training, awareness-raising and disciplinary processes with regard to cyber resilience are in place for staff at all organisational levels.	
TARGET	1. All users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies including removable media security and mobile device utilisation.	

	2. All users should receive regular refresher training on the security risks to the organisation.	
	3. The effectiveness of security training is monitored to test the effectiveness and value of the security training provided to all users.	
	4. Employees receive appropriate training, support and technology to help them manage personal data securely.	
	5. Senior accountable individuals receive appropriate training and guidance on cyber security and risk management and promote a culture of awareness and education about cyber security across the organisation.	
ADVANCED	1. Individuals' cyber security training is monitored to ensure update training is completed and delivered at regular intervals.	
	2. Cyber security training and awareness activities are evaluated for efficacy.	
6.4 STAFF SKILLS ASSESSMENT: Staff, including SMT and board members, are appropriately trained in cyber security and risk assessment. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	
TARGET	1. A formal assessment of security skills is undertaken.	
	2. Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognised certification scheme.	
ADVANCED	1. Necessary roles for the security of networks and information systems have been identified and appropriately capable and knowledgeable staff fill those roles.	
6.5 MOBILE / REMOTE WORKING POLICY: The organisation has in place policies and security measures to manage the risks introduced by people using mobile devices and remote working. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	

TARGET	1. A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	
	For PSN: • Services presented outside of the protected enterprise (online services for staff, mobile working etc.) should be delivered from an appropriate architecture, with access to any core information or services constrained. • The architecture will include services to identify malware at the gateway. Where encryption prevents this, the organisation shall implement an equivalent level of protection at the end point. • If you are using cloud services: You may consider procurement of services which respond to different business needs and therefore have different security attributes. It is important that any interfaces between services are within scope. • If cloud services are accessed from the organisation's PSN-connected infrastructure, security assessments of these services should be conducted against the NCSC Cloud Security Principles. • Unmanaged devices: must not have access to the PSN. Where a corporate service contains information that has been sent over the PSN, you should have the data owner's permission before allowing unmanaged devices to access that data. Additionally, you must ensure that an unmanaged device: a) Is not able to use the corporate service to access the PSN in an unmediated fashion b) Accesses the corporate service through an appropriately secured connection c) For example, at the network layer via a VPN, or at the application layer via a protocol that implements TLS, is authenticated prior to the information being accessed with a mechanism that does not solely rely on a username and password.	

ADVANCED	1. A policy and supporting security measures shall be implemented to protect information and data accessed, processed or stored at remote sites.	
	2. Mobile devices that hold data are catalogued, controlled and configured according to best practice for the platform, with appropriate technical and procedural policies in place.	
	3. A remote-wipe capability is in place for all mobile devices.	
	4. Data held on mobile devices has been minimised and some data may be automatically deleted off mobile devices after a certain period.	

PROTECT: Category 7: Services Resilience

SERVICES RESILIENCE	Network and information systems are designed to be resilient to cyber security incidents.	
RESOURCES: N/A		
7.1 SERVICES RESILIENCE: **Systems are appropriately segregated and resource limitations are mitigated.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified	
TARGET	1. Key operational services have been identified with resource, technology and service dependencies defined (e.g. power, bandwidth, cooling, data, people).	
ADVANCED	1. Key operational systems are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration).	
	2. Geographical constraints or weaknesses have been identified and mitigated.	
	3. Systems that key services depend upon have redundancy and are replicated to an alternative location.	
	4. There are alternative physical paths and service providers for network connectivity with known separacy and diversity of bearers.	
	5. Dependencies, resource and geographical limitation assessments are regularly reviewed with update mitigations when required.	

PROTECT: Category 8: Access Control

ACCESS CONTROL	Access to information, services and systems is controlled, managed and monitored through policies and procedures.	
RESOURCES: N/A		
8.1 ACCOUNT MANAGEMENT: **User accounts are effectively managed throughout their lifecycle to provide minimum access to sensitive information or key operational services.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. All user account creation is subject to a provisioning and approval process.	
	2. Each user authenticates using a unique username and strong password before being granted access to applications, computers and network devices.	
	3. All default passwords are removed and changed.	
	4. There is a robust password policy which avoids users having weak passwords, such as those trivially guessable.	
	5. Password or account sharing between users is not permitted.	
	6. User accounts and special access privileges are removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g. 3 months).	
	7. Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.	
TARGET	**For PSN:** • High-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts. • Passwords are combined with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication. • Passwords are never stored as plain text, but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a salt before hashing passwords.	

ADVANCED	No additional requirements.	
8.2 IDENTITY AUTHENTICATION: Procedures are in place to verify, authenticate and authorise access to the organisational networks and information systems. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Only individually authenticated and authorised users can connect to or access your networks or information systems.	
	2. Each user authenticates using a unique username and strong password before being granted access to applications, computers and network devices.	
TARGET	1. Users that can access personal data are appropriately authenticated.	
	2. Users who have privileged access are strongly authenticated by two-factor or device authentication measures.	
	3. Multi-factor authentication shall be used for access to enterprise level social media accounts.	
	In addition for PCI: • Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. For example, use technologies such as remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.	
ADVANCED	1. Additional authentication mechanisms, such as two-factor or hardware-backed certificates are employed for all systems that operate or support key services.	
	2. There is an auditable, robust procedure in place to verify each user and issue minimum required access rights.	

	3. Attempts by unauthorised users to connect to systems are alerted, promptly assessed and investigated.	
8.3 PRIVILEGE MANAGEMENT: The allocation and use of privileged access rights to networks and information systems is restricted and controlled. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Special access privileges are restricted to a limited number of authorised individuals.	
	2. Details about special access privileges (e.g. the individual and purpose) are documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly).	
	3. Special access privileges are controlled, periodically reviewed and removed or disabled when no longer required.	
TARGET	1. Users who have privileged access accounts are strongly authenticated by two-factor or hardware authentication measures.	
	2. Access to sensitive information and services is only provided to authorised, known and individually referenced users or systems.	
	3. Access to logging data is limited to those with business need and no others. Legitimate reasons for accessing logging data are given in use policies and users are trained on this.	
ADVANCED	1. Systems and devices supporting the delivery services are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.	
	2. Privileged access (e.g. to systems controlling the essential service or system administration) is carried out with separate accounts that are closely monitored.	
	3. All privileged access to your networks and information systems is routinely validated and subject to real-time security monitoring, with all privileged user sessions recorded and stored for offline analysis and investigation.	

	4. Temporary, time-bound rights for privileged access and external third-party support access are employed where appropriate.	
	5. The use of utility programs that might be capable of overriding systems and applications shall be restricted.	
	6. Access to program source code shall be restricted.	
8.4 ADMINISTRATOR ACCOUNT MANAGEMENT: System administrator accounts are controlled and monitored with the activity logs protected and regularly reviewed. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the internet.	
	2. Administrative accounts should be configured to require a password change on a regular basis (e.g. at least every 60 days).	
TARGET	1. Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email.	
	2. Administrators do not conduct 'normal' day-to-day business from their high privilege account and use normal accounts for standard business use.	
ADVANCED	1. The list of system administrators is regularly reviewed, e.g. every 6 months.	

Category 9: Media Management

MEDIA MANAGEMENT	Fixed and portable storage media and devices are managed and data / information is appropriately protected.	
RESOURCES: N/A		
9.1 STORAGE MEDIA: **Policies and procedures are in place to protect stored data and prevent unauthorised disclosure, modification, removal or destruction of information stored on media.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. The organisation can identify and account for all end user devices and removable media.	
	2. Tracking and recording of all assets that process personal data, including end user devices and removable media is in place.	
	In addition for PCI: • Media back-ups are stored in a secure location, preferably off site. • All media is physically secure. • There is strict control over the internal or external distribution of any kind of media. • Management approves any and all media moved from a secured area, especially when media is distributed to individuals. • There is strict control over the storage and accessibility of media. • All media is destroyed when it is no longer needed for business or legal reasons.	
ADVANCED	1. All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal.	
	2. Cloud service providers appropriately sanitise data storage areas before reallocating to another user.	
9.2 MOBILE MEDIA / DEVICES: **The organisation can identify and account for all mobile end-user devices and removable media and monitors the data protection measures that are in place on mobile devices.** *[Click **here** to go to mappings]*		NOTES

BASELINE	Not specified.	
TARGET	1. Where the use of removable media is required to support the business need, it is limited to the minimum media types and users needed.	
	2. Removable media is automatically scanned for malware when it is introduced to any system.	
	3. Any media brought into the organisation is scanned for malicious content by a standalone machine before any data transfer takes place.	
	4. All removable media is formally issued to individual users who are accountable for its use and safe keeping.	
	5. Users do not use unofficial media, such as USB sticks given away at conferences.	
	6. Sensitive information is encrypted at rest on media.	
	7. Where removable media is to be reused or destroyed then it will be done securely with appropriate steps taken to ensure that previously stored information is not accessible.	
	8. All data is sanitised from all devices, equipment or removable media before disposal.	
	9. All users are made aware of their personal responsibilities for following the removable media security policy.	
	10. A secure baseline build and configuration is applied to all mobile devices.	
ADVANCED	1. Mobile devices are catalogued, tracked and configured according to best practice for the platform, with appropriate technical and procedural policies in place.	
	2. The data held on mobile devices is minimised.	
	3. Some data may be automatically deleted off mobile devices after a certain period.	
	4. Procedures are implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	

9.3 CRYPTOGRAPHY: There is proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information at rest, in transit and on mobile devices or removable media. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified	
TARGET	1. Sensitive information should be encrypted at rest on devices and media and when transmitted electronically, especially over an untrusted carrier.	
	In addition for PCI: • Any keys used for encryption of cardholder data are protected from disclosure and misuse. • All appropriate key management processes and procedures for cryptographic keys used for encryption of cardholder data are documented and implemented. • Strong cryptography and security protocols such as SSL/TLS, SSH or IPSec are used to safeguard sensitive cardholder data during transmission over open, public networks. • Wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. • The use of WEP as a security control is prohibited.	
ADVANCED	1. There is a policy on the adoption of cryptography including the use and protection of cryptographic keys and their lifetime management.	
9.4 REMOTE WIPE CAPABILITY: The organisation has the ability to remotely wipe and/or revoke access from an end user device. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	

TARGET	1. The organisation has the ability to remotely wipe and/or revoke access from all mobile devices.	
ADVANCED	No additional requirement.	

PROTECT: Category 10: Environmental Security

ENVIRONMENTAL SECURITY	Appropriate procedures are in place to reduce the risks from internal and external environmental threats and hazards.	
RESOURCES: N/A		
10.1 EQUIPMENT LOCATION: **Equipment shall be sited and protected to reduce environmental impacts on information systems and service delivery.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	Not specified.	
ADVANCED	1. Equipment on premise and with third parties is sited and protected to reduce the risks from physical and environmental threats and hazards.	
	2. Network and connectivity cabling is resilient, and protected from interception, interference or damage with redundancy in place.	
10.2 POWER RESILIENCE: **Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	Not specified.	
ADVANCED	1. Dependencies on supporting infrastructure (e.g. power, cooling) are identified and recorded.	
	2. Equipment is protected from power failures and other disruptions caused by failures in supporting utilities such as telecommunications with redundancy in place.	

PROTECT: Category 11: Physical/building security

PHYSICAL / BUILDING SECURITY	To prevent unauthorised physical access, damage and interference with the organisation's information systems and services.	
RESOURCES: N/A		
11.1 ACCESS CONTROL: **Building and secure areas access shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed admittance.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. Appropriately secure accommodation, and appropriate policies and practices governing its use, are in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise.	
	In addition for PCI: • Appropriate facility entry controls are used to limit and monitor physical access to systems. • Procedures are in place to easily distinguish between onsite personnel and visitors. • All visitors are authorized before entering secure areas; given a physical badge or token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical badge or token before leaving the facility or at the date of expiration. • A visitor log is used to maintain a physical audit trail of visitor information and activity, including visitor name and company and the onsite personnel authorising physical access. The visitor log is retained for at least three months unless otherwise restricted by law.	
ADVANCED	1. Delivery and loading areas and other access points are controlled.	

11.2 INTERNAL SECURITY: Internal security perimeters shall be defined with policies and active alerting systems used to protect areas that contain sensitive data, critical information and essential information systems. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Secure accommodation areas are defined and segregated to protect areas that contain either sensitive data or information processing facilities.	
	2. Appropriate policies and practices governing use of the secure accommodation and access are in place.	
ADVANCED	1. Secure areas are protected by entry controls to ensure that only authorised personnel are allowed access.	
	2. Physical security for offices, rooms and facilities shall be defined and implemented; to include, for example, intruder detection, fire and flood alarms and alerting systems.	

PROTECT: Category 12: System Management

SYSTEM MANAGEMENT	Information systems are protected from cyber-attack throughout their lifecycle.	
RESOURCES: N/A		
12.1 SECURE CONFIGURATION: **The network and information systems that support the delivery of essential services are securely configured.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.	
	2. Any default password for a user account should be changed to an alternative, strong password.	
	3. Unnecessary software (including application, system utilities and network services) should be removed or disabled.	
	4. The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).	
	5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.	
TARGET	1. A secure baseline build is implemented for all systems, platforms and components, including hardware and software to reduce the level of inherent vulnerability.	
	2. Any functionality or application, services or ports not required to support a user or business need is removed or disabled.	
	3. The secure build profile is managed by a configuration control process and any deviation from the standard build is documented and approved.	
	In addition for PSN:	

	• Configuration control of applications installed and technology is in place. All changes and new applications are recorded and managed, including a formal approval and documentation process. • Devices, systems and services have the capability to detect, isolate and respond to malicious software. • The underlying infrastructure and platform are secure. This includes verification that the hosting environment is maintained securely.	
ADVANCED	1. Network and system configurations changes are managed, secure and documented.	
	2. Network and information systems are regularly reviewed and validated to ensure that they have the expected, secured settings and configuration.	
	3. There are regular reviews and updates to technical knowledge about networks and information systems, such as documentation and network diagrams, and these are securely stored.	
	4. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.	
12.2 SECURE DESIGN / DEVELOPMENT: Information security is designed and implemented within the development lifecycle of information systems and networks. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	**For PCI:** • Software applications (internal and external, and including web-based administrative access) are developed in accordance with PCI DSS and based on industry best practices. • Information security is embedded throughout the software development life cycle.	

	• Change control processes and procedures are followed for all changes to system components. • Applications are developed based on secure coding guidelines and custom application code is reviewed to identify coding vulnerabilities. • All public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.	
ADVANCED	1. A secure development policy with guidance is in place that defines rules for the development of software and systems and is applied.	
	2. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	
	3. The organisation shall supervise and monitor the activity of outsourced system development.	
	4. Change control procedures are in place to manage the development lifecycle.	
	5. Appropriate expertise is employed to design and review network and information systems.	
	6. Network information systems and sensitive data are segregated into appropriate security zones (e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone).	
	7. The networks and information systems are designed to have simple data flows between components to support effective security monitoring.	
	8. The networks and information systems are designed to be easy to recover.	
12.3 CHANGE CONTROL PROCEDURES: Changes to systems and software configurations are controlled by formal change control procedures. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	Not specified.	
TARGET	1. Policies that set out configuration control and change management processes for all systems are in place.	
	2. The ability of users to change configuration is restricted. Users with 'normal' privileges are prevented from installing or disabling any software or services running on the system.	
ADVANCED	1. Modifications to software are restricted and all changes are subject to change control procedures.	
	2. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.	
	3. Change management is in place to control changes to business processes, information processing facilities and systems.	
12.4 SYSTEM TESTING: Testing of security functionality shall be carried out during development of new systems, upgrades and new versions or configurations. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Regular testing is undertaken to evaluate the effectiveness of security measures, including virus and malware scanning, vulnerability scanning and penetration testing.	
	2. The results of any testing and remediating action plans are recorded.	
	In addition for PSN: • Regular IT Health Checks (ITHCs) are implemented to demonstrate that any security mechanisms put in place are ongoing and effective and identify any current vulnerability. ITHCs should normally be conducted annually, or more frequently where appropriate. • Issues identified in the ITHC (including systemic issues) are addressed, with critical and high risks areas resolved immediately or a viable plan for resolution is agreed. Medium and Low risks may be accepted or subject to remedial action plans.	

	In addition for PCI: • The presence of wireless access points is tested to detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. • External and internal penetration testing is performed at least annually and after any significant infrastructure or application upgrade or modification, including network- and application-layer penetration tests. • Network intrusion detection systems and/or intrusion prevention systems are used to (a) monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and (b) alert personnel to suspected compromises. • IDS/IPS engines, baselines, and signatures are kept up to date. • File integrity monitoring tools are deployed to alert personnel to unauthorized modification of critical system files, configuration files or content files. Critical file comparisons are performed at least weekly.	
ADVANCED	1. Regular testing by third-parties is undertaken to identify vulnerabilities in the networks and information systems.	
	2. Penetration testing is undertaken following changes to operating systems, business applications and software development and deployment.	
	3. Test data shall be securely marked, protected and controlled.	
	4. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	

PROTECT: Category 13: Operational Security

OPERATIONAL SECURITY	Appropriate technical and organisational measures are in place to protect systems and digital services from cyber attack	
RESOURCES: NCSC Active Cyber Defence Programme		
13.1 MALWARE POLICIES & PROTECTION: Detection, prevention and recovery controls to protect against malware shall be implemented. *[Click **here** to go to mappings]*		NOTES
BASELINE	1. Malware protection software is: a. installed and actively running on all computers that are connected to or capable of connecting to the internet and generates audit logs b. kept up-to-date (e.g. at least daily, either by configuring it to update automatically or through the use of centrally managed deployment). c. configured to i. scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) ii. scan web pages when being accessed (via a web browser). d. configured to perform regular scans of all files (e.g. daily). e. preventing connections to malicious websites on the internet (e.g. by using website blacklisting).	
TARGET	1. Anti-malware policies and standards are developed and implemented across the organisational infrastructure.	
	2. End user device protection is in place through anti-virus software and application whitelisting.	
	3. Stand-alone workstations are provided as required, equipped with appropriate anti-virus software capable of scanning the content on any type of media.	
ADVANCED	No additional requirements.	
13.2 EMAIL SECURITY: Information involved in electronic messaging shall be appropriately protected. *[Click **here** to go to mappings]*		NOTES

BASELINE	1. The NCSC Active Cyber Defence (ACD) programme is implemented where appropriate and available.	
TARGET	1. Transport Layer Security Version 1.2 (TLS v1.2) is used for sending and receiving email securely.	
	2. Domain-based Message Authentication Reporting and Conformance (DMARC) is in place along with Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records.	
	3. Spam and malware filtering is present and DMARC is enforced on inbound email.	
ADVANCED	No additional requirement.	
13.3 APPLICATION SECURITY: Applications are tested for susceptibility to security vulnerabilities on development and following system changes. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. The NCSC's Web Check service has been adopted.	
TARGET	1. Web applications are regularly tested for the presence of known security vulnerabilities (such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities) and common configuration errors.	
ADVANCED	No additional requirements.	
13.4 VULNERABILITY MANAGEMENT & SCANNING: Network and information systems are managed to prevent exploitation of technical vulnerabilities. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. The NCSC Active Cyber Defence (ACD) programme is implemented where appropriate and available.	
TARGET	1. There is a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities.	
	2. Regular vulnerability scans are conducted via automated vulnerability scanning tools against all networked devices and any identified vulnerabilities are remedied or managed within an agreed time frame.	
	3. Regular discovery scans to detect unknown devices are undertaken and any anomalous findings are investigated.	

	4. Antivirus and malicious code checking solutions are deployed to scan inbound and outbound objects at the network perimeter. Any suspicious or infected malicious objects are quarantined for further analysis.	
	In addition for PCI: • Internal and external network vulnerability scans are run at least quarterly and after any significant change in the network. • Quarterly external scans are performed by an Approved Scanning Vendor (ASV). • Scans conducted after network changes are performed by internal staff. • File integrity monitoring tools are deployed to alert personnel to unauthorised modification of critical system files, configuration files or content files. The software is configured to perform critical file comparisons at least weekly.	
ADVANCED	1. Information about vulnerabilities for all software packages, network equipment and operating systems is obtained in a timely fashion.	
	2. Vulnerabilities are prioritised and subject to a risk assessment to determine the organisation's exposure and vulnerability.	
	3. Selected threat intelligence feeds are in place to enable risk-based and threat-informed decisions based on business needs.	
13.5 DATA EXFILTRATION MONITORING: Network traffic is monitored to identify unusual activity. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Network traffic, services and content is limited to that required to support business need (for example, by setting effective firewall rule sets).	

	2. Inbound and outbound traffic traversing network boundaries is monitored to identify unusual large data transfers which automatically generate security alerts that are promptly managed by appropriately trained staff.	
ADVANCED	No additional requirements.	
13.6 SOFTWARE SUPPORTED & UPDATED: Operating systems and software packages are patched regularly and in vendor support. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Software running on computers and network devices is kept up-to-date and has the latest security patches installed. Specifically: a) Software running on computers and network devices that are connected to or capable of connecting to the internet is licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available. b) Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet are installed in a timely manner (e.g. within 30 days of release or automatically when they become available from vendors). c) Out-of-date software (i.e. software that is no longer supported) is removed from computer and network devices that are connected to or capable of connecting to the internet. d) All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet is installed in a timely manner (e.g. within 14 days of release or automatically when available from vendors).	
TARGET	1. There is an organisation policy that specifies specific patch application periods and a process for auditing compliance. Critical and high risk vulnerabilities are patched within 14 days, important vulnerabilities patched within 30 days and all others patched within 60 days. Where vulnerability is being actively exploited then mitigating actions are taken immediately.	

	2. Where a patch is not available or cannot be deployed within the timescales above, there are alternative mitigating actions in place, such as disabling or reducing access to the vulnerable service.	
ADVANCED	1. You maximise the use of supported software, firmware and hardware in your networks and information systems.	
13.7 WEBSITE SCREENING: Malware protection software should prevent connections to malicious websites. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Malware protection software is in place to prevent connections to known malicious websites on the internet (e.g. by using website blacklisting).	
TARGET	No additional requirements.	
ADVANCED	No additional requirements.	
13.8 BROWSER MANAGEMENT: Web browsers should be configured to minimise security vulnerabilities and risk. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Deploy a content filtering capability on all external gateways to try to prevent attackers delivering malicious code to common desktop applications such as the web browser.	
	2. Browsers are kept current and configured to mitigate against code exploits.	
	3. Unnecessary browser plugins or scripting languages are disabled.	
ADVANCED	No additional requirements.	
13.9 MONITOR / AUDIT USER ACTIVITY: User access and activity are monitored to identify unauthorised access attempts, policy violations and unusual behaviour. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. All user access and activity is monitored, particularly access to sensitive information and the use of privileged account actions.	

	2. The monitoring capability has the ability to identify unauthorised or accidental misuse of systems or data. It is able to tie specific users to suspicious activity.	
	3. Activities that are outside of normal, expected bounds; policy violation; suspicious or undesirable behaviour (such as access to large amounts of sensitive information outside of standard working hours) are recorded and investigated.	
	In addition for PCI: • An automated audit trails system is in place for all system components for reconstructing these events: a) all individual user accesses to cardholder data; b) all actions taken by any individual with root or administrative privileges; c) access to all audit trails; d) invalid logical access attempts; e) use of identification and authentication mechanisms; f) initialisation of the audit logs; g) creation and deletion of system-level objects. • Audit trail entries are recorded for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource. • All critical system clocks and times are synchronised with controls for acquiring, distributing, and storing time. • Audit trails are secured so they cannot be altered. • Logs for all system components related to security functions are reviewed at least daily. • Audit trail history is retained for at least one year; at least three months of history is immediately available for analysis.	

ADVANCED	1. All user's access is logged and monitored for offline analysis and investigation as required.	
	2. Logging facilities and log information shall be protected against tampering and unauthorised access.	
	3. All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.	
	4. Audit logs recording user activities, exceptions, faults and information security events are created, maintained securely and regularly reviewed.	
	5. Attempts by unauthorised users to connect to systems are alerted, promptly assessed and investigated where relevant.	
13.10 DISABLED AUTO-RUN: The auto-run feature should be disabled to prevent software programs automatically running. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. The auto-run feature is disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).	
TARGET	No additional requirements.	
ADVANCED	No additional requirements.	

PROTECT: Category 14: Network Security

NETWORK SECURITY	Appropriate measures are in place to ensure the protection of information systems and information held in networks.	
RESOURCES: NCSC Active Cyber Defence Programme		
14.1 PATCH MANAGEMENT: **Operating systems and software packages on networks and devices are kept up-to-date with the latest security patches installed.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet are installed in a timely manner (e.g. within 14 days of release or automatically when available from vendors).	
TARGET	1. There is a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities. The policy specifies specific patch application periods and a process for auditing compliance.	
	2. Critical vulnerabilities are patched within 14 days, important vulnerabilities patched within 30 days and all others patched within 60 days.	
	3. Where a vulnerability is being actively exploited then mitigating action (e.g. patch applied) is immediately taken.	
	4. Where a patch is not deployed (or available) within the timescales above there is alternative mitigating actions employed, such as disabling or reducing access to the vulnerable service.	
ADVANCED	No additional requirements.	
14.2 DEVICE MANAGEMENT: **Devices that are used to access organisational networks, information systems and data are known and recorded with integrated security management policies and systems.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. Unnecessary peripheral devices are disabled.	

	2. All end-user devices are recorded, managed and tracked.	
	3. Technical policies are applied and controls exerted on devices over software and applications.	
	4. Devices used to access sensitive information and data or key operational services are authenticated and authorised.	
	In addition for PSN: • Unmanaged devices do not have access to the PSN. Where a corporate service contains information that has been sent over the PSN, the data owner's permission is sought before allowing unmanaged devices to access that data. Additionally, unmanaged devices: a) are not able to use the corporate service to access the PSN in an unmediated fashion b) access the corporate service through an appropriately secured connection (e.g. via a VPN, or via a protocol that implements TLS). c) are authenticated prior to the information being accessed with a mechanism that does not solely rely on a username and password.	
ADVANCED	1. Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.	
	2. Device identity management which is cryptographically backed is performed and only known devices are able to access systems.	
	3. Regular discovery scans are performed to detect unknown devices and any findings are investigated.	
	4. Privileged access is only granted on owned and managed devices that are technically segregated and secured to the same level as the networks and systems being maintained.	

14.3 CONTENT SCREENING: Content-based attacks are mitigated with inbound and outbound screening. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Content filtering capability is present on all external gateways to prevent malicious code being deployed to common desktop applications such as the web browser. The antivirus and malware solutions used at the perimeter are different to those used to protect internal networks and systems in order to provide some additional defence in depth.	
	2. Dedicated, stand-alone media scanning machines are provided and equipped with appropriate anti-virus products capable of scanning the content contained on any type of media and inspect recursive content within files.	
ADVANCED	No additional requirements.	
14.4 INTERNAL SEGREGATION: Networks and information systems are segregated into appropriate security zones. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Information services, sensitive data, users and information systems are segregated into appropriate security zones on networks.	
	2. Key operational systems are segregated in a highly trusted, more secure zone isolated with appropriate network security controls.	
ADVANCED	1. Key operational systems are segregated from other business and external systems by appropriate technical and physical means.	
	2. Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.	
	3. Internet services are not accessible from operational systems.	
	4. Logging data is segregated from the rest of the network, and is not affected by disruption or corruption of network data.	
14.5 WIRELESS SECURITY: Wireless access points should be securely configured and segregated as appropriate. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	1. Wireless access points are securely configured.	
TARGET	1. All wireless access points only allow known devices to connect to corporate Wi-Fi services.	
	2. Security scanning tools are in place to detect and locate unauthorised or spoof wireless access points.	
	In addition for PCI: • Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption.	
ADVANCED	No additional requirements.	
14.6 BOUNDARY / FIREWALL MANAGEMENT: Manage access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. One or more firewalls (or equivalent network device) are installed on the boundary of the organisation's internal network(s).	
	2. The default administrative password for any firewall (or equivalent network device) is changed to an alternative, strong password.	
	3. Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall) is subject to approval by an authorised individual and documented (including an explanation of business need).	
	4. Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), are disabled (blocked) at the boundary firewall by default.	
	5. Firewall rules that are no longer required (e.g. because a service is no longer required) are removed or disabled in a timely manner.	

	6. The administrative interface used to manage boundary firewall configuration is not accessible from the internet. (The interface is protected by additional security arrangements, which include using a strong password, encrypting the connection (e.g. using SSL), restricting access to a limited number of authorised individuals and only enabling the administrative interface for the period it is required.)	
TARGET	1. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary.	
	In addition for PCI: • Firewall and router configuration standards are established that formalise testing whenever configurations change; that identify *all* connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months. • Firewall and router configurations that restrict all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment. • Direct public access between the Internet and any system component in the cardholder data environment is prohibited. • Personal firewall software is installed on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network • All public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.	
ADVANCED	1. Traffic crossing the network boundary (including IP address connections as a minimum) is monitored.	
14.7 ADMINISTRATOR CONTROL: System administrators are strongly authenticated and authorisation is reviewed. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	Not specified.	
TARGET	1. Administrator access to any network component is properly authenticated and authorised.	
	2. Default administrative passwords for network equipment are changed.	
	3. Changes to the authoritative DNS entries can only be made by strongly authenticated and authorised administrators.	
ADVANCED	1. The list of system administrators is regularly reviewed, e.g. every 6 months.	
14.8 ERROR MESSAGE MANAGEMENT: Error messages do not contain sensitive information that could compromise systems. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. The exception handling processes is configured to ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.	
ADVANCED	No additional requirements.	
14.9 PENETRATION TESTING: Network and application penetration tests are performed on a regular basis and following systems change. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Regular penetration testing for the presence of known vulnerabilities or common configuration errors is undertaken with third-parties to ensure that security controls have been well implemented and are effective.	
	In addition for PCI: • Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.	
	In addition for PSN:	

	• Regular IT Health Checks (ITHCs) are implemented to seek evidence that any security mechanisms put in place are ongoing and effective and identify any current vulnerability. ITHCs should normally be conducted annually, but may be employed more frequently where appropriate. • Issues identified in the ITHC (including systemic issues) are addressed. Critical and High risks are either be resolved immediately or by a viable plan for resolution. Medium and Low risks may be accepted or subject to remedial action plans.	
ADVANCED	No additional requirements.	
14.10 IP & DNS MANAGEMENT: Organisational IP ranges are known, recorded and managed; DNS changes and queries are effectively managed. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. The NCSC's ACD P-DNS service is implemented where appropriate and available.	
TARGET	1. The UK Public Sector DNS Service is used to resolve internet DNS queries.	
	2. Organisational IP ranges are known and recorded.	
ADVANCED	1. IP address traffic crossing the network boundary are monitored.	

DETECT: Category 15: Incident Detection

INCIDENT DETECTION	Organisations shall have in place monitoring systems and procedures to detect cyber-attacks.	
RESOURCES: NCSC Cyber Security Information Sharing Partnership; NCSC Logging Made Easy (for smaller organisations)		
15.1 DETECTION CAPABILITY: **Attempts to access or compromise systems are alerted, promptly assessed and investigated.** *[Click **here** to go to mappings]*		NOTES
BASELINE	Not specified.	
TARGET	1. Attackers attempting to use common cyber-attack techniques should not be able to gain access to data or any control of technology services without being detected.	
	For PSN: • Event data is collected and retained to detect actual or potential security incidents. • The organisation has a policy that describes the use cases to be detected, which define event data collection. • The policy includes both detection of technical attacks as well as important abuses of business processes.	
ADVANCED	1. Detection (and prevention and recovery) controls to protect against malware are in place.	
	2. Policy violations are detected against an agreed list of suspicious or undesirable behaviour.	
	3. There is the capability to investigate AV alerts.	
	4. Threat intelligence services are employed and used to inform anomalous activity profiles.	
	5. There is a sufficient understanding of normal system activity (e.g. which system components should and should not be communicating with each other) to ensure that searching for system abnormalities is an effective way of detecting malicious activity.	

	6. Descriptions of some system abnormalities that might signify malicious activity are maintained and updated, informed by past attacks and threat intelligence that takes into account the nature of attacks likely to impact on the networks and information systems.	
	7. Routine search for system abnormalities are undertaken and alerts generated.	
15.2 SECURITY MONITORING: Risk-based organisational monitoring policy and procedures are in place for the timely identification of security events. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. The network is monitored with intrusion detection and prevention solutions that are configured by qualified staff. These solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour. Coverage includes internal and host-based monitoring.	
	2. Inbound and outbound traffic traversing network boundaries is monitored to identify unusual activity or trends that could indicate attacks. Unusual network traffic (such as connections from unexpected IP ranges overseas) or large data transfers automatically generate security alerts.	
	3. Policies and processes are in place to promptly manage and respond to incidents detected by monitoring solutions.	
	4. Alerts generated by the system monitoring strategy are based on business need and an assessment of risk. This includes both technical and transactional monitoring as appropriate.	
	5. The monitoring capability has the ability to identify the unauthorised or accidental misuse of systems processing personal data and user access to that data, including anomalous user activity. It can tie specific users to suspicious activity.	
	6. A centralised capability has been deployed that can collect and analyse information and alerts from across the organisation. This is automated due to the	

	volume of data involved, enabling analysts to concentrate on anomalies or high priority alerts.	
	7. The monitoring and analysis of audit logs is supported by a centralised and synchronised timing source that is used across the entire organisation to support incident response and investigation.	
	8. Processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability.	
	In addition for PSN: • If you are using cloud services: Cloud Security Principle 5.3 *Protective Monitoring* should be factored into your overall monitoring strategy. Note that a cloud service will only provide monitoring with respect to the service provisioned. If you consume Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), you are responsible for monitoring of capability deployed onto the infrastructure. If you are consuming Software as a Service (SaaS), you should consider how you will be able to monitor for any potential abuse of business process or privilege.	
ADVANCED	1. As well as the network boundary, monitoring coverage includes internal and host-based monitoring.	
	2. The process for bringing new systems online includes considerations for access to monitoring data sources.	
	3. Monitoring staff: a) are responsible for investigating and reporting monitoring alerts. b) have roles and skills that covers all parts of the monitoring/investigation workflow. c) have workflows that address all governance reporting requirements, internal and external.	

	d) are empowered to look beyond fixed workflows to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	

RESPOND AND RECOVER: Category 16: Incident Management

INCIDENT MANAGEMENT	Well-defined incident management processes are in place, documented and regularly tested.	
RESOURCES: Scottish Government Common Incident Response Materials; Central Notification And Coordination Policy; NCSC Board Toolkit: Planning your response to cyber incidents; NCSC Exercise in a Box; NCSC Response and Recovery Guide		
16.1 INCIDENT RESPONSE PROTOCOL: **A risk-based and up-to-date incident response plan is in place.** *[Click **here** to go to mappings]*		NOTES
BASELINE	1. Cyber incident response policies and process are in place and these integrate with central cyber incident reporting , notification and coordination protocols.	
TARGET	1. There is an incident response capability and management plan in place, documented, with clear pre-defined processes, actions, roles and responsibilities and clear terms of reference for decision-making and incident management.	
	2. Specialist training is provided as required to the incident response team.	
	3. In the event of an incident the response team is provided with audit logs holding user activities, exceptions and information security events to assist in investigations.	
	4. The contact details of key personnel are readily available to use in the event of an incident.	
	5. The supporting policy, processes and plans are risk based and cover any legal or regulatory reporting requirements.	
	6. All incidents are recorded regardless of the need to report them.	
	7. All plans supporting security incident management (including business continuity and disaster recovery plans) are regularly tested.	
	8. The outcome of the tests and knowledge from incident management events are used to inform the future development of the incident management plans.	
	In addition for PSN:	

	• For incidents that impact on the PSN, these are reported to the PSN team and other entities as required.	
ADVANCED	1. The incident response plan is communicated and understood by the wider organisational business and integrated with supply chain response plans.	
	2. Thresholds for incident definitions, classifications and assessments are in place.	
	3. Procedures for the identification, collection, acquisition and preservation of evidence have been defined and implemented	
16.2 INCIDENT REPORTING PROCEDURE: Security events are reported through defined procedures known to staff. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. Cyber incident response policies and process are in place and these integrate with central cyber incident reporting , notification and coordination protocols.	
TARGET	1. The organisation promotes an incident reporting culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, with positive recognition and without fear of recrimination.	
	2. Users (employees and contractors) are security aware, know their responsibilities, and understand how to report any observed or suspected security weaknesses in systems or services and how to respond to incidents.	
	3. Users are encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination.	
	4. There are communication plans in place in the event of an incident and all internal and external reporting requirements are identified in the incident management plan. This includes notifying the relevant supervisory body, senior accountable individuals, the National Cyber Security Centre (NCSC), the Information Commissioner's Office (ICO) and law enforcement as applicable.	
ADVANCED	No additional requirement.	
16.3 STAFF TRAINING & TESTING: Staff are trained in incident response with assigned roles and responsibilities and the organisation carries out exercises to test response plans. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	Not specified.	
TARGET	1. A staff induction process is in place for new users (including contractors and third parties).	
	2. All employees receive regular training on the security risks to the organisation. This is tracked and refresher training is completed at suitable intervals.	
	3. Cyber security information and good practice guidance is easily and widely available.	
	4. Senior accountable individuals receive appropriate training and guidance on cyber security and risk management.	
	5. Employees in security roles are encouraged to develop and formally validate their security skills through recognised certifications and specialist training.	
	6. The effectiveness of security training and awareness activities is monitored and tested.	
ADVANCED	No additional requirements	
16.4 POST-INCIDENT REVIEW & LEARNING: The organisation reviews incidents and uses lessons learned from incidents to improve security measures. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	1. The senior team should take ownership of the lessons process to ensure that any actions required to improve the organisation's cyber resilience are undertaken.	
TARGET	1. Post-incident evidence is collected, preserved and analysed to identify and remedy the root cause.	
	2. Root cause analysis is conducted routinely as a key part of the lessons learned activities following an incident. This is comprehensive, covering organisational process issues, as well as vulnerabilities in networks, systems or software.	
	3. Lessons-learned reviews are conducted: actions taken during an incident are logged and reviewed to evaluate the performance of the incident management process.	
	4. Post incident lessons are assessed and lessons implemented into future iterations of the incident management plan and the monitoring capability.	

ADVANCED	1. There is a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.	
	2. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.	
	3. Improvements identified as a result of lessons learned exercises are prioritised, with the highest priority improvements completed quickly.	

RESPOND AND RECOVER: Category 17: Business Continuity

BUSINESS CONTINUITY	Information security continuity shall be embedded in the organisation's business continuity management systems	
RESOURCES: Scottish Government Common Incident Response Materials; Central Notification and Coordination Policy; NCSC Board Toolkit: Planning your response to cyber incidents; NCSC Exercise in a Box; DPIA Guidance; NCSC Response and Recovery Guide		
17.1 DATA RECOVERY CAPABILITY: Recovery controls are in place and tested to protect against information /data being lost or compromised. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. A data recovery capability is in place that includes a systematic approach to the backup of essential data.	
ADVANCED	1. The organisation has applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.	
17.2 BACKUP POLICIES & PROCEDURES: Backup copies of information, software and system images shall be taken and tested regularly.		**NOTES**
BASELINE	Not specified.	
TARGET	1. There is a backup policy and measures are in place to routinely maintain backup media.	
	2. The ability to recover archived data for operational use is regularly tested.	
	3. Physical backup media (where used) is held in a physically secure location, offsite.	
ADVANCED	1. Backup copies of information, data, software and system images are taken, tested, documented and routinely reviewed.	
	2. There are secured backups of data to allow services to continue should the original data not be available.	
	3. Automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.	
17.3 DISASTER RECOVERY POLICIES & PROCEDURES: The organisation has well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise. *[Click **here** to go to mappings]*		**NOTES**

BASELINE	Not specified.	
TARGET	1. Contingency mechanisms to continue to deliver services in the event of any failure, forced shutdown, or compromise of any system or service have been identified, documented and tested.	
	2. Restoring data and services to normal operation is a well-practised scenario.	
ADVANCED	1. Disaster recovery plans and processes have been tested for practicality, effectiveness and completeness.	
	2. Restore times to operational service are known and documented.	
	3. The resources needed to carry out any required response activities are known, with arrangements in place to make these resources available.	
	4. You understand the types of information that will likely be needed to inform response decisions, and arrangements are in place to make this information available, including with third-party suppliers as appropriate and where required.	
	5. Disaster response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.	
	6. Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.	
17.4 BC/DR Testing Policies & Procedures: Scenario-based exercises and processes to test recovery response plans are planned and performed. *[Click **here** to go to mappings]*		**Notes**
BASELINE	Not specified.	
TARGET	1. Contingency mechanisms have been identified and tested to enable service continuity in the event of any failure, forced shutdown, or compromise of any system or service.	

	2. Restoring the service to normal operation is a well-practised scenario.	
ADVANCED	1. The established and implemented information security continuity controls are tested and reviewed at regular intervals in order to ensure that they are valid and effective.	
	2. Business continuity and disaster recovery plans are tested for practicality, effectiveness and completeness to ensure they remain valid.	
	3. Exercise scenarios are based on incidents experienced by the organisation, other organisations, or are composed using experience or threat intelligence.	
	4. Exercise scenarios are documented, regularly reviewed, and validated.	
	5. Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.	
	6. Exercises test all parts of the response cycle relating to particular services or scenarios (e.g. restoration of normal service levels).	
17.5 DATA PROTECTION IMPACT ASSESSMENTS (DPIA): DPIAs are undertaken to determine the impact of the intended processing on the protection of personal data where the processing is likely to result in a high risk to the rights and freedoms of individuals. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. The impact of loss of availability of the service is known, understood and mitigated.	

ADVANCED	1. The impact on your service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data, are understood and documented.	
	2. You validate these impact statements regularly, e.g. annually.	
17.6 BC CONTINGENCY PLAN: Contingency mechanisms are in place to continue to deliver services in the event of any failure or compromise of any system or service. *[Click **here** to go to mappings]*		**NOTES**
BASELINE	Not specified.	
TARGET	1. Contingency mechanisms to continue to deliver services in the event of any failure, forced shutdown, or compromise of any system or service are identified, documented, and implemented.	
ADVANCED	1. Suitable alternative transmission paths are available where there is a risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).	
	2. Information security continuity is embedded in the organisation's wider business continuity management planning.	
	3. Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.	
	4. The resources that will be needed to carry out any required response activities, and arrangements are in place to make these resources available.	
	5. The types of information that will likely be needed to inform response decisions are known and documented and arrangements are in place to make this information available.	
	6. Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.	
	7. Where necessary, arrangements are in place to augment incident response capabilities with external support (e.g. specialist providers of cyber incident response capability).	

Annex A: Standards Mapping Matrix

Annex A – Standards Mapping Matrix

TABLE A1.1: Domains, Categories and Sub-categories mapped to standards and frameworks.
The numbers in each subcategory cross-reference to the respective standards or frameworks.

	Category/Sub Category	CE	PSN	PCI	PSAP	10 Steps	GDPR	HMG SPF	ISO 27001	NIS	Dig. First
MANAGE	**ORGANISATIONAL GOVERNANCE**										
	Governance framework				2	1.1	A1	1a	5.1a, 5.1f	A1.a	
	Leadership & responsibility				2			1a	5.1a	A1.b	
	- SMT				2				5.1f	A1.a	
	- Board				2	Intro			5.1f	A1.a, A1.c	
	Adoption of assurance standards				4	1.6			5.1, 5.2	A2.b	12
	Information Asset Register				2		A3	2a	A8.1.1 A8.1.2		
	Audit/assurance compliance		7		4			1d	A12.7.1 A18.2.1 A18.2.2 A18.2.2	A2.b	
	RISK MANAGEMENT										
	Risk management policy & process				2	1.4	A1	1c	6.1.2	A1.b; 1.c; A2.a; B1.a	12
	Cyber / Information Risk Assessment		4	6, 12	2	1.2; 10.1	A2	1c; 2e	6.1.2	A1.c; A2.a; B1.a	
	Risk treatment & tolerance				2	1.2	A2	1c	6.1.3	A1.c	
	Risk governance				2	1.1	A2		6.1.3	A1.c	
	- Risk assurance & management				2	1.2; 1.7			6.1.3	A1.b	
	- Risk register review				2	1.1				A2.a	
	- Board responsibility				2	1.3				A1.a	
	- Risk training & culture				6	1.8; 1.9		1e		A1.c	
	SUPPLIER MANAGEMENT										
	Supply chain security assurance & management		5		8		A4	1d	A13.2.2 A13.2.4 A15.1 A15.2	A4.a; B2.b	
	Roles & responsibilities defined							6a.6		A4.a	
	Access control									A4.a; B2.b	

	Security in system procurements								A14.1.1	A4.a	
	ASSET MANAGEMENT								A8.1		
	Hardware assets register & management			12		2.3	B4	2d; 6a.1; 6b.1	A8.1.1 A8.1.2 A8.1.3 A8.1.4 A11.2.5 A11.2.6 A11.2.7	A3.a	
	Software assets register & management	2			4	2.3		6a.1	A8.1.1 A8.1.2 A8.1.3 A8.1.4 A12.6.2	A3.a	
	Infrastructure management								A11.2.1 A11.2.2 A11.2.3 A11.2.4	A3.a	
	INFORMATION SECURITY MANAGEMENT										
	Security policy & processes		1a	12.2 , 12.3			A1; B1	1b	A5.1 A9.1.1 A12.1.1 A18.1.1 A18.1.2 A18.1.3 A18.1.4	B1.a	12
	Lifecycle management			3, 9		9.6	A3	2b	A8.2.3 A8.3.2	A3.a; B3.a; B3.d	12
	Storage			9				2c		B3.a; B3.c	
	- cloud/3rd party			9			B3			A4.a; B3.a	18
	- on premise			9			B3			B3.a	
	Information/data classification						A2	2a	A8.2.1 A8.2.2 A8.2.3	B3.a	
	Information assets register						A3	2a	A8.2.1 A8.2.3	A3.a; B3.a	
	Information/data transfer controls		4	4		10.4; 10.5	B2; B3	2d; 6d	A8.3.3 A13.2.1 A14.1.3	A4.a; B3.a; B3.b	
	PEOPLE										
	Prior to employment								A7.1		
	- Security screening		6						A7.1.1		
	- T&C								A7.1.2		
	During employment								A7.2		
	- induction					5.2			A7.2.1 A7.2.2	B6.b	
PROTECT	- security roles & responsibilities			12					A61.1 A7.2.1 A7.3.1	A1.b; B1.a; C1.e	

	- acceptable use policy		1d			5.1; 9.1			A7.2.1 A9.3.1 A11.2.8 A11.2.9	B1.a	
	- disciplinary procedures					5.7			A7.2.3	B1.a	
	Staff training & awareness culture			12	6	4.7; 5.3; 5.5; 9.7; 10.2	B5	1e	A7.2.2	A1.b; B1.a; B6.a; B6.c; C1.e	
	Staff skills assessment					5.4					
	- Board										
	- SMT									B6.c	
	- Staff									A1.b; B6.b	
	- Interim & contractor										
	Mobile/remote working policy		3						A6.2.1 A6.2.2 A14.1.2.	B3.d	
	SERVICES RESILIENCE							3a,b,c	A17.2.1	B5.b	10
	ACCESS CONTROL	3			4		B2		A9.1	B3.a	
	Account management	2, 3	2	7	4	4.1		4b	A9.1.2 A9.2 A9.4.1 A12.6.2	B2.a; B2.c	
	Identity authentication	3	2	8		4.2	B2	5b	A9.4.1	B2.a; B2.d	
	- Password policy	1, 2	2	2	4		B2	7c	A9.4.3		
	- Multi factor authentication						B2	7b	A9.4.3	B2.a; B2.c	
	Privilege management	3	2; 5	7	4	4.1; 4.3	B2	4a; 5a,b	A9.1.2A 9.2.3 A9.4.4	B2.a; B2.c; B4.c; C1.b	
									A9.4.5		
	Administrator account management	3	5	7	4	4.4; 4.6	B2	5a	A9.1.2 A9.2.3 A9.4.4 A9.4.5	B2.a; B4.c	
									A12.4.3		
	MEDIA MANAGEMENT								A8.1		
	Storage media management			9		9.2; 9.3; 9.4; 9.5	B4	6b.1	A8.1.1 A8.1.2 A8.1.3 A8.1.4 A8.3.2	B3.d B3.e	
	-Mobile media/devices					2.7; 9.2; 9.5; 9.6	B3	6b.1; 6b.4	A6.2 A8.1.1 A8.1.2 A8.3.1 A8.3.3	B3.a; B3.d B3.e	
	Cryptography			3, 4		9.5	B4	6b.4	A10.1 A18.1.5	B3.b; B3.c	
	Remote wipe capability							6b.5		B3.d	

	ENVIRONMENTAL SECURITY										
	Equipment location								A11.1.4 A11.2.1		
	Power resilience								A11.2.2	A3a	
	PHYSICAL/BUILDING SECURITY										
	Access control		1c	9					A11.1 A11.1.2		
	Internal security		1c	9					A11.1 A11.1.3 A11.1.6		
	SYSTEM MANAGEMENT										
	Secure configuration	2	1b		4	2.4; 10.3	B4	6a.2; 6d.2	A12.4.4 A12.5.1	B4.b	
	Secure design/development			6					A12.1.3 A14.2.1 A14.2.3 A14.2.5 A14.2.6 A14.2.7 A14.2.8	B4.a	
	Change control procedures					2.6; 2.9	B4		A12.1.2 A14.2.2 A14.2.4	B4.b	
	System Testing		7	11			B4	6a.3; 6d.4	A.2.1.3 A14.2.3 A14.2.8 A14.2.9 A14.3.1	B4.d	
	OPERATIONAL SECURITY						B4; C1				
	Malware policies & protection	4	1b	5	4	5.1; 7.1		1b	A12.2.1	B4.c	12
	- AV screening	4		5	4	7.5; 7.6.1		6c.3		B4.c	
	- Media scanning	4			4	7.5					
	- File scanning	4			4	7.5					
	Email security				5			6c.1; 6c.2	A13.2.3		
	Application security				5			6d.1			
	Vulnerability management & scanning		1a	5, 6, 11	5	2.5			A12.6.1	A2.b; B2.b; B4.a; B4.d	12
	- Executables prevention	4			4, 5	3.1.2; 7.2; 7.5				B4.b	
	- Peripheral device management					2.7					
	Data exfiltration monitoring					7.2				C1.a	
	Software supported & updated	4, 5		5	4, 5	2.1	B4	6b.3		B4.d	12

	Web site screening	4			4	7.3					
	Browser management					7.6.4					
	Monitor/audit user activity			10		4.5; 8.4	B2; C1		A12.4.1 A12.4.3	B2.c; B2.d; C1.a	
	Disabled auto-run	2				7.6.5					
	NETWORK SECURITY						B4		A13.1		
	Patch management	5	1a	6	4	2.2	B4	6a.2; 6b.3		B4.d	12
	Device management		3			2.7; 7.5; 7.6.6 10.3	B4	5b; 6b.2; 6b.4		B2.b; B2.c; B4.c	
	Content screening					3.1.2; 7.2; 7.4; 7.5.3				B4.a	
	Internal segregation					3.2.1			A.12.1.3 A13.1.3	B4.a; B5.b	
	Wireless security	2				3.2.3					
	Boundary/Firewall management	1	3	1, 6	4	3.1.17 .6.3				B4.a	
	Administrator control					3.2.4		6a.5	A.12.4.3	B2.c	
	Error message management					3.2.5					
	Penetration testing		7	11		3.2.6		6a.3	A.14.2.9	B4.d	
	IP & DNS management							6a.4; 6a.6		C1.a	
DETECT	**INCIDENT DETECTION**										
	Detection capability		1d					8d	A12.2.1	B2.d; B4.c C1.a; C1.c; C1.d; C2.a; C2.b	
	Security Monitoring		1d			3.2.58 .1 8.2 8.3 8.4 8.5 8.6 8.7	C1	8b 8c 8e	A12.4	C1.a; C1.e	
RESPOND & RECOVER	**INCIDENT MANAGEMENT**										
	Incident response protocol		1d; 1e	12	7	6.1; 6.3; 6.5; 8.8; 10.6	C1	8a; 9a	A12.2.1 A16.1.1 A16.1.4 A16.1.5	D1.a	10
	Incident reporting procedure		1d; 1e		7	5.6; 6.6; 6.9; 6.10	C1, D2	9a; 9b; 9c	A12.4 A16.1.2 A16.1.3	B6.a; D1.a	
	Staff training & testing					5.2; 5.3	D1	9a; 9d	A7.2.2 A12.2.1	B6.a; B6b; B6.c	

	Post-incident review & learning		1.e		3	6.7; 6.8; 8.9	D2	9d; 9e; 9f; 10c	A16.1.6 A16.1.7	D2.a; D2.b	
	BUSINESS CONTINUITY						D1				
	Data recovery capability					6.4	D1		A12.3.1	B3.c; D1.a	10
	Back up policies & procedures						D1		A12.3.1	B3.c; B5.c	
	Disaster recovery policies & procedures						D1	10a	A12.3.1 A17.1.1 A17.1.2	B3.c; B5.a; B5.c; D1.b	10
	BC/DR testing policies & procedures						D1	10a; 10b	A12.3.1 A17.1.3	B5.a; B5.c; D1.c	10
	Data Loss impact assessments							3d		B3.a	
	BC contingency plan							10a	A17.1.1 A17.2.1	A3.a; B3.b; D1.a	10
	SUMMARY	**CE**	**PSN**	**PCI**	**PSAP**	**10 Steps**	**GDPR**	**HMG SPF**	**ISO 27001**	**NIS**	**Dig. First**
	% of sub-categories included within each framework/standard	**18%**	**31%**	**31%**	**39%**	**58%**	**60%**	**62%**	**72%**	**80%**	**15%**

TABLE A2.1 – FRAMEWORK CONTROLS AND MAPPING MATRIX

NB: You can click on any reference in the table below to be taken to the source wording in the original standard/guidance document at Annex B (Note: the ISO standard is not reproduced for reasons of copyright).

		Requirements aligned with the following core standards and guidance									
1. ORGANISATIONAL GOVERNANCE	**Appropriate organisational structures, policies, and are processes in place to understand, assess and systematically manage security risks to the network and information systems.**										
1.1 GOVERNANCE FRAMEWORK: You have effective organisational security management led at board level and articulated clearly in corresponding policies. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. There is a Board/Senior Management-level commitment to manage the risks arising from the cyber threat				2						
TARGET	1. There are appropriate data protection and information security policies and processes in place to direct the organisations overall approach to cyber security. 2. The personal data processed is catalogued and the purpose for processing it is defined and described. 3. There are clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services.					1.1	A1	1a			

	4. Senior accountable individuals have received appropriate training and guidance on cyber security and risk management. 5. There is a culture of awareness and education about cyber security across the organisation.										
ADVANCED	1. Significant risks to sensitive information and key operational services have been identified and are managed. 2. The security issues that arise because of dependencies on external suppliers or through the supply chain are detailed, organised and managed.								5.1a 5.1f	A1.a	
1.2 LEADERSHIP & RESPONSIBILITY: There is a board-level individual who has overall accountability for the security of networks and information systems. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	1. A named Board and Senior Management member of staff have been identified as responsible for organisational cyber resilience arrangements 2. Clear lines of responsibility and accountability to named individuals for the cyber resilience of sensitive information and key operational services have been defined and understood. 3. There is a written information security policy in place, which is championed by senior management. 4. There is regular staff training in cyber security and information risk management.				2						

TARGET	1. Senior accountable individuals have received appropriate training and guidance on cyber security and risk management. 2. There is a culture of awareness and education about cyber security across the organisation.										
ADVANCED	1. Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems 2. The board shall ensure that the organisation has planned and budgeted for adequate resources for the delivery, maintenance and improvement of cyber resilience and network and information security, and that these activities are supported by senior management. 3. The organisation has established roles and responsibilities for the security of networks and information systems at all levels, 4. There are clear and well-understood channels for communicating and escalating risks 5. There is senior-level accountability for the security of networks and information systems with delegated decision-making authority.							1a	5.1a 5.1f	A1.a A1.b A1.c	
1.3 ADOPTION OF ASSURANCE STANDARDS: There is demonstrable confidence in the effectiveness of the security of the organisations technology, people and processes.		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

[Click here to return to Framework]											
BASELINE	1. There is demonstrable and appropriate independent assurance that the five critical network controls of Cyber Essentials are in place: f) firewalls g) secure configuration h) user access control i) malware protection j) patch management				4						
TARGET	1. The organisation has obtained assurance that suppliers of 3rd party services have appropriate, proportional and adequate cyber security policies and practices that are certified or aligned with recognised standards or their equivalent. (e.g. HMG Cyber Security Standard, Cyber Essentials, ISO 27001).					1.6					
ADVANCED	1. Security as it relates to technology, people, and processes can be demonstrated and verified by a third party audit. 2. There are procedures to ensure security measures that are in place to protect the networks and information systems are effective, and remain effective for the service lifetime. 3. The assurance methods available are recognised and appropriate methods to gain confidence in the security of essential services are adopted and implemented.								5.1 5.2	A2.b	

1.4 INFORMATION ASSET REGISTER: There is a catalogue of sensitive information and stored with appropriate management procedures. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Key information assets have been identified and recorded. 2. Key information assets have been assessed for their vulnerability to cyber-attack.				2						
TARGET	1. Organisations shall know and record: f) What sensitive information they hold or process g) Why they hold or process that information h) Where the information is held i) Which computer systems or services process it j) The impact of its loss, compromise or disclosure						A3	2a			
ADVANCED	1. Assets associated with information and information processing have been identified 2. An inventory of these assets has been established and is maintained through recognised process. 3. Assets maintained in the inventory have ascribed owners.								A8.1.1 A8.1.2		
1.5 AUDIT/ASSURANCE COMPLIANCE: There are in place procedures to provide assurance on the security of systems and services. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

BASELINE	1. There is demonstrable and appropriate independent assurance that the five critical network controls of Cyber Essentials are in place: f) firewalls g) secure configuration h) user access control i) malware protection j) patch management				4						
TARGET	1. The organisation has obtained assurance that suppliers of 3rd party services have appropriate, proportional and adequate cyber security policies and practices that are certified or aligned with recognised standards or their equivalent. (e.g. HMG Cyber Security Standard, Cyber Essentials, ISO 27001). **In addition for PSN:** You must implement regular IT Health Checks and ensure the IA conditions of the PSN Code of Connection are met.		7					1d			
ADVANCED	1. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes. 2. The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.								A12.7.1 A18.2.1 A18.2.2	A2.b	

	3. Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.										
2. RISK MANAGEMENT	**Appropriate steps are in place to identify, assess and understand security risks to the network and information systems. This includes an overall organisational approach to risk management.**										
2.1 POLICY & PROCESSES: Your organisation has effective internal processes that manage and mitigate risks to the security of network and information systems and services. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. There are information risk management policies and assessment procedures in place				2						12
TARGET	1. Organisations shall identify and manage the significant risks to sensitive information and key operational services. 2. Senior management and boards regularly review the organisational cyber risks and threats.					1.4	A1	1c			
ADVANCED	1. The organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. 2. Risk owners are identified.								6.1.2	A1.b A1.c A2.a B1.a	

	3. The output from the risk management process is a clear set of security requirements that will address the risks in line with the organisational approach to security 4. Significant conclusions reached in the course of the risk management process are communicated to key security decision-makers and accountable individuals. 5. The effectiveness of the risk management process is reviewed periodically and improvements made as required.										
2.2 CYBER / INFORMATION RISK ASSESSMENT: The organisation has effective and robust risk assessment methodology and processes that identify and prioritise threats and vulnerabilities. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Key information and IT assets have been identified, thoroughly risk assessed and prioritised for their vulnerability to cyber-attack.				2						12
TARGET	1. Organisations should establish a process to identify security vulnerabilities and rank them according to their level of risk. 2. A systematic risk-based approach is taken to information security, data protection and the security of systems and services. This risk assessment takes into consideration: the technology available, cost of implementation, the nature, scope, context and purpose of any data		4	6 12		1.2 10.1	A2	1c 2e			

	processing, the probability and impact of the risk being realised. 3. The criteria for performing risk assessments are well defined to ensure risk assessments produce consistent, valid and comparable results.										
ADVANCED	1. The risk assessments are based on a clearly articulated set of threat assumptions; these are kept up-to-date through an understanding of changing security threats. 2. Risk assessments are conducted when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat 3. The risk assessments are dynamic and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.								6.1.2	A1.c A2.a B1.a	
2.3 RISK TREATMENT & TOLERANCE: The organisation has risk treatment policies and procedures in place with defined risk appetite and mitigation controls documented. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Key information and IT assets have been identified, thoroughly risk assessed and prioritised for their vulnerability to cyber-attack.				2						12

TARGET	1. The information and cyber risk that the organisation is prepared to tolerate is defined, understood and communicated. 2. A risk appetite statement shall be produced and used to guide risk management decisions.					1.2	A2	1c			
ADVANCED	1. The organization shall define and apply an information security risk treatment process that identifies appropriate risk treatment options and associated mitigation controls. 2. A risk treatment plan shall be produced 3. A Statement of Applicability shall be prepared to document the risk treatment and controls adopted. 4. The senior management shall assess and sign-off the risk treatment regime, policies and procedures.								6.1.3	A1.c	
2.4 RISK GOVERNANCE: Risks to network and information systems effectively managed, communicated, regularly considered throughout the organisation and led by senior management. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	1. Responsibility for cyber security risks have been allocated appropriately with named individuals. 2. Cyber security risks are on the organisational risk register 3. Knowledge sharing of risk management through peer-networks and membership of CiSP is actively undertaken.				2 6						
TARGET	1. The board routinely reviews cyber risks which are a standing agenda item.					1.1 1.2 1.3	A2	1c 1e			

	2. There is board-level accountability for cyber risk with a named individual. 3. Staff members are trained in cyber risk assessment and management relevant to their role. 4. An organisation-wide risk management culture is promoted by the senior management with demonstrable participation at all levels.					1.7 1.8 1.9					
ADVANCED	1. Senior accountable officers receive appropriate training and guidance on cyber security and risk management. 2. Senior management regularly reviews the resource allocations to ensure these are sufficient to permit prioritised information security and cyber risk mitigation measures to be implemented.								6.1.3	A1.a A1.b A1.c	
3. SUPPLIER MANAGEMENT	**The organisation understands and manages security risks to that arise as a result of dependencies on external suppliers and third party services.**										
3.1 SUPPLY CHAIN ASSURANCE: The organisation has a deep understanding of the security provisions and assurances around systems and services provided by third parties and their supply chain. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified.										
TARGET	1. Organisations shall adopt a proportionate, risk-based policy in respect of supply chain cyber security. Specifically, they shall implement the		5		8		A4	1d			

	Scottish Public Sector Guidance Note on Supplier Cyber Security from Financial Year 2019-20. 2. Organisations that adopt cloud-based services shall ensure the NCSC 14 principles of cloud security are adopted from Financial year 2019-20. 3. The organisation has assessed, understands and has procedures in place to manage security risks that may arise as a result of dependencies on third party suppliers. 4. Documented and suitable assurances have been obtained from suppliers and their immediate supply chain that proportionate and appropriate security measures to protect systems, services, data and information are in place. 5. The security requirements and stipulations necessary to ensure GDPR and other regulatory compliance are incorporated into supplier contracts, are mutually agreed and understood..										
ADVANCED	No additional requirements								A13.2.2 A13.2.4 A15.1 A15.2	A4.a B2.b	

3.2 ROLES AND RESPONSIBILITIES: The organisation has defined the respective duties and responsibilities of third-party suppliers and the supply chain and these are understand and agreed by all parties. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified.										
TARGET	1. Where services are outsourced (for example by use of cloud infrastructure or services), you shall understand and accurately record which security related responsibilities remain with the organisation and which are the supplier's responsibility. 2. It is essential, where cloud services are employed (particularly with respect to IaaS and PaaS), that there is clarity (whether through contractual agreement or other arrangements) whether the responsibility to carry out certain actions (i.e. patching) lies with the organisation or the cloud supplier.							6a.6			
ADVANCED	1. There is a clear and documented shared-responsibility model with suppliers for incident management.									A4.a	

3.3 ACCESS CONTROL: There is visibility and control on third-party users (or automated functions) that can access organisational systems, services, data and information data and these are appropriately verified, authenticated and authorised. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified										
TARGET	Not specified										
ADVANCED	1. Only individually authenticated and authorised users can connect to or access your networks or information systems. 2. Both electronic and physical access requires individual authentication and authorisation. 3. Where cloud-based services are employed, there is sufficient separation of the organisation's data and service from other users of the service. 4. User access to all your networks and information systems is limited to the minimum necessary. 5. Additional authentication mechanisms, such as two-factor or hardware-backed certificates are employed, to individually authenticate and authorise all remote access to all networks and information systems that support essential services. 6. The list of external users with access to essential service networks and systems is reviewed on a regular basis, e.g. every 6 months.									A4.a B2.b	

3.4 SECURITY IN PROCUREMENTS: The organisation has security embedded within procurement procedures. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified										
TARGET	Not specified										
ADVANCED	1. The cyber risk and information security related requirements shall be considered as an integral part of the procurement process and, where relevant, included in tender requirements for new systems, services or enhancements to existing provisions. 2. Organisations shall regularly monitor, review and audit supplier service delivery and associated security provisions. 3. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.								A14.1.1		
4. ASSET MANAGEMENT	**Everything required to deliver, maintain or support networks and information**										

	systems and services is determined and understood.										
4.1 HARDWARE ASSETS: The organisation has visibility and effective management of all hardware assets. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified										
TARGET	1. All hardware assets and their configuration are tracked and recorded, including end user devices and removable media. 2. End user devices are managed to enable organisational controls to be applied over software or applications **In addition for PSN:** 1. The security of End User Devices (EUDs) meets the CESG guidance on End User Devices Security Principles and BYOD Guidance: Device Security Considerations.		IA Para 4	12		2.3	B4	2d 6a.1 6b.1			
ADVANCED	1. All assets are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. 2. Assets are securely managed throughout their lifecycle, from creation through to eventual decommissioning or disposal. 3. All items of equipment containing storage media shall be verified to ensure that any sensitive data								A8.1.1 A8.1.2 A8.1.3 A8.1.4 A11.2.5 A11.2.6 A11.2.7	A3.a	

	and licensed software has been removed or securely overwritten prior to disposal or re-use. 4. Assets are prioritised according to their importance to the delivery of the essential service. 5. Responsibility for managing the physical assets has been assigned 6. Assets management is in place; assets shall not be taken off-site without prior authorisation with associated documentation. 7. Security is applied to all asset used off-site.										
4.2 SOFTWARE ASSETS: The organisation has visibility and effective management of all software assets. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	1. All its software is maintained and up to date. 2. Software must: ➢ be licensed and supported ➢ be removed from devices when no longer supported ➢ Critical or High risk vulnerabilities are patched within 14 days of an update being released ➢ have other mitigating steps must be in place where patches cannot be applied	2			4						
TARGET	1. All software assets with licence and configuration details must be tracked and recorded 2. Software vulnerabilities monitoring, including using in-support software, must be implemented.					2.3		6a.1			
ADVANCED	1. The installation of software shall be controlled and shall not be permitted by general users.								A8.1.1 A8.1.2	A3.a	

									A8.1.3 A8.1.4 A12.6.2		
4.3 INFRASTRUCTURE MANAGEMENT: The organisation recognises critical infrastructure assets and dependencies. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified										
TARGET	1. Critical infrastructure assets are identified; threats evaluated and proportionate security measures are in place.							3.a			
ADVANCED	1. Network assets shall be regularly maintained to ensure service continuity. 2. Network assets shall be protected from power surges and failures. 3. Dependencies on supporting infrastructure (e.g. power, cooling etc.) shall be identified and recorded. 4. Equipment and devices on premise shall be sited to ensure protection from external and internal environmental risks (e.g. water ingress)								A11.2.1 A11.2.2 A11.2.3 A11.2.4		
5. INFORMATION SECURITY MANAGEMENT	**Proportionate security measures in place to protect information, data, services and systems from cyber attack.**										
5.1 SECURITY POLICY & PROCESSES: The organisation has developed and continues to improve a set of protection policies and processes that		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

manage and mitigate the risk of security-related service disruption or data loss. [Click here to return to Framework]											
BASELINE	Not specified										
TARGET	1. Appropriate policies and processes that direct the organisation's overall approach to securing systems are defined, implemented, communicated and enforced. 2. Security governance, risk assessment and technical security practices are documented. 3. Each organisation shall determine the boundaries and scope of its security policy. This should be defined to cover all relevant operations, which shall include interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations. 4. Security governance, risk assessment and technical security practices are documented. 5. Key security performance indicators are defined and reported to the executive management. 6. Acceptable usage policies that define the proper use of technology by all personnel are in place. (These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.) 7. The security policy and procedures clearly define information security responsibilities for all personnel.		1a	12.1 12.2 12.3			A1 B1	1b			12

ADVANCED	1. Policies and processes are reviewed at suitably regular intervals to ensure they remain relevant to threats, business processes, accommodate lessons learned and remain appropriate and effective. 2. Security policies and processes are integrated with other organisational policies and processes. 3. All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date.								A5.1 A9.1.1 A12.1 A18.1.1 A18.1.2 A18.1.3 A18.1.4	B1.a	
5.2 LIFECYCLE MANAGEMENT: Information assets are managed throughout their lifecycle, from creation through to eventual decommissioning or disposal. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Information and data should be classified according to retention and disposal policies and legal requirements. 2. Where removable media is to be reused or destroyed then appropriate steps should be taken to ensure that previously stored information will not be accessible. 3. Personal data processed should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary. 4. The rationale for collecting, holding or processing personal information should be documented.			3 9		9.6	A3	2b			12

	5. Technical controls are in place to prevent unauthorised or unlawful processing of personal data that might remain in memory when technology is sent for repair or disposal. 6. Information and data records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislation, regulatory, contractual or business requirements. **In addition for PCI:** 7. Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in the data retention policy. 8. Purge unnecessary stored data at least quarterly. 9. Do not store sensitive authentication data after authorisation (even if it is encrypted).										
ADVANCED	1. Information, data and media destruction and disposal processes should have assurance procedures and have an audit trail from collection to destruction.								A8.2.3 A8.3.2	A3.a B3.a B3.d	
5.3 STORAGE: The organisation knows where data and information are stored and has security in place whether on premise, mobile, removable or cloud based storage is employed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. There are suitable physical or technical means to protect stored data from unauthorised access,			9			B3	2c			18

	modification or deletion through unauthorised access to storage media.										
ADVANCED	1. There is a detailed understanding and mapping of data and information flows from creation, transit and storage. 2. The organisation has processes to remove or minimise unnecessary copies or unneeded historic records. 3. Where outsourced or third-party storage is employed, appropriate secured measures are in place and enforced, with appropriate assurance procedures consistent with data retention policies. 4. All data is sanitised from all devices, equipment or removable media before disposal.									A4.a B3.a B3.c	
5.4 INFORMATION / DATA CLASSIFICATION: Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification to ensure it receives an appropriate level of protection in accordance with its importance to the organization. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified										

TARGET	1. Organisations shall know and record the information they hold or process.						A2	2a			
ADVANCED	1. All data and information assets have been identified and classified. 2. Information has been classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. 3. An appropriate set of procedures for information labelling has been developed and implemented in accordance with the information classification scheme adopted by the organization								A8.2.1 A8.2.2 A8.2.3	B3.a	
5.5 INFORMATION ASSETS REGISTER: Data and information assets are identified and an inventory of these assets is created and maintained. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified.										
TARGET	1. All data and information assets have been catalogued by type and classification and recorded in an information assets register. 2. The register records where the information/data are held and which computer systems or services process it. 3. The purpose for processing the personal data held by the organisation has been described and recorded.						A3	2a			
ADVANCED	1. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme.								A8.2.1 A8.2.3	A3.a B3.a	

	2. The register maintains a current understanding of the location, quantity and quality of data and information stored.										
5.6 INFORMATION / DATA TRANSFER CONTROLS: The organisation has an understanding of information / data flows including the transfer of data to third parties and the associated security protocols that are in place. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified.										
TARGET	1. Data at rest on all devices is protected by appropriate measures including physical protection (when hosted within a secure data centre) and encryption. 2. There are technical controls in place (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest 3. Data in transit accessed by remote workers and third parties is protected by encryption and the application of a virtual private network (VPN). 4. Protect data in transit using well-configured TLS v1.2. **In addition for PCI:** 5. Strong cryptography and security protocols such as SSL/TLS, SSH or IPSec are employed to safeguard sensitive cardholder data during transmission over open, public networks.		4	4		10.4 10.5	B2 B3	2d 6d			

	6. Wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g. IEEE 802.11i) to implement strong encryption for authentication and transmission. 7. The use of WEP as a security control is prohibited. 8. Unprotected PANs are not sent by end user messaging technologies.										
ADVANCED	1. There is a current understanding and record of the data links and routes used to transmit data. 2. Appropriate physical or technical means are applied to protect data that travels over an untrusted carrier. 3. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. 4. Agreements shall address the secure transfer of business information between the organization and external parties.								A8.3.3 A13.2.1 A14.1.3	A4.a B3.a B3.b	
6. PEOPLE	**The organisation has policies and procedures in place to ensure staff and contractors are screened, trained and know their security responsibilities.**										

6.1 PRIOR TO EMPLOYMENT: Employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified										
TARGET	**In addition for PSN:** 1. For users who have administrative privileges, pre-employment checks which are aligned with the Baseline Personnel Security Standard (BPSS) should be implemented.		6								
ADVANCED	1. Pre-employment checks have been performed on all candidates proportional to the role and responsibilities, the classification of the information to be accessed and the perceived risks. 2. Employee and contractor contract terms and conditions shall state their responsibilities for information security.								A7.1 A7.1.1 A7.1.2		
6.2 DURING EMPLOYMENT: Staff and contractors are aware of and fulfil their cyber security & information security responsibilities. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. A staff induction process is in place for new users (including contractors and third party users). 2. As part of the induction process staff are made aware of their personal responsibility and obligations to comply with the corporate security policies with regards to system security, data handling, and acceptable use.		1d	12		5.1 5.2 5.7 9.1					

	3. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action. 4. Acceptable usage policies are in place that include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet. 5. The security policy and procedures clearly define information security responsibilities for all personnel.										
ADVANCED	1. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced. 2. All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement. 3. There are 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. 4. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. 5. Users shall ensure that unattended equipment has appropriate protection.								A6.1.1 A6.1.2 A7.2.1 A7.2.3 A7.3.1 A9.3.1 A11.2.8 A11.2.9	A1.b B1.a B6.b C1.e	

	6. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.										
6.3 STAFF TRAINING & AWARENESS CULTURE: All employees and contractors receive appropriate awareness education and training with regular assessments and updates as relevant for their job function. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Appropriate staff training, awareness-raising and disciplinary processes with regard to cyber resilience are in place for staff at all organisational levels.				6						
TARGET	1. All users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies including removable media security and mobile device utilisation. 2. All users should receive regular refresher training on the security risks to the organisation. 3. The effectiveness of security training is monitored to test the effectiveness and value of the security training provided to all users. 4. Employees receive appropriate training, support and technology to help them manage personal data securely. 5. Senior accountable individuals receive appropriate training and guidance on cyber security and risk management and promote a culture of awareness and education about cyber security across the organisation..				12		4.7 5.3 5.5 9.7 10.2	B5	1e			

ADVANCED	1. Individuals' cyber security training is monitored to ensure update training is completed and delivered at regular intervals. 2. Cyber security training and awareness activities are evaluated for efficacy.								7.4 A7.2.2	A1.b B1.a B6.a B6.b C1.e	
6.4 STAFF SKILLS ASSESSMENT: Staff, including SMT and board members, are appropriately trained in cyber security and risk assessment. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified										
TARGET	1. A formal assessment of security skills is undertaken. 2. Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognised certification scheme.					5.4					
ADVANCED	1. Necessary roles for the security of networks and information systems have been identified and appropriately capable and knowledgeable staff fill those roles.									A1.b B6.b	
6.5 MOBILE / REMOTE WORKING POLICY: The organisation has in place policies and security measures to manage the risks introduced by using mobile devices and remote working. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

BASELINE	Not specified										
TARGET	1. A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. **In addition for PSN:** 1. Services presented outside of the protected enterprise (online services for staff, mobile working etc.), should be delivered from an appropriate architecture, with access to any core information or services constrained. 2. The architecture will include services to identify malware at the gateway. Where encryption prevents this, the organisation shall implement an equivalent level of protection at the end point. 3. If you are using cloud services: You may consider procurement of services which respond to different business needs and therefore have different security attributes. It is important that any interfaces between services are within scope. 4. If cloud services are accessed from the organisation's PSN-connected infrastructure, security assessments of these services should be conducted against the NCSC Cloud Security Principles. 5. Unmanaged devices: must not have access to the PSN. Where a corporate service contains information that has been sent over the PSN, you should have the data owner's permission before		3			10.1					

	allowing unmanaged devices to access that data. Additionally, you must ensure that an unmanaged device: d) Is not able to use the corporate service to access the PSN in an unmediated fashion e) Accesses the corporate service through an appropriately secured connection f) For example, at the network layer via a VPN, or at the application layer via a protocol that implements TLS Is authenticated prior to the information being accessed with a mechanism that does not solely rely on a username and password.										
ADVANCED	1. A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. 2. A policy and supporting security measures shall be implemented to protect information and data accessed, processed or stored at remote sites. 3. Mobile devices that hold data are catalogued, controlled and configured according to best practice for the platform, with appropriate technical and procedural policies in place. 4. A remote-wipe capability is in place for all mobile devices. 5. Data held on mobile devices has been minimised and some data may be automatically deleted off mobile devices after a certain period.								A6.2.1 A6.2.2 A14.1.2	B3.d	

7. SERVICES RESILIENCE	Network and information systems are designed to be resilient to cyber security incidents.										
7.1 SERVICES RESILIENCE: Systems are appropriately segregated and resource limitations are mitigated. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified										
TARGET	1. Key operational services have been identified with resource, technology and service dependencies defined (e.g. power, bandwidth, cooling, data, people).							3a 3b 3c			10
ADVANCED	1. Key operational systems are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration). 2. Geographical constraints or weaknesses have been identified and mitigated. 3. Systems that key services depend upon have redundancy and are replicated to an alternative location. 4. There are alternative physical paths and service providers for network connectivity with known separacy and diversity of bearers. 5. Dependencies, resource and geographical limitation assessments are regularly reviewed with update mitigations when required.								A17.2.1	B5.b	

8. ACCESS CONTROL	**Access to information, services and systems is controlled managed and monitored through policies and procedures.**										
8.1 ACCOUNT MANAGEMENT: User accounts are effectively managed throughout their lifecycle to provide minimum access to sensitive information or key operational services. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. All user account creation is subject to a provisioning and approval process. 2. Each user authenticates using a unique username and strong password before being granted access to applications, computers and network devices. 3. All default passwords are removed and changed. 4. There is a robust password policy which avoids users having weak passwords, such as those trivially guessable. 5. Password or account sharing between users is not permitted. 6. User accounts and special access privileges are removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g. 3 months). 7. Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.	2 3			4						
TARGET	No additional requirements		2	7		4.1		4b			

	For PSN 1. Password or account sharing between users is not permitted. 2. High-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts. 3. Passwords are combined with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication. 4. Passwords are never stored as plain text, but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a salt before hashing passwords.										
ADVANCED	No additional requirements.								A9.1.2 A9.2 A9.4.1 A9.4.3 A12.6.2	B2.a B2.c	
8.2 IDENTITY AUTHENTICATION: Procedures are in place to verify, authenticate and authorise access to the organisational networks and information systems. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Only individually authenticated and authorised users can connect to or access your networks or information systems.	1 2 3			4						

	2. Each user authenticates using a unique username and strong password before being granted access to applications, computers and network devices.										
TARGET	1. Users that can access personal data are appropriately authenticated. 2. Users who have privileged access are strongly authenticated by two-factor or device authentication measures. 3. Multi-factor authentication shall be used for access to enterprise level social media accounts. **In addition for PCI:** 4. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. For example, use technologies such as remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.		2	2 8		4.2	B2	5b 7b 7c			
ADVANCED	1. Additional authentication mechanisms, such as two-factor or hardware-backed certificates are employed for all systems that operate or support key services. 2. There is an auditable, robust procedure in place to verify each user and issue minimum required access rights.								A9.4.1 A9.4.3	B2.a B2.c B2.d	

	3. Attempts by unauthorised users to connect to systems are alerted, promptly assessed and investigated.										
8.3 PRIVILEGE MANAGEMENT: The allocation and use of privileged access rights to networks and information systems is restricted and controlled. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Special access privileges are restricted to a limited number of authorised individuals. 2. Details about special access privileges (e.g. the individual and purpose) are documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly). 3. Special access privileges are controlled, periodically reviewed and removed or disabled when no longer required.	3			4						
TARGET	1. Users who have privileged access accounts are strongly authenticated by two-factor or hardware authentication measures. 2. Access to sensitive information and services is only provided to authorised, known and individually referenced users or systems. 3. Access to logging data is limited to those with business need and no others. Legitimate reasons for accessing logging data are given in use policies and users are trained on this.		2 5	7		4.1 4.3	B2	4a 5a 5b			
ADVANCED	1. Systems and devices supporting the delivery services are only administered or maintained by authorised privileged users from dedicated devices that are								A9.1.2 A9.2.3 A9.4.4 A9.4.5	B2.a B2.c B4.c C1.b	

	technically segregated and secured to the same level as the networks and systems being maintained. 2. Privileged access (e.g. to systems controlling the essential service or system administration) is carried out with separate accounts that are closely monitored 3. All privileged access to your networks and information systems is routinely validated and subject to real-time security monitoring, with all privileged user sessions recorded and stored for offline analysis and investigation 4. Temporary, time-bound rights for privileged access and external third-party support access are employed where appropriate. 5. The use of utility programs that might be capable of overriding systems and applications shall be restricted. 6. Access to program source code shall be restricted.										
8.4 ADMINISTRATOR ACCOUNT MANAGEMENT: System administrator accounts are controlled and monitored with the activity logs protected and regularly reviewed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Administrative accounts should only be used to perform legitimate administrative activities, and	3			4						

	should not be granted access to email or the internet. 2. Administrative accounts should be configured to require a password change on a regular basis (e.g. at least every 60 days).										
TARGET	1. Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email. 2. Administrators do not conduct 'normal' day-to-day business from their high privilege account and use normal accounts for standard business use		5	7		4.4 4.6	B2	5a			
ADVANCED	1. The list of system administrators is regularly reviewed, e.g. every 6 months.								A9.1.2 A9.2.3 A9.4.4 A9.4.5	B2.a B4.c	
9. MEDIA MANAGEMENT	**Fixed and portable storage media and devices are managed and data / information is appropriately protected.**								A8.1		
9.1 STORAGE MEDIA: Policies and procedures are in place to protect stored data and prevent unauthorised disclosure, modification, removal or destruction of information stored on media. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

BASELINE	Not specified.										
TARGET	1. The organisation can identify and account for all end user devices and removable media. 2. Tracking and recording of all assets that process personal data, including end user devices and removable media is in place. **In addition for PCI:** 3. Media back-ups are stored in a secure location, preferably off site. 4. All media is physically secure. 5. There is strict control over the internal or external distribution of any kind of media. 6. Management approves any and all media moved from a secured area, especially when media is distributed to individuals. 7. There is strict control over the storage and accessibility of media. 8. All media is destroyed when it is no longer needed for business or legal reasons.			9		9.2 9.3 9.4 9.5	B4	6b.1			
ADVANCED	1. All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal. 2. Cloud service providers appropriately sanitise data storage areas before reallocating to another user.								A8.1.1 A8.1.2 A8.1.3 A8.1.4 A8.3.2	B3.d B3.e	
9.2 MOBILE MEDIA / DEVICES: The organisation can identify and account for all end user devices and removable media and monitors the data protection measures that are in place on mobile devices. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										

TARGET	1. Where the use of removable media is required to support the business need, it is limited to the minimum media types and users needed. 2. Removable media is automatically scanned for malware when it is introduced to any system. 3. Any media brought into the organisation is scanned for malicious content by a standalone machine before any data transfer takes place. 4. All removable media is formally issued to individual users who are accountable for its use and safe keeping. 5. Users do not use unofficial media, such as USB sticks given away at conferences. 6. Sensitive information is encrypted at rest on media. 7. Where removable media is to be reused or destroyed then it will be done securely with appropriate steps taken to ensure that previously stored information is not accessible. 8. All data is sanitised from all devices, equipment or removable media before disposal. 9. All users are made aware of their personal responsibilities for following the removable media security policy. 10. A secure baseline build and configuration is applied to all of mobile devices.					2.7 9.2 9.5 9.6	B3	6b.1 6b.4			
ADVANCED	1. Mobile devices are catalogued, tracked and configured according to best practice for the platform, with appropriate technical and procedural policies in place.								A6.2 A8.1.1 A8.1.2 A8.3.1 A8.3.3	B3.a B3.d B3.e	

	2. The data held on mobile devices is minimised. 3. Some data may be automatically deleted off mobile devices after a certain period. 4. Procedures are implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.										
9.3 CRYPTOGRAPHY: There is proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information at rest, in transit and on mobile devices or removable media. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified										
TARGET	1. Sensitive information should be encrypted at rest on devices and media and when transmitted electronically, especially over an untrusted carrier. **In addition for PCI:** 1. Any keys used for encryption of cardholder data are protected from disclosure and misuse. 2. All appropriate key management processes and procedures for cryptographic keys used for encryption of cardholder data are documented and implemented. 3. Strong cryptography and security protocols such as SSL/TLS, SSH or IPSec are used to safeguard sensitive cardholder data during transmission over open, public networks. 4. Wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to			3 4		9.5	B4	6b.4			

	implement strong encryption for authentication and transmission. 5. The use of WEP as a security control is prohibited.										
ADVANCED	1. There is a policy on the adoption of cryptography including the use and protection of cryptographic keys and their lifetime management.								A10.1 A18.1.5	B3.b B3.c	
9.4 REMOTE WIPE CAPABILITY: The organisation has the ability to remotely wipe and/or revoke access from an end user device. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. The organisation has the ability to remotely wipe and/or revoke access from all mobile devices.							6b.5			
ADVANCED	No additional requirement.									B3.d	
10. ENVIRONMENTAL SECURITY	**Appropriate procedures are in place to reduce the risks from internal and external environmental threats and hazards.**										
10.1 EQUIPMENT LOCATION: Equipment shall be sited and protected to reduce environmental impacts on information systems and service delivery. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	Not specified.										

ADVANCED	1. Equipment on premise and with third parties is sited and protected to reduce the risks from physical and environmental threats and hazards. 2. Network and connectivity cabling is resilient, protected from interception, interference or damage with redundancy in place.								A11.1.4 A11.2.1		
10.2 POWER RESILIENCE: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	Not specified.										
ADVANCED	1. Dependencies on supporting infrastructure (e.g. power, cooling) are identified and recorded. 2. Equipment is protected from power failures and other disruptions caused by failures in supporting utilities such as telecommunications with redundancy in place.								A11.2.2	A3.a	
11. PHYSICAL / BUILDING SECURITY	**To prevent unauthorised physical access, damage and interference with the organisation's information systems and services.**										
11.1 ACCESS CONTROL: Building and secure areas access shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed admittance. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										

TARGET	1. Appropriately secure accommodation and appropriate policies and practices governing its use is in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise. **In addition for PCI:** 1. Appropriate facility entry controls are used to limit and monitor physical access to systems. 2. Procedures are in place to easily distinguish between onsite personnel and visitors. 3. All visitors are authorized before entering secure areas; given a physical badge or token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical badge or token before leaving the facility or at the date of expiration. 4. A visitor log is used to maintain a physical audit trail of visitor information and activity, including visitor name and company and the onsite personnel authorising physical access. 5. The visitor log is retained for at least three months unless otherwise restricted by law.		1c	9							
ADVANCED	1. Delivery and loading areas and other access points are controlled.								A11.1.1 A11.1.2		
11.2 INTERNAL SECURITY: Internal security perimeters shall be defined with policies and active alerting systems used to protect areas that contain sensitive data, critical information and essential information systems. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

BASELINE	Not specified.										
TARGET	1. Secure accommodation areas are defined and segregated to protect areas that contain either sensitive data or information processing facilities. 2. Appropriate policies and practices governing the use of the secure accommodation and access are in place.		1c	9							
ADVANCED	1. Secure areas are protected by entry controls to ensure that only authorised personnel are allowed access. 2. Physical security for offices, rooms and facilities shall be defined and implemented; to include for example intruder detection, fire and flood alarms and alerting systems.								A11.1.1 A11.1.3 A11.1.6		
12. SYSTEM MANAGEMENT	**Information systems are protected from cyber-attack throughout their lifecycle.**										
12.1 SECURE CONFIGURATION: The network and information systems that support the delivery of essential services are securely configured. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled. 2. Any default password for a user account should be changed to an alternative, strong password. 3. Unnecessary software (including application, system utilities and network services) should be removed or disabled. 4. The auto-run feature should be disabled (to prevent software programs running automatically when	2			4						

	removable storage media is connected to a computer or when network folders are accessed). 5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.										
TARGET	1. A secure baseline build is implemented for all systems, platforms and components, including hardware and software to reduce the level of inherent vulnerability. 2. Any functionality or application, services or ports not required to support a user or business need is removed or disabled. 3. The secure build profile is managed by a configuration control process and any deviation from the standard build is documented and approved. **In addition for PSN:** 1. Configuration control of applications installed and technology is in place. All changes and new applications are recorded and managed, including a formal approval and documentation process. 2. Devices, systems and services have the capability to detect, isolate and respond to malicious software. 3. The underlying infrastructure and platform are secure. This includes verification that the hosting environment is maintained securely.		1b			2.4 10.3	B4	6a.2 6d.2			

ADVANCED	1. Network and system configurations changes are managed, secure and documented. 2. Network and information systems are regularly reviewed and validated to ensure that they have the expected, secured settings and configuration. 3. There are regular reviews and updates to technical knowledge about networks and information systems, such as documentation and network diagrams, and these are securely stored. 4. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.								A12.4.4 A12.5.1	B4.b	
12.2 SECURE DESIGN / DEVELOPMENT: Information security is designed and implemented within the development lifecycle of information systems and networks. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	Not specified. **In addition for PCI:** 1. Software applications (internal and external, and including web-based administrative access) are developed in accordance with PCI DSS and based on industry best practices. 2. Information security is embedded throughout the software development life cycle. 3. Change control processes and procedures are followed for all changes to system components.			6							

	4. Applications are developed based on secure coding guidelines and custom application code is reviewed to identify coding vulnerabilities. 5. All public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.										
ADVANCED	1. A secure development policy with guidance is in place that defines rules for the development of software and systems and is applied. 2. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. 3. The organisation shall supervise and monitor the activity of outsourced system development. 4. Change control procedures are in place to manage the development lifecycle. 5. Appropriate expertise is employed to design and review network and information systems. 6. Network information systems and sensitive data are segregated into appropriate security zones (e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone).The networks and information systems are designed to have simple data flows between								A12.1.3 A13.1.3 A14.2.1 A14.2.3 A14.2.5 A14.2.6 A14.2.7 A14.2.8	B4.a	

	components to support effective security monitoring. 7. The networks and information systems are designed to be easy to recover.										
12.3 CHANGE CONTROL PROCEDURES: Changes to systems and software configurations are controlled by formal change control procedures. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	
BASELINE	Not specified.										
TARGET	1. Policies that set out configuration control and change management processes for all systems are in place. 2. The ability of users to change configuration is restricted. Users with 'normal' privileges are prevented from installing or disabling any software or services running on the system.					2.6 2.9	B4				
ADVANCED	1. Modifications to software are restricted and all changes are subject to change control procedures. 2. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation. 3. Change management is in place to control changes to business processes, information processing facilities and systems.								A12.1.2 A14.2.2 A14.2.4	B4.b	
12.4 SYSTEM TESTING: Testing of security functionality shall be carried out during development of new systems, upgrades and new versions or configurations. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										

TARGET	1. Regular testing is undertaken to evaluate the effectiveness of security measures, including virus and malware scanning, vulnerability scanning and penetration testing. 2. The results of any testing and remediating action plans are recorded. **In addition for PSN:** 1. Regular IT Health Checks (ITHCs) are implemented to demonstrate that any security mechanisms put in place are ongoing and effective and identify any current vulnerability. ITHCs should normally be conducted annually, or more frequently where appropriate. 2. Issues identified in the ITHC (including systemic issues) are addressed, with critical and high risks areas resolved immediately or a viable plan for resolution is agreed. Medium and Low risks may be accepted or subject to remedial action plans. **In addition for PCI:** 1. The presence of wireless access points is tested to detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. 2. External and internal penetration testing is performed at least annually and after any significant infrastructure or application upgrade or		7	11			B4	6a.3 6d.4			

	modification, including network- and application-layer penetration tests. 3. Network intrusion detection systems and/or intrusion prevention systems are used to (a) monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and (b) alert personnel to suspected compromises. 4. IDS/IPS engines, baselines, and signatures are kept up to date. 5. File integrity monitoring tools are deployed to alert personnel to unauthorized modification of critical system files, configuration files or content files. Critical file comparisons are performed at least weekly.										
ADVANCED	1. Regular testing by third-parties is undertaken to identify vulnerabilities in the networks and information systems. 2. Penetration testing is undertaken following changes to operating systems, business applications and software development and deployment. 3. Test data shall be securely marked, protected and controlled. 4. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.								A2.1.3 A14.2.3 A14.2.8 A14.2.9 A14.3.1	B4.d	
13. OPERATIONAL SECURITY	**Appropriate technical and organisational measures are in place to**										

	protect systems and digital services from cyber attack										
13.1 MALWARE POLICIES & PROTECTION: Detection, prevention and recovery controls to protect against malware shall be implemented. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Malware protection software is: f. installed and actively running on all computers that are connected to or capable of connecting to the internet and generates audit logs g. kept up-to-date (e.g. at least daily, either by configuring it to update automatically or through the use of centrally managed deployment). h. configured to i. scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) ii. scan web pages when being accessed (via a web browser). i. configured to perform regular scans of all files (e.g. daily). j. preventing connections to malicious websites on the internet (e.g. by using website blacklisting).	4			4						12

TARGET	1. Anti-malware policies and standards are developed and implemented across the organisational infrastructure. 2. End user device protection is in place through anti-virus software and application whitelisting. 3. Stand-alone workstations are provided as required equipped with appropriate anti-virus software capable of scanning the content on any type of media.		1b	5		5.1 7.1 7.4 7.5.1	B4 C1	1b 6c.3			12
ADVANCED	No additional requirements.								A12.2.1	B4.c	
13.2 EMAIL SECURITY: Information involved in electronic messaging shall be appropriately protected. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The NCSC Active Cyber Defence (ACD) programme is implemented where appropriate.				5						
TARGET	1. Transport Layer Security Version 1.2 (TLS v1.2) is used for sending and receiving email securely. 2. Domain-based Message Authentication Reporting and Conformance (DMARC) is in place along with Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records. 3. Spam and malware filtering is present and DMARC is enforced on inbound email.							6c.1 6c.2			
ADVANCED	No additional requirement.								A13.2.3		
13.3 APPLICATION SECURITY: Applications are tested for susceptibility to security vulnerabilities on development and following system changes. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The NCSC's Web Check service has been adopted				5						

TARGET	1. Web applications are regularly tested for the presence of known security vulnerabilities (such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities) and common configuration errors.							6d.1			
ADVANCED	No additional requirements.										
13.4 VULNERABILITY MANAGEMENT & SCANNING: Network and information systems are managed to prevent exploitation of technical vulnerabilities. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The NCSC Active Cyber Defence (ACD) programme is implemented where appropriate.	4			5						
TARGET	1. There is a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities. 2. Regular vulnerability scans are conducted via automated vulnerability scanning tools against all networked devices and any identified vulnerabilities are remedied or manage within an agreed time frame. 3. Regular discovery scans to detect unknown devices are undertaken and any anomalous findings are investigated. 4. Antivirus and malicious code checking solutions are deployed to scan inbound and outbound objects at the network perimeter. Any suspicious or infected malicious objects are quarantined for further analysis. **In addition for PCI:**		1a	5 6 11		2.5 2.7 3.1.2 7.2 7.5	B4 C1				12

	1. Internal and external network vulnerability scans are run at least quarterly and after any significant change in the network. 2. Quarterly external scans are performed by an Approved Scanning Vendor (ASV). 3. Scans conducted after network changes are performed by internal staff. 4. File integrity monitoring tools are deployed to alert personnel to unauthorised modification of critical system files, configuration files or content files. The software is configured to perform critical file comparisons at least weekly.										
ADVANCED	1. Information about vulnerabilities for all software packages, network equipment and operating systems is obtained in a timely fashion 2. Vulnerabilities are prioritised and subject to a risk assessment to determine the organisation's exposure and vulnerability. 3. Selected threat intelligence feeds are in place to enable risk-based and threat-informed decisions based on business needs.								A12.6.1	B4.b	
13.5 DATA EXFILTRATION MONITORING: Network traffic is monitored to identify unusual activity. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Network traffic, services and content is limited to that required to support business need (for example, by setting effective firewall rule sets).					7.2					

	2. Inbound and outbound traffic traversing network boundaries is monitored to identify unusual large data transfers which automatically generate security alerts that are promptly managed by appropriately trained staff.										
ADVANCED	No additional requirements.									C1.a	
13.6 SOFTWARE SUPPORTED & UPDATED: Operating systems and software packages are patched regularly and in vendor support. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Software running on computers and network devices is kept up-to-date and has the latest security patches installed. Specifically: e) Software running on computers and network devices that are connected to or capable of connecting to the internet is licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available. f) Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet are installed in a timely manner (e.g. within 30 days of release or automatically when they become available from vendors). g) Out-of-date software (i.e. software that is no longer supported) is removed from computer and network devices that are connected to or capable of connecting to the internet.	4 5			4 5						12

	h) All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet is installed in a timely manner (e.g. within 14 days of release or automatically when available from vendors).										
TARGET	1. There is an organisation policy that specifies specific patch application periods and a process for auditing compliance. Critical and high-risk vulnerabilities are patched within 14 days, important vulnerabilities patched within 30 days and all others patched within 60 days. Where vulnerability is being actively exploited then mitigating actions are taken immediately. 2. Where a patch is not available or cannot be deployed within the timescales above, there are alternative mitigating actions in place, such as disabling or reducing access to the vulnerable service.			5		2.1	B4	6b.3			
ADVANCED	1. You maximise the use of supported software, firmware and hardware in your networks and information systems.									B4.d	
13.7 WEBSITE SCREENING: Malware protection software should prevent connections to malicious websites. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Malware protection software is in place to prevent connections to known malicious websites on the internet (e.g. by using website blacklisting).	4			4						
TARGET	No additional requirements.					7.3					

ADVANCED	No additional requirements.										
13.8 BROWSER MANAGEMENT: Web browsers should be configured to minimise security vulnerabilities and risk. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Deploy a content filtering capability on all external gateways to try to prevent attackers delivering malicious code to common desktop applications such as the web browser. 2. Browsers are kept current and configured to mitigate against code exploits. 3. Unnecessary browser plugins or scripting languages are disabled.					7.6.4					
ADVANCED	No additional requirements.										
13.9 MONITOR / AUDIT USER ACTIVITY: User access and activity are monitored to identify unauthorised access attempts, policy violations and unusual behaviour. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. All user access and activity is monitored, particularly access to sensitive information and the use of privileged account actions. 2. The monitoring capability has the ability to identify unauthorised or accidental misuse of systems or data. It is able to tie specific users to suspicious activity. 3. Activities that are outside of normal, expected bounds; policy violation; suspicious or undesirable behaviour (such as access to large amounts of			10		4.5 8.4	B2 C1				

	sensitive information outside of standard working hours) are recorded and investigated. **In addition for PCI:** 1. An automated audit trails system is in place for all system components for reconstructing these events: h) all individual user accesses to cardholder data; i) all actions taken by any individual with root or administrative privileges; j) access to all audit trails; k) invalid logical access attempts; l) use of identification and authentication mechanisms; m) initialisation of the audit logs; n) creation and deletion of system-level objects. 2. Audit trail entries are recorded for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource. 3. All critical system clocks and times are synchronised with controls for acquiring, distributing, and storing time. 4. Audit trails are secured so they cannot be altered. 5. Logs for all system components related to security functions are reviewed at least daily.										

	6. Audit trail history is retained for at least one year; at least three months of history is immediately available for analysis.										
ADVANCED	1. All user's access is logged and monitored for offline analysis and investigation as required. 2. Logging facilities and log information shall be protected against tampering and unauthorised access. 3. All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user. 4. Audit logs recording user activities, exceptions, faults and information security events are created, maintained securely and regularly reviewed. 5. Attempts by unauthorised users to connect to systems are alerted, promptly assessed and investigated where relevant.								A12.4.1 A12.4.2 A12.4.3	B2.c B2.d C1.a	
13.10 DISABLED AUTO-RUN: The auto-run feature should be disabled to prevent software programs automatically running. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The auto-run feature is disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).	2									
TARGET	No additional requirements.					7.6.5					
ADVANCED	No additional requirements.										

14. NETWORK SECURITY	To ensure the protection of information systems and information held in networks.								A13.1		
14.1 PATCH MANAGEMENT: Operating systems and software packages on networks and devices are kept up-to-date with the latest security patches installed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet are installed in a timely manner (e.g. within 14 days of release or automatically when available from vendors).	5			4						12
TARGET	1. There is a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities. The policy specifies specific patch application periods and a process for auditing compliance. 2. Critical vulnerabilities are patched within 14 days, important vulnerabilities patched within 30 days and all others patched within 60 days. 3. Where a vulnerability is being actively exploited then mitigating action (e.g. patch applied) is immediately taken. 4. Where a patch is not deployed (or available) within the timescales above there is alternative mitigating actions employed, such as disabling or reducing access to the vulnerable service.		1a	6		2.2	B4	6a.2 6b.3			
ADVANCED	No additional requirements.								B4.d		

14.2 DEVICE MANAGEMENT: Devices that are used to access organisational networks, information systems and data are known and recorded with integrated security management policies and systems. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Unnecessary peripheral devices are disabled. 2. All end-user devices are recorded, managed and tracked. 3. Technical policies are applied and controls exerted on devices over software and applications' 4. Devices used to access sensitive information and data or key operational services are authenticated and authorised. **In addition for PSN:** 5. Unmanaged devices do not have access to the PSN. Where a corporate service contains information that has been sent over the PSN, the data owner's permission is sought before allowing unmanaged devices to access that data. Additionally, unmanaged devices: d) are not able to use the corporate service to access the PSN in an unmediated fashion e) access the corporate service through an appropriately secured connection (e.g. via a VPN, or via a protocol that implements TLS). f) are authenticated prior to the information being accessed with a mechanism that does not solely rely on a username and password.		3			2.7 7.5 10.3	B4	5b 6b.2 6b.4			

ADVANCED	1. Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email. 2. Device identity management which is cryptographically backed is performed and only known devices are able to access systems. 3. Regular discovery scans are performed to detect unknown devices and any findings are investigated. 4. Privileged access is only granted on owned and managed devices that are technically segregated and secured to the same level as the networks and systems being maintained.									B2.b B2.c B4.c	
14.3 CONTENT SCREENING: Content-based attacks are mitigated with inbound and outbound screening. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Content filtering capability is present on all external gateways to prevent malicious code being deployed to common desktop applications such as the web browser. The antivirus and malware solutions used at the perimeter are different to those used to protect internal networks and systems in order to provide some additional defence in depth. 2. Dedicated, stand-alone media scanning machines are provided and equipped with appropriate anti-virus products capable of scanning the content					3.1.2 7.2 7.4 7.5.3					

	contained on any type of media and inspect recursive content within files.										
ADVANCED	No additional requirements.									B4.a	
14.4 INTERNAL SEGREGATION: Networks and information systems are segregated into appropriate security zones. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Information services, sensitive data, users and information systems are segregated into appropriate security zones on networks. 2. Key operational systems are segregated in a highly trusted, more secure zone isolated with appropriate network security controls.					3.2.1					
ADVANCED	1. Key operational systems are segregated from other business and external systems by appropriate technical and physical means. 2. Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment. 3. Internet services are not accessible from operational systems. 4. Logging data is segregated from the rest of the network, and is not affected by disruption or corruption of network data.								A12.1.3 A13.1.3	B4.a B5.b	

14.5 Wireless Security: Wireless access points should be securely configured and segregated as appropriate. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Wireless access points are securely configured.	2									
TARGET	1. All wireless access points only allow known devices to connect to corporate Wi-Fi services. 2. Security scanning tools are in place to detect and locate unauthorised or spoof wireless access points. **In addition for PCI:** 1. Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption					3.2.3					
ADVANCED	No additional requirements.										
14.6 Boundary / Firewall Management: Manage access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. One or more firewalls (or equivalent network device) are installed on the boundary of the organisation's internal network(s). 2. The default administrative password for any firewall (or equivalent network device) is changed to an alternative, strong password. 3. Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall) is subject to approval by an authorised	1			4						

	individual and documented (including an explanation of business need). 4. Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), are disabled (blocked) at the boundary firewall by default. 5. Firewall rules that are no longer required (e.g. because a service is no longer required) are removed or disabled in a timely manner. 6. The administrative interface used to manage boundary firewall configuration is not accessible from the internet.(the interface is protected by additional security arrangements, which include using a strong password, encrypting the connection (e.g. using SSL), restricting access to a limited number of authorised individuals and only enabling the administrative interface for the period it is required.)										
TARGET	1. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. **In addition for PCI:** 2. Firewall and router configuration standards are established that formalise testing whenever 3. configurations change; that identify *all* connections to cardholder data (including wireless); that		3	1 6		3.1.1 7.6.3					

	4. use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months. 5. Firewall and router configurations that restrict all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment. 6. Direct public access between the Internet and any system component in the cardholder data environment is prohibited. 7. Personal firewall software is installed on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network. 8. All public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.										
ADVANCED	1. Traffic crossing the network boundary (including IP address connections as a minimum) is monitored.									B4.a C1.a	
14.7 ADMINISTRATOR CONTROL: System administrators are strongly authenticated and authorisation is reviewed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Administrator access to any network component is properly authenticated and authorised. 2. Default administrative passwords for network equipment are changed.					3.2.4		6a.5			

	3. Changes to the authoritative DNS entries can only be made by strongly authenticated and authorised administrators.										
ADVANCED	1. The list of system administrators is regularly reviewed, e.g. every 6 months.								A12.4.3	B2.c	
14.8 Error Message Management: Error messages do not contain sensitive information that could compromise systems. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. The exception handling processes is configured to ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.					3.2.5					
ADVANCED	No additional requirements.										
14.9 Penetration Testing: Network and application penetration tests are performed on a regular basis and following systems change. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Regular penetration testing for the presence of known vulnerabilities or common configuration errors is undertaken with third-parties to ensure that security controls have been well implemented and are effective. **In addition for PCI:** 1. Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.		7	11		3.2.6		6a.3			

	In addition for PSN: 1. Regular IT Health Checks (ITHCs) are implemented to seek evidence that any security mechanisms put in place are ongoing and effective and identify any current vulnerability. ITHCs should normally be conducted annually, but may be employed more frequently where appropriate. 2. Issues identified in the ITHC (including systemic issues) are addressed. Critical and High risks are either be resolved immediately or by a viable plan for resolution. Medium and Low risks may be accepted or subject to remedial action plans.										
ADVANCED	No additional requirements.								A14.2.9	B4.d	
14.10 IP & DNS MANAGEMENT: Organisational IP ranges are known, recorded and managed; DNS changes and queries are effectively managed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The NCSC's ACD P-DNS service is implemented where appropriate and available.										
TARGET	1. The UK Public Sector DNS Service is used to resolve internet DNS queries. 2. Organisational IP ranges are known and recorded							6a.4 6a.6			
ADVANCED	1. IP address traffic crossing the network boundary are monitored.									C1.a	
15. INCIDENT DETECTION	**Organisations shall have in place monitoring systems and procedures to detect cyber-attacks**										

15.1 DETECTION CAPABILITY: Attempts to access or compromise systems are alerted, promptly assessed and investigated. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Attackers attempting to use common cyber-attack techniques should not be able to gain access to data or any control of technology services without being detected. **In addition for PSN:** 1. Event data is collected and retained to detect actual or potential security incidents. 2. The organisation has a policy that describes the use cases to be detected, which define event data collection. 3. The policy includes both detection of technical attacks as well as important abuses of business processes.		1d					8d			
ADVANCED	1. Detection, prevention and recovery controls to protect against malware are in place. 2. Policy violations are detected against an agreed list of suspicious or undesirable behaviour. 3. There is the capability to investigate AV alerts. 4. Threat intelligence services are employed and used to inform anomalous activity profiles. 5. There is a sufficient understanding of normal system activity (e.g. which system components should and should not be communicating with each other) to ensure that searching for system								A12.2.1	B2.d B4.c C1.a C1.c C2.a C2.b	

	abnormalities is an effective way of detecting malicious activity. 6. Descriptions of some system abnormalities that might signify malicious activity are maintained and updated, informed by past attacks and threat intelligence that takes into account the nature of attacks likely to impact on the networks and information systems. 7. Routine search for system abnormalities are undertaken and alerts generated.										
15.2 SECURITY MONITORING: Risk-based organisational monitoring policy and procedures are in place for the timely identification of security events. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. The network is monitored with intrusion detection and prevention solutions that are configured by qualified staff. These solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour. coverage includes internal and host-based monitoring. 2. Inbound and outbound traffic traversing network boundaries is monitored to identify unusual activity or trends that could indicate attacks. Unusual network traffic (such as connections from unexpected IP ranges overseas) or large data transfers automatically generate security alerts.		1d			3.2.5 8.1 8.2 8.3 8.4 8.5 8.6 8.7	C1	8b 8c 8e			

	3. Policies and processes are in place to promptly manage and respond to incidents detected by monitoring solutions. 4. Alerts generated by the system monitoring strategy are based on business need and an assessment of risk. This includes both technical and transactional monitoring as appropriate. 5. The monitoring capability has the ability to identify the unauthorised or accidental misuse of systems processing personal data and user access to that data, including anomalous user activity. It can tie specific users to suspicious activity. 6. A centralised capability has been deployed that can collect and analyse information and alerts from across the organisation. This is automated due to the volume of data involved, enabling analysts to concentrate on anomalies or high priority alerts. 7. The monitoring and analysis of audit logs is supported by a centralised and synchronised timing source that is used across the entire organisation to support incident response and investigation. 8. Processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability. **In addition for PSN:** 1. If you are using cloud services: Cloud Security Principle 5.3 *Protective Monitoring* should be factored into your overall monitoring strategy. Note that a cloud service will only provide monitoring										

	with respect to the service provisioned. If you consume Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), you are responsible for monitoring of capability deployed onto the infrastructure. If you are consuming Software as a Service (SaaS), you should consider how you will be able to monitor for any potential abuse of business process or privilege.										
ADVANCED	1. As well as the network boundary, monitoring coverage includes internal and host-based monitoring. 2. Process for bringing new systems on line includes considerations for access to monitoring data sources. 3. Monitoring staff: e) are responsible for investigating and reporting monitoring alerts. f) have roles and skills that covers all parts of the monitoring/investigation workflow. g) have workflows that address all governance reporting requirements, internal and external. h) are empowered to look beyond fixed workflows to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.								A12.4	C1.a C1.e	
16. INCIDENT MANAGEMENT	**Well-defined incident management processes are in place, documented and regularly tested.**										

16.1 INCIDENT RESPONSE PROTOCOL: A risk-based and up-to-date incident response plan is in place. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Cyber incident response policies and process are in place and these integrate with central cyber incident reporting , notification and coordination protocols.				7						10
TARGET	1. There is an incident response capability and management plan in place, documented, with clear pre-defined processes, actions, roles and responsibilities and clear terms of reference for decision-making and incident management. 2. Specialist training is provided as required to the incident response team. 3. In the event of an incident the response team is provided with audit logs holding user activities, exceptions and information security events to assist in investigations. 4. The contact details of key personnel are readily available to use in the event of an incident. 5. The supporting policy, processes and plans are risk based and cover any legal or regulatory reporting requirements. 6. All incidents are recorded regardless of the need to report them. 7. All plans supporting security incident management (including business continuity and disaster recovery plans) are regularly tested. 8. The outcome of the tests and knowledge from incident management events are used to inform the		1d 1e	12		6.1 6.3 6.5 8.8 10.6	C1	8a 9a			10

	future development of the incident management plans. **In addition for PSN:** 1. For incidents that impact on the PSN, these are reported to the PSN team and other entities as required.										
ADVANCED	1. The incident response plan is communicated and understood by the wider organisational business and integrated with supply chain response plans. 2. Thresholds for incident definitions, classifications and assessments are in place. 3. Procedures for the identification, collection, acquisition and preservation of evidence have been defined and implemented								A12.2.1 A16.1.1 A16.1.4 A16.1.5	D1.a	
16.2 INCIDENT REPORTING PROCEDURE: Security events are reported through defined procedures known to staff. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. Cyber incident response policies and process are in place and these integrate with central cyber incident reporting , notification and coordination protocols.				7						
TARGET	1. The organisation promotes an incident reporting culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, with positive recognition and without fear of recrimination. 2. Users (employees and contractors) are security aware, know their responsibilities, and understand how to report any observed or suspected security		1d 1e			5.6 6.6 6.9 6.10	C1 D2	9a 9b 9c			

	weaknesses in systems or services and how to respond to incidents. 3. Users are encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination. 4. There are communication plans in place in the event of an incident and all internal and external reporting requirements are identified in the incident management plan. This includes notifying the relevant supervisory body, senior accountable individuals, the National Cyber Security Centre (NCSC), the Information Commissioner's Office (ICO) and law enforcement as applicable.										
ADVANCED	No additional requirement.								A12.4 A16.1.2 A16.1.3	B6.a D1.a	
16.3 STAFF TRAINING & TESTING: Staff are trained in incident response with assigned roles and responsibilities and the organisation carries out exercises to test response plans. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. A staff induction process is in place for new users (including contractors and third parties). 2. All employees receive regular training on the security risks to the organisation. This is tracked and refresh update training is completed at suitable intervals. 3. Cyber security information and good practice guidance is easily and widely available.					5.2 5.3	D1	1a			

	4. Senior accountable individuals receive appropriate training and guidance on cyber security and risk management. 5. Employees in security roles are encouraged to develop and formally validate their security skills through recognised certifications and specialist training. 6. The effectiveness of security training and awareness activities is monitored and tested.										
ADVANCED	No additional requirements								A7.2.2 A12.2.1	B6.a B6.b	
16.4 POST-INCIDENT REVIEW & LEARNING: The organisation reviews incidents and uses lessons learned from incidents to improve security measures. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	1. The senior team should take ownership of the lessons process to ensure that any actions required to improve the organisation's cyber resilience are undertaken.				3						
TARGET	1. Post-incident evidence is collected, preserved and analysed to identify and remedy the root cause. 2. Root cause analysis is conducted routinely as a key part of the lessons learned activities following an incident. This is comprehensive, covering organisational process issues, as well as vulnerabilities in networks, systems or software. 3. Lessons-learned reviews are conducted: actions taken during an incident are logged and reviewed to evaluate the performance of the incident management process.					5.6 5.7 6.7 6.8 8.9	D2	9d 9e 9f 10c			

	4. Post incident lessons are assessed and lessons implemented into future iterations of the incident management plan and the monitoring capability.										
ADVANCED	1. There is a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon. 2. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems. 3. Improvements identified as a result of lessons learned exercises are prioritised, with the highest priority improvements completed quickly.								A16.1.6 A16.1.7	D2.a D2.b	
17. BUSINESS CONTINUITY	**Information security continuity shall be embedded in the organisation's business continuity management systems**										
17.1 DATA RECOVERY CAPABILITY: Recovery controls are in place and tested to protect against information /data being lost or compromised. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. A data recovery capability is in place that includes a systematic approach to the backup of essential data.					6.4	D1				10
ADVANCED	1. The organisation has applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.								A12.3.1	B3.c D1.a	

17.2 BACKUP POLICIES & PROCEDURES: Backup copies of information, software and system images shall be taken and tested regularly. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. There is a backup policy and measures are in place to routinely maintain backup media. 2. The ability to recover archived data for operational use is regularly tested. 3. Physical backup media (where used) is held in a physically secure location, offsite.						D1				
ADVANCED	1. Backup copies of information, data, software and system images are taken, tested, documented and routinely reviewed. 2. There are secured backups of data to allow services to continue should the original data not be available. 3. Automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.								A12.3.1	B3.c B5.c	
17.3 DISASTER RECOVERY POLICIES & PROCEDURES: The organisation has well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Contingency mechanisms to continue to deliver services in the event of any failure, forced shutdown, or compromise of any system or service have been identified, documented and tested. 2. Restoring data and services to normal operation is a well-practised scenario.						D1	10a			10

ADVANCED	1. Disaster recovery plans and processes have been tested for practicality, effectiveness and completeness . 2. Restore times to operational service are known and documented. 3. The resources needed to carry out any required response activities are known with arrangements in place to make these resources available. 4. You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available, including with third-party suppliers as appropriate and where required. 5. Disaster response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out. 6. Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.								A12.3.1 A17.1.1 A17.1.2	B3.c B5.a B5.c D1.b	
17.4 BC/DR Testing Policies & Procedures: Scenario-based exercises and processes to test recovery response plans are planned and performed. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										

TARGET	1. Contingency mechanisms have been identified and tested to enable service continuity in the event of any failure, forced shutdown, or compromise of any system or service. 2. Restoring the service to normal operation is a well-practised scenario.						D1	10a 10b			10
ADVANCED	1. The established and implemented information security continuity controls are tested and reviewed at regular intervals in order to ensure that they are valid and effective. 2. Business continuity and disaster recovery plans are tested for practicality, effectiveness and completeness to ensure they remain valid. 3. Exercise scenarios are based on incidents experienced by the organisation, other organisations, or are composed using experience or threat intelligence. 4. Exercise scenarios are documented, regularly reviewed, and validated. 5. Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned. 6. Exercises test all parts of the response cycle relating to particular services or scenarios (e.g. restoration of normal service levels).								A12.3.1 A17.1.3	B5.a B5.c D1.c	
17.5 DATA PROTECTION IMPACT ASSESSMENTS (DPIA): DPIAs are undertaken to determine the impact of the intended processing on the protection of personal data where the processing is likely to result in a high risk to		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF

the rights and freedoms of individuals. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. [Click here to return to Framework]											
BASELINE	Not specified.										
TARGET	1. The impact of loss of availability of the service is known, understood and mitigated.							3d			
ADVANCED	1. The impact on the service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data are understood and documented. 2. The impact statements are validated regularly, e.g. annually.									B3.a	
17.6 BC CONTINGENCY PLAN: Contingency mechanisms are in place to continue to deliver services in the event of any failure or compromise of any system or service. [Click here to return to Framework]		CE	PSN	PCI	PSAP	10 Steps	GDPR-ICO	HMG SPF	ISO 27001	NIS	DF
BASELINE	Not specified.										
TARGET	1. Contingency mechanisms to continue to deliver services in the event of any failure, forced shutdown, or compromise of any system or service are identified, documented, and implemented.							10a			10
ADVANCED	1. Suitable alternative transmission paths are available where there is a risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).								A17.1.1 A17.2.1	A3.a B3.b D1.a	

	2. Information security continuity is embedded in the organisation's wider business continuity management planning. 3. Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service. 4. The resources that will be needed to carry out any required response activities, and arrangements are in place to make these resources available. 5. The types of information that will likely be needed to inform response decisions are known and documented and arrangements are in place to make this information available. 6. Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable. 7. Where necessary, arrangements are in place to augment incident response capabilities with external support (e.g. specialist providers of cyber incident response capability).										

Annex B:
Individual Standards and Guidance

Annex B: Cyber Resilience Framework: Individual Standards and Guidance

This annex provides an easily accessible reference document to standards and guidance employed in the development of the Cyber Resilience Framework and the concept self-assessment tool. The standards and guidance set out here are as follows:

- The Scottish Government's Public Sector Action Plan (PSAP)
- Cyber Essentials (CE)
- Public Services Network (PSN)
- Payment Card Industry Data Security Standard (PCI)
- The NCSC's 10 Steps to Cyber Security (10 Steps)
- NCSC – ICO guidance on GDPR Security Outcomes (GDPR-ICO)
- The UK Government Security Policy Framework Minimum Cyber Security Standard (HMG SPF)
- The NIS regulations and the NCSC NIS Cyber Assurance Framework (NIS)

The International Standard in Information Security (ISO 27001) is not reproduced in this document for copyright reasons.

Some of the guidance documents do not number paragraphs or bullet points. In these instances, to ease cross reference, paragraph numbers have been added to the documents reproduced here.

1. PSAP (Initial Baseline Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

***Sources**: Safe, secure and prosperous: a cyber resilience strategy for Scotland. Public Sector Action Plan 2017-18, 2017, 50pp.*
https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/

Safe, secure and prosperous: a cyber resilience strategy for Scotland. Public Sector Action Plan 2017-18, Implementation Toolkit, version 2, March 2018, 31pp.
https://www.gov.scot/publications/cyber-resilience-public-sector-toolkit/

The Scottish Government will ask public bodies to achieve the following requirements to the following timelines:

Key Action 2 *[Return to Framework] [Return to Mapping Matrix]*

Have in place minimum cyber risk governance arrangements, by end June 2018:

- A **named Board/Senior Management member** identified as responsible for organisational cyber resilience arrangements, with clear lines of responsibility and accountability for the cyber resilience of sensitive information and key operational services.

- **Regular Board/Senior Management-level consideration** of the cyber threat and the arrangements the organisation has in place to manage risks arising from it, with appropriate management policies and processes in place to direct the organisation's overall approach to cyber resilience.

Key Action 3 *[Return to Framework] [Return to Mapping Matrix]*

Ensure that public bodies that manage their own networks become active members of the NCSC's Cyber security Information Sharing Partnership (CiSP), in order to promote sharing of cyber threat intelligence, by end June 2018.

Key Action 4 *[Return to Framework] [Return to Mapping Matrix]*

Ensure they have in place appropriate independent assurance of critical cyber security controls by end October 2018. To support this goal, funding will be made available for public bodies to undergo Cyber Essentials "pre-assessments", by end March 2018. The adoption, **as a minimum**, of five critical network controls:

a) **Boundary firewalls and internet gateways –** information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

b) **Secure configuration –** computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.
c) **Access control –** user accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.
d) **Malware protection –** Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software.
e) **Patch management –** Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

Key Action 5 *[Return to Framework] [Return to Mapping Matrix]*

Implement as appropriate the NCSC's Active Cyber Defence Programme, which aims to make internet-based products and services safer to use, by end June 2018.

- **Protected DNS**, which takes the data GCHQ and commercial partners have about known malicious addresses, and then simply blocks users in public sector bodies from going there. In this way it automatically prevents public servants visiting infected sites whilst using work systems.

- **DMARC anti-spoofing**, which is a protocol that makes it much harder for attackers to send fake emails that look as if they come from Scottish public sector bodies (which is often done in email spoofing and spear-phishing, the most common way of introducing malware into victims' systems). What this means for the citizen is that instead of being advised 'not to open a dodgy looking email' the 'dodgy email' does not arrive. In parallel, NCSC have built the **MailCheck service**, which monitors adoption of the standard and provides data on trends. MailCheck also processes

  DMARC reports centrally, to generate data which further enhances the NCSC's knowledge of the threat picture.

- **Webcheck**, which helps public bodies fix vulnerabilities on their websites. One thing victims and attackers both do is scan for vulnerabilities in Internet facing services so that they know what to defend, or attack. Commercial services are available to do this. But for smaller public bodies the cost of these services might prove prohibitive, and they may not be able to afford to employ anyone who understands the results. The NCSC offers a free service known as Webcheck to scan the websites of public bodies and generate a report on what needs fixing, and how to fix it.

- **Phishing and malware mitigation (Netcraft)**, a service that NCSC have worked on with Netcraft, a private sector company, which public bodies will benefit from automatically without having to do anything. However, public bodies can help augment the service by notifying Netcraft if they themselves discover they are the target of a phishing campaign, or

if there are malicious emails purporting to be from them. Netcraft will then issue takedown notifications to the hosts of the email and phishing sites.

Key Action 6 ***[Return to Framework] [Return to Mapping Matrix]***

Have in place appropriate cyber resilience training and awareness raising arrangements for individuals at all levels of the organisation, by end June 2018.

a) Boards, senior executives and their support functions
b) Managers
c) Security-focused staff (including cyber security and front of house staff)
d) Specialist staff, including IT, HR, finance, audit, legal and procurement
e) Privileged users
f) All staff in both policy and delivery roles, whether permanent, temporary or contractors

Key Action 7 ***[Return to Framework] [Return to Mapping Matrix]***

Have in place appropriate cyber incident response plans as part of wider response arrangements, and ensure these align with central incident reporting and coordination mechanisms, by end June 2018.

2. Cyber Essentials (Initial Baseline Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Sources: https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure.html

Requirements for IT Infrastructure

We specify the requirements under five technical control themes:

- firewalls
- secure configuration
- user access control
- malware protection
- patch management

As a Cyber Essentials scheme Applicant, you must ensure that your organisation meets all the requirements. You may also be required to supply various forms of evidence before your chosen Certification Body can award certification at the level you seek. Proceed as follows:

1. Establish the **boundary of scope** for your organisation, and determine **what is in scope within this boundary**.
2. Review each of the five **technical control themes** and the **controls they embody as requirements**.
3. Take steps as necessary to **ensure that your organisation meets every requirement**, throughout the scope you have determined.

Definitions

- **Software** includes operating systems, commercial off-the-shelf applications, plugins, interpreters, scripts, libraries, network software and firmware.
- **Devices** includes all types of hosts, networking equipment, servers, networks and end-user equipment such as desktop computers, laptop computers, tablets and mobile phones (smartphones) — whether physical or virtual.
- **Applicant** means the organisation seeking certification, or sometimes the individual acting as the main point of contact, depending on context.

Scope

Overview of the scope

Assessment and certification can cover the whole of the Applicant's IT infrastructure, or a sub-set. Either way, the boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. The scope must be agreed between the Applicant and the Certification Body before assessment begins.

Information: We strongly recommend that the scope should include the whole IT infrastructure if possible, to achieve the best protection.

The requirements apply to all the devices and software that are within this boundary and that meet the conditions below:

- accept incoming network connections from untrusted Internet-connected hosts
- establish user-initiated outbound connections to arbitrary devices via the Internet
- control the flow of data between any of the above devices and the Internet

Bring your own device (BYOD)

- In addition to mobile or remote devices owned by the organisation, user-owned devices which access organisational data or services are in **scope**.
- Traditionally, user devices were managed through centralised administration, ensuring consistency across the organisation. In such cases, certification of the security controls is straightforward as there will be a standard build or reference to assess.
- BYOD complicates matters, as users are given more freedom to 'customise' their experience making consistent implementation of the controls more challenging.

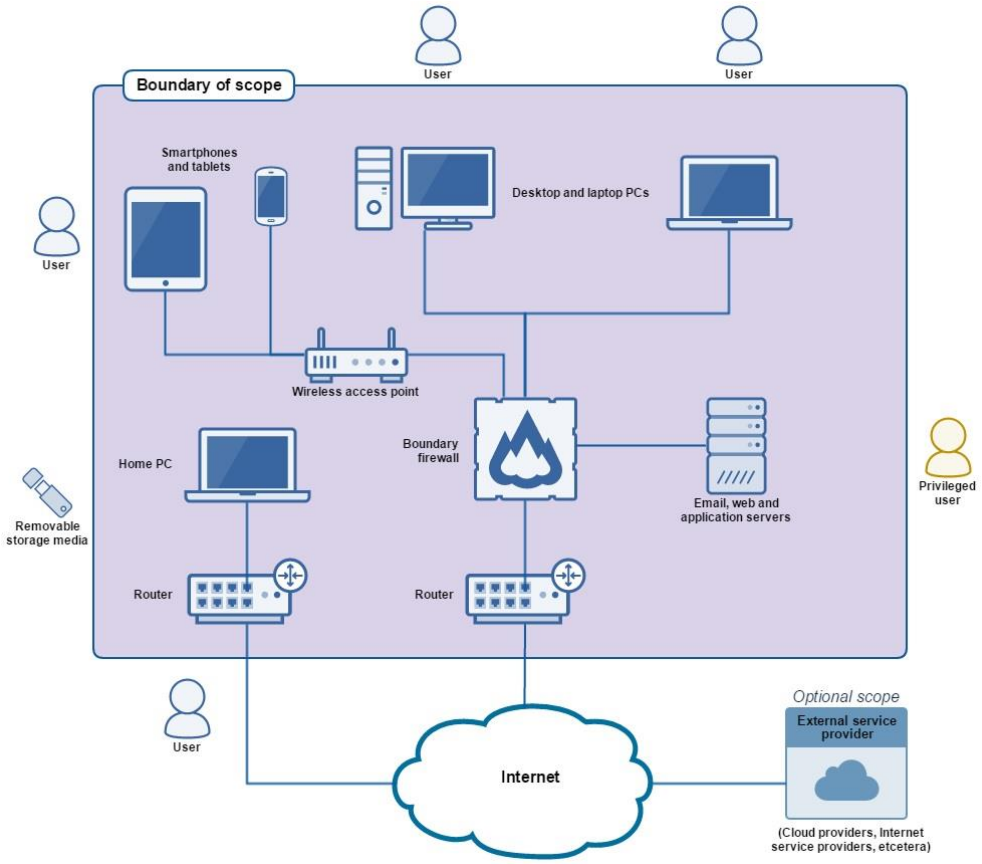


Figure 1: Scope of the requirements for IT infrastructure.

Wireless devices

Wireless devices (including wireless access points) are:

- **in scope** if they can communicate with other devices via the Internet
- **not in scope** if it is not possible for an attacker to attack directly from the Internet (the Cyber Essentials scheme is not concerned with attacks that can only be launched from within the signal range of the wireless device)

Externally managed services — cloud

If it is practicable for the Applicant to apply the requirements to its cloud services then it should include these services within the boundary of scope.

Example

Acme Corporation has procured infrastructure as a service (IaaS) from a cloud service provider. Acme has control of the operating systems on the infrastructure, and so it is able to apply the requirements. Acme will therefore include this service in its scope.

At present, software as a service (SaaS) and platform as a service (PaaS) are **not in scope** — the current requirements can not be mapped against them.

Externally managed services — other

Where the Applicant is using other externally managed services (such as remote administration) it may not be possible for the Applicant to meet all the requirements directly. The Applicant may **choose** whether or not to include these services within the boundary of scope, according to feasibility.

If included then the Applicant must be able to attest that the requirements that are outside of the Applicant's control are being adequately met by the service provider. Existing evidence may be considered (such as that provided through PCI certification of a cloud service, and ISO 27001 certifications that cover an appropriate scope).

Web applications

Commercial web applications created by development companies (rather than in-house developers) and which are publicly accessible from the Internet are **in scope** by default. Bespoke and custom components of web applications are **not in scope**. The primary mitigation against vulnerabilities in such applications is robust development and testing in line with commercial best practices, such as the Open Web Application Security Project (OWASP) standards.

Requirements, by technical control theme:

1. Firewalls *[Return to Framework] [Return to Mapping Matrix]*

Applies to : boundary firewalls; desktop computers; laptop computers; routers; servers.

Objective

Ensure that only safe and necessary network services can be accessed from the Internet.

Introduction

All devices run network services, which create some form of communication with other devices and services. By restricting access to these services, you reduce your exposure to attacks. This can be achieved using firewalls and equivalent network devices.

A boundary firewall is a network device which can restrict the inbound and outbound network traffic to services on its network of computers and mobile devices. It can help protect against cyber attacks by implementing restrictions, known as 'firewall rules', which can allow or block traffic according to its source, destination and type of communication protocol.

Alternatively, a host-based firewall may be configured on a device. This works in the same way as a boundary firewall but only protects the single device on which it is configured. This approach can provide for more tailored rules and means that the rules apply to the device wherever it is used. However, this increases the administrative overhead of managing firewall rules.

Requirements under this technical control theme

Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device).

For all firewalls (or equivalent network devices), the Applicant organisation must routinely:

a) change any default administrative password to an alternative that is difficult to guess (see Password-based authentication) — or disable remote administrative access entirely

b) prevent access to the administrative interface (used to manage firewall configuration) from the Internet, unless there is a clear and documented business need and the interface is protected by one of the following controls:

   i. a second authentication factor, such as a one-time token

   ii. an IP whitelist that limits access to a small range of trusted addresses

c) block unauthenticated inbound connections by default

d) ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation

e) remove or disable permissive firewall rules quickly, when they are no longer needed. Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

2. Secure configuration ***[Return to Framework] [Return to Mapping Matrix]***

Applies to: email, web, and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

Objective

Ensure that computers and network devices are properly configured to:

- reduce the level of inherent vulnerabilities
- provide only the services required to fulfil their role

Introduction

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:

- an administrative account with a predetermined, publicly known default password
- pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- pre-installed but unnecessary applications or services

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Requirements under this technical control theme

a) **Computers and network devices**

The Applicant must be active in its management of computers and network devices. It must routinely:

i. remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)

ii. change any default or guessable account passwords to something non-obvious

iii. remove or disable unnecessary software (including applications, system utilities and network services)

iv. disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet)

v. authenticate users before allowing Internet-based access to commercially or personally sensitive data, or data which is critical to the running of the organisation

b) **Password-based authentication**

The Applicant must make good use of the technical controls available to it on password-protected systems. As much as is reasonably practicable, technical controls and policies must shift the burden away from individual users and reduce reliance on them knowing and using good practices.

Users are still expected to pick sensible passwords.

For password-based authentication in Internet-facing services the Applicant must:

i. protect against brute-force password guessing, by using at least one of the following methods:
   - lock accounts after **no more** than 10 unsuccessful attempts
   - limit the number of guesses allowed in a specified time period to **no more** than 10 guesses within 5 minutes

ii. set a **minimum** password length of at least 8 characters

iii. **not** set a maximum password length

iv. change passwords promptly when the Applicant knows or suspects they have been compromised

v. have a password policy that tells users:
   - how to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet)
   - not to choose common passwords — this could be implemented by technical means, using a password blacklist
   - not to use the same password anywhere else, at work or at home
   - where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
   - if they may use password management software — if so, which software and how
   - which passwords they really must memorise and not record anywhere

The Applicant is *not* required to:

- enforce regular password expiry for any account (we actually advise against this — for more information see The problems with forcing regular password expiry)
- enforce password complexity requirements

3. User access control *[Return to Framework] [Return to Mapping Matrix]*

Applies to: email, web and application servers; desktop computers; laptop computers; tablets; mobile phones.

Objective

Ensure user accounts:

- are assigned to authorised individuals only
- provide access to only those applications, computers and networks actually required for the user to perform their role

Introduction

Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information. By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. When such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation.

'Administrative accounts' are especially highly privileged, for example. Such accounts typically allow:

- execution of software that has the ability to make significant and security relevant changes to the operating system
- changes to the operating system for some or all users
- creation of new accounts and allocation of their privileges

All types of Administrator will have such accounts, including Domain Administrators and Local Administrators.

Now consider that if a user opens a malicious URL or email attachment, any associated malware is typically executed with the privilege level of the account that user is currently operating. Clearly, you must take special care over the allocation and use of privileged accounts.

Example

Jody is logged in with an administrative account. If Jody opens a malicious URL or email attachment, any associated malware is likely to acquire administrative privileges. Unfortunately, this is exactly what happens. Using Jody's administrative privileges, a type of malware known as ransomware encrypts all of the data on the network and then demands a ransom. The ransomware was able to encrypt far more data than would have been possible with standard user privileges, making the problem that much more serious. **

Requirements under this technical control theme

The Applicant must be in control of its user accounts and the access privileges granted to each user account. It must also understand how user accounts authenticate and control the strength of that authentication. This means the Applicant must:

a) have a user account creation and approval process

b) authenticate users before granting access to applications or devices, using unique credentials (see Password-based authentication)

c) remove or disable user accounts when no longer required (when a user leaves the organisation or after a defined period of account inactivity, for example)

d) implement two-factor authentication, where available

e) use administrative accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

f) remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

4. Malware protection *[Return to Framework] [Return to Mapping Matrix]*

Applies to: desktop computers; laptop computers; tablets; mobile phones.

Objective

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

Introduction

The execution of software downloaded from the Internet can expose a device to malware infection.

Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources of malware infection include malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

If a system is infected with malware, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm from malware by:

- detecting and disabling malware before it causes harm (anti-malware)
- executing only software that you know to be worthy of trust (whitelisting)
- executing untrusted software in an environment that controls access to other data (sandboxing)

Example

Acme Corporation implements code signing alongside a rule that allows only vetted applications from the device application store to execute on devices. Unsigned and unapproved applications will not run on devices. The fact that users can only install trusted (whitelisted) applications leads to a reduced risk of malware infection.

Requirements under this technical control theme

The Applicant must implement a malware protection mechanism on all devices that are in scope. For each such device, the Applicant must use at least one of the three mechanisms listed below:

a) Anti-malware software

i. The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.

ii. The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.

iii. The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).

iv. The software must prevent connections to malicious websites on the Internet (by means of blacklisting, for example) — unless there is a clear, documented business need and the Applicant understands and accepts the associated risk.

Application whitelisting

- Only approved applications, restricted by code signing, are allowed to execute on devices. The Applicant must:
  - actively approve such applications before deploying them to devices
  - maintain a current list of approved applications Users must not be able to install any application that is unsigned or has an * invalid signature.

Application sandboxing

- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user. This includes:
  - other sandboxed applications
  - data stores, such as those holding documents and photos
  - sensitive peripherals, such as the camera, microphone and GPS
  - local network access

5. Patch management *[Return to Framework] [Return to Mapping Matrix]*

Applies to: web, email and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

Objective

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

Introduction

Any device that runs software can contain security flaws, known as 'vulnerabilities'.

Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks in organisations with these weaknesses.

Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as 'patches'. Patches may be made available to customers immediately or on a regular release schedule (perhaps monthly).

Caution

Product vendors do not generally release patches for products they no longer support — not even to fix vulnerabilities.

Requirements under this technical control theme

a) The Applicant must keep all its software up to date. Software must be:

i. licensed and supported
ii. removed from devices when no longer supported
iii. patched within 14 days of an update being released, where the patch fixes a * vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’ *

Information

- If the vendor uses different terms to describe the severity of vulnerabilities, see the precise definition in the Common Vulnerability Scoring System (CVSS). For the purposes of the Cyber Essentials scheme, ‘critical’ or ‘high risk’ vulnerabilities are those with the following values:
- attack vector: **network** only
- attack complexity: **low** only
- privileges required: **none** only
- user interaction: **none** only
- exploit code maturity: **functional** or **high**
- report confidence: **confirmed** or **high**

Caution

Some vendors release patches for multiple issues with differing severity levels as a single update. If such an update covers any ‘critical’ or ‘high risk’ issues then it must be installed within 14 days.

3. HMG-SPF (Target Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Source: HMG, Minimum Cyber Security Standard, Version 1.0 - June 2018, 7pp.
https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

Definitions:
"Shall" means that there is an obligation to perform the activity, without exception.
"Should" means that there is an expectation that the activity will be performed. There can be rare exceptions when the activity is not performed. However there must be a clear process in place to manage any risks.
"Users/Individuals/Administrators" also refers to staff, employees and contractors.
"**Departments**" also refers to organisations, agencies, Arm's Length Bodies and contractors.

The HMG Security Policy Framework (SPF) provides the mandatory protective security outcomes that all Departments are required to achieve. This document defines the minimum security measures that Departments **shall** implement with regards to protecting their information, technology and digital services to meet their SPF and National Cyber Security Strategy obligations.

As far as possible the security standards define outcomes, allowing Departments flexibility in how the standards are implemented, dependent on their local context. The definition of 'sensitive', 'essential', 'important' and 'appropriate' are deliberately left open, so that Departments can apply their own values based on their particular circumstances, however Departments are accountable for the effectiveness of these decisions and they **shall** reflect the HMG Government Security Classifications Policy[5] where relevant.

Compliance with the standards can be achieved in many ways, depending on the technology choices and business requirements in question. For Digital Services, this set of standards is complementary to the Digital Service Manual.

The standard presents a minimum set of measures and departments should look to exceed them wherever possible. Over time, the measures will be incremented to continually 'raise the bar', address new threats or classes of vulnerabilities and to incorporate the use of new Active Cyber Defence measures that Departments will be expected to use. This **shall** be read in conjunction with the minimum physical, personnel and incident management standards for Government.

[5] The HMG Government Security Classifications Policy describes how Government classifies information assets and applies to all information that Government processes to deliver services and conduct business, including information received from or exchanged with external partners.

IDENTIFY 1. Departments shall put in place appropriate cyber security governance processes. ***[Return to Framework]*** ***[Return to Mapping Matrix]***	a) There **shall** be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services. b) There **shall** be appropriate management policies and processes in place to direct the Departments overall approach to cyber security. c) Departments **shall** identify and manage the significant risks to sensitive information and key operational services. d) Departments **shall** understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain. This includes ensuring that the standards defined in this document are met by the suppliers of 3rd party services. This could be achieved by having suppliers assure their cyber security against the HMG Cyber Security Standard, or by requiring them to hold a valid Cyber Essentials[6] certificate as a minimum. Cyber Essentials allows a supplier to demonstrate appropriate diligence with regards to standard number six but the Department **should**, as part of their risk assessment, determine whether this is sufficient assurance. e) Departments **shall** ensure that senior accountable individuals receive appropriate training and guidance on cyber security and risk management and **should** promote a culture of awareness and education about cyber security across the Department.
2. Departments shall identify and catalogue sensitive information they hold. ***[Return to Framework] [Return to Mapping Matrix]***	a) Departments **shall** know and record: I. What sensitive information they hold or process II. Why they hold or process that information III. Where the information is held IV. Which computer systems or services process it V. The impact of its loss, compromise or disclosure
3. Departments shall identify and catalogue the key operational services they provide. ***[Return to Framework] [Return to Mapping Matrix]***	a) Departments **shall** know and record: I. What their key operational services are II. What technologies and services their operational services rely on to remain available and secure III. What other dependencies the operational services have (power, cooling, data, people etc.) IV. The impact of loss of availability of the service
4. The need for users to access sensitive information or key operational services shall be understood and continually managed. ***[Return to***	a) Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. b) Access **shall** be removed when individuals leave their role or the organisation. Periodic reviews **should** also take place to ensure appropriate access is maintained.

[6] Cyber Essentials helps guard against the most common cyber threats and demonstrates a commitment to cyber security. It is based on five technical controls but does not cover the entirety of the HMG Cyber Security Standard.

Framework *] [**Return to Mapping Matrix**]*	
PROTECT 5. Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems. *[**Return to Framework**] [**Return to Mapping Matrix**]*	a) Access to sensitive information and services **shall** only be provided to authorised, known and individually referenced users or systems. b) Users and systems **shall** always be identified and authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service, you may also need to authenticate and authorise the device being used for access.
6. Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities. *[**Return to Framework**] [**Return to Mapping Matrix**]*	**a) To protect your enterprise technology, you shall:** I. Track and record all hardware and software assets and their configuration II. Ensure that any infrastructure is not vulnerable to common cyber-attacks. This **should** be through secure configuration and patching, but where this is not possible, then other mitigations (such as logical separation) **shall** be applied. III. Validate that through regular testing for the presence of known vulnerabilities or common configuration errors. IV. Use the UK Public Sector DNS Service to resolve internet DNS queries. V. Ensure that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators. VI. Understand and record the Departmental IP ranges. VII. Where services are outsourced (for example by use of cloud infrastructure or services), you **shall** understand and accurately record which security related responsibilities remain with the Departments and which are the supplier's responsibility. **b) To protect your end user devices, you shall:** I. Identify and account for all end user devices and removable media. II. Manage devices which have access to sensitive information, or key operational services, such that technical policies can be applied and controls can be exerted over software that interacts with sensitive information. III. Be running operating systems and software packages which are patched regularly, and as a minimum in vendor support. IV. Encrypt data at rest where the Department cannot expect physical protection, such as when a mobile device or laptop is taken off-site or on removable media.

	V. Have the ability to remotely wipe and/or revoke access from an end user device. **c) To protect email, you <u>shall</u>:** 1. Support Transport Layer Security Version 1.2 (TLS v1.2) for sending and receiving email securely. 2. Have Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domains to make email spoofing difficult. 3. Implement spam and malware filtering, and enforce DMARC on inbound email. **d) To protect digital services, you <u>shall</u>:** I. Ensure the web application is not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities[7]. II. Ensure the underlying infrastructure is secure, including verifying that the hosting environment is maintained securely and that you have appropriately exercised your responsibilities for securely configuring the infrastructure and platform. III. Protect data in transit using well-configured TLS v1.2. IV. Regularly test for the presence of known vulnerabilities and common configuration errors. You **shall** register for and use the NCSC's Web Check service.
7. Highly privileged accounts should not be vulnerable to common cyber-attacks. ***[Return to Framework] [Return to Mapping Matrix]***	a) Users with wide ranging or extensive system privilege **shall** not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing. b) Multi-factor authentication **shall** be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi-factor authentication **shall** be used for access to enterprise level social media accounts. c) Passwords for highly privileged system accounts, social media accounts and infrastructure components **shall** be changed from default values and **shall** not be easy to guess. Passwords which would on their own grant extensive system access, **should** have high complexity.
DETECT 8. Departments shall take steps to detect common cyber-attacks. ***[Return to***	a) As a minimum, Departments **shall** capture events that could be combined with common threat intelligence sources e.g. Cyber Security Information Sharing Partnership (CISP) to detect known threats. b) Departments **shall** have a clear definition of what must be protected and why (based upon Standard 1), which in turn

[7] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

***Framework*] [*Return to Mapping Matrix*]**	influences and directs the monitoring solution to detect events which might indicate a situation the Department wishes to avoid. c) Any monitoring solution **should** evolve with the Department's business and technology changes, as well as changes in threat. d) Attackers attempting to use common cyber-attack techniques **should** not be able to gain access to data or any control of technology services without being detected. e) Digital services that are attractive to cyber criminals for the purposes of fraud **should** implement transactional monitoring techniques from the outset.
RESPOND 9. Departments shall have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services. ***[Return to Framework] [Return to Mapping Matrix]***	a) Departments **shall** develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents **shall** be recorded regardless of the need to report them. b) Departments **shall** have communication plans in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive). c) In the event of an incident that involves a personal data breach Departments **shall** comply with any legal obligation to report the breach to the Information Commissioner's Office. Further information on this can be found here. d) The incident response and management plan **should** be tested at regular intervals to ensure all parties understand their roles and responsibilities as part of the plan. Post testing findings **should** inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated. e) On discovery of an incident, mitigating measures **shall** be assessed and applied at the earliest opportunity, drawing on expert advice where necessary (e.g. a Cyber Incident Response (CIR) company or NCSC). f) Post incident lessons **shall** be assessed and lessons implemented into future iterations of the incident management plan.
RECOVER 10. Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.	a) Departments **shall** identify and test contingency mechanisms to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service. This may include the preservation of out of band or manual processes for essential services or CNI. b) Restoring the service to normal operation **should** be a well-practised scenario. c) Post incident recovery activities **shall** inform the immediate future technical protection of the system or service, to ensure the same

[Return to Framework] [Return to Mapping Matrix]	issue cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated.

4. 10 Steps to Cyber Security (Target Progression Stage) [Return to Framework] [Return to Mapping Matrix]

Source: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

1. Risk Management Regime [Return to Framework] [Return to Mapping Matrix]

Summary
Organisations rely on technology, systems and Information to support their business goals. It is important that organisations apply a similar level of rigour to assessing the risks to its technology, systems and information assets as it would to other risks that might have a material business impact, such as regulatory, financial or operational risks. This can be achieved by embedding an appropriate risk management regime across the organisation, which is actively supported by the board, senior managers and an empowered governance structure.

Defining and communicating the organisation's attitude and approach to risk management is crucial. Boards may wish to consider communicating their risk management approach and policies across the organisation to ensure that employees, contractors and suppliers are aware of the organisation's risk management boundaries.

What is the risk?
Taking risk is a necessary part of doing business in order to create opportunities and help deliver business objectives. For any organisation to operate successfully it needs to address risk and respond proportionately and appropriately to a level which is consistent with what risks an organisation is willing, or not, to tolerate. If an organisation does not identify and manage risk it can lead to business failure.

The lack of an effective risk management and governance structure may lead to the following:

- **Exposure to risk:** Without effective governance processes the Board will be unlikely to understand and manage the overall risk exposure of the organisation.
- **Missed business opportunities:** Risk decisions taken within a dedicated security function, rather than organisationally, will be motivated by achieving high levels of security. This may promote an overly cautious approach to risk leading to missed business opportunities or additional cost.
- **Ineffective policy implementation:** The board has overall ownership of the corporate security policy. Without effective risk management and governance processes the Board won't have confidence that its stated policies are being consistently applied across the business as a whole.

How can the risk be managed?

1. **Establish a governance framework:** A governance framework needs to be established that enables and supports a consistent and empowered approach to risk management across the organisation, with ultimate responsibility residing at board level;

2. **Determine what risks an organisation is willing to tolerate and what is unacceptable:** Agree what risks you are prepared to tolerate in pursuit of your business objectives. Produce guidance and statements that helps individuals throughout the organisation make appropriate risk based decisions.
3. **Maintain board engagement:** The board should regularly review risks that may arise from an attack on technology or systems used. To ensure senior ownership and oversight, the risks resulting from attack should be documented in the corporate risk register and regularly reviewed. Entering into knowledge sharing partnerships with other companies and law enforcement, and joining the CiSP Information Sharing Platform, can help you understand new and emerging threats as well as share approaches and mitigations that might work.
4. **Produce supporting policies:** An overarching technology and security risk policy should be created and owned by the board to help communicate and support risk management objectives, setting out the risk management strategy for the organisation as a whole.
5. **Adopt a lifecycle approach to risk management:** Technology changes, as does the threat and therefore risks change over time. A continuous through-life process needs to be adopted to ensure security controls remain effective and appropriate.
6. **Apply recognised standards:** Consider the application of recognised sources of security management good practice, such as the ISO/IEC 27000 series of standards.
7. **Make use of endorsed assurance schemes:** Consider adopting the Cyber Essentials Scheme. It provides guidance on the basic controls that should be put in place to manage risk of online cyber attack to enterprise technology and offers a certification process that demonstrates your commitment to cyber security.
8. **Educate users and maintain awareness:** All users have a responsibility to help manage security risks. Provide appropriate training and user education that is relevant to their role and refresh it regularly. Encourage staff to participate in knowledge sharing exchanges with peers across your organisation and beyond.
9. **Promote a risk management culture**: Risk management needs to be organisation-wide, driven by corporate governance from the top down, with user participation demonstrated at every level of the business.

2. Secure Configuration *[Return to Framework] [Return to Mapping Matrix]*

Summary
Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

What is the risk?

Establishing and actively maintaining the secure configuration of systems should be seen as a key security control. Systems that are not effectively managed will be vulnerable to attacks that may have been preventable. Failure to implement good configuration and patch management can lead to the following risks:

- **Unauthorised changes to systems:** The protections you believe you have in-place may be changed by unauthorised individuals, either internal or external, leaving information at risk.
- **Exploitation of software bugs:** Attackers will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patches have been issued but not applied.
- **Exploitation of insecure system configuration:** An attacker could exploit a system that has been poorly configured by:
    - gaining access to information they are not authorised to see
    - taking advantage of unnecessary user rights or system privilege
    - exploiting unnecessary functionality that has not been removed or disabled
    - connecting unauthorised equipment that is then able to compromise information or introduce malware
    - creating a back door to use in the future for malicious purposes

How can the risk be managed?
Organisations need to ensure that they have put in place measures to minimise the risk of poor system configuration. The following security controls should be considered:

1. **Use supported software:** Use versions of operating systems, web browsers and applications that are vendor (or community) supported.
2. **Develop and implement policies to update and patch systems:** Implement policies to ensure that security patches are applied in an appropriate time frame, such a 14 days for critical patches. Automated patch management and software update tools might be helpful. In cases where it is not possible to patch a vulnerability steps should be taken to make it very difficult to exploit. This might include making it difficult for an attacker to communicate with the system.
3. **Create and maintain hardware and software inventories:** Create inventories of all authorised hardware and software used across the organisation. Ideally the inventory should capture the physical location, business owner and purpose of hardware together with the version and patch status of all software. Tools can be used to help identify unauthorised hardware or software.
4. **Manage your operating systems and software:** Implement a secure baseline build for all systems and components, including hardware and software. Any functionality or application that does not support a user or business need should be removed or disabled. The secure build profile should be managed by a configuration control process and any deviation from the standard build should be documented and approved.

5. **Conduct regular vulnerability scans:** Regularly run automated vulnerability scanning tools against all networked devices and remedy or manage any identified vulnerabilities within an agreed time frame.
6. **Establish configuration control and management:** Implement policies that set out a configuration control and change management process for all systems.
7. **Disable unnecessary peripheral devices and removable media access**: Assess the need for access to peripheral devices and removable media. Disable ports and system functionality that does not support a user or business need.
8. **Implement white-listing and execution control**: Create and maintain a whitelist of authorised applications and software that can be executed. In addition, systems should be capable of preventing the installation and execution of unauthorised software by employing process execution controls.
9. **Limit user ability to change configuration:** Provide users with the permissions that they need to fulfil their business role. Users with 'normal' privileges should be prevented from installing or disabling any software or services running on the system.
10. **Limit privileged user functionality:** Ensure that users with privileged system rights (administrators) have constrained internet and email access from their privileged account. This limits exposure to spear phishing and reduces the ability of an attacker to achieve wide system access through exploiting a single vulnerability

3. Network Security *[Return to Framework] [Return to Mapping Matrix]*

Summary

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation).

Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

What is the risk?

Networks need to be protected against both internal and external threats. Organisations that fail to protect their networks appropriately could be subject to a number of risks, including:

- **Exploitation of systems:** Ineffective network design may allow an attacker to compromise systems that perform critical functions, affecting the organisations ability to deliver essential services or resulting in severe loss of customer or user confidence.
- **Compromise of information**: A poor network architecture may allow an attacker to compromise sensitive information in a number of ways. They may be able to access systems hosting sensitive information directly or perhaps allow an attacker to intercept

poorly protected information whilst in transit (such as between your end user devices and a cloud service).

- **Import and export of malware:** Failure to put in place appropriate security controls could lead to the import of malware and the potential to compromise business systems. Conversely users could deliberately or accidentally release malware or other malicious content externally with associated reputational damage.
- **Denial of service:** Internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks, where access to services and resources are denied to legitimate users or customers.
- **Damage or defacement of corporate resources:** Attackers that have successfully compromised the network may be able to further damage internal and externally facing systems and information (such as defacing your organisation's websites, or posting onto your social media accounts), harming the organisation's reputation and customer confidence.

How can the risk be managed?

Produce, implement and maintain network security designs and policies that align with the organisation's broader risk management approach. It may be helpful to follow recognised network design principles (eg ISO 27033) to help define an appropriate network architecture including both the network perimeter, any internal networks, and links with other organisations such as service providers or partners.

1. **Manage the network perimeter**: Manage access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content:

    a) **Use firewalls:** Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a white list should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Ensure you have effective processes for managing changes to avoid workarounds.

    b) **Prevent malicious content**: Deploy malware checking solutions and reputation-based scanning services to examine both inbound and outbound data at the perimeter in addition to protection deployed internally. The antivirus and malware solutions used at the perimeter should ideally be different to those used to protect internal networks and systems in order to provide some additional defence in depth.

2. **Protect the internal network:** Ensure that there is no direct routing between internal and external networks (especially the Internet), which limits the exposure of internal systems to network attack from the Internet. Monitor network traffic to detect and react to attempted or actual network intrusions.

a) **Segregate networks as sets**: Identify, group and isolate critical business systems and apply appropriate network security controls to them.

b) **Secure wireless access:** All wireless access points should be appropriately secured, only allowing known devices to connect to corporate Wi-Fi services. Security scanning tools may be useful to detect and locate unauthorised or spoof wireless access points.

c) **Enable secure administration:** Administrator access to any network component should properly authenticated and authorised. Make sure default administrative passwords for network equipment are changed.

d) **Configure the exception handling processes:** Ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.

e) **Monitor the network:** Network intrusion detection and prevention tools should be deployed on the network and configured by qualified staff. The capabilities should monitor all traffic for unusual incoming and outgoing activity that could be indicative of an attack. Alerts generated by the system should be promptly managed by appropriately trained staff.

f) **Assurance processes**: Conduct regular penetration tests of the network architecture and undertake simulated cyber attack exercises to ensure that security controls have been well implemented and are effective.

4. Managing User Privileges *[Return to Framework] [Return to Mapping Matrix]*

Summary
If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

What is the risk?
Organisations should understand what level of access employees need to information, services and resources in order to do their job otherwise it won't be possible to manage rights appropriately. Failure to effectively manage user privileges could result in the following risks being realised:

- **Misuse of privileges:** Users could either accidentally or deliberately misuse the privileges assigned to them. This may result in unauthorised access to information to either the user or a third party or to unauthorised system changes having a direct security or operational impact.

- **Increased attacker capability:** Attackers may use redundant or compromised user accounts to carry out attacks and, if able, they may return to reuse the compromised account or possibly sell access to others. The system privileges provided to the original user of the compromised account will be available to the attacker to use which is why they particularly seek to gain access to highly privileged or administrative accounts.
- **Negating established security controls:** Where attackers have privileged system access they may make changes to security controls to enable further or future attack or might attempt to cover their tracks by making changing or audit logs.

How can the risk be managed?
Organisations should determine what rights and privileges users need to effectively perform their duties and implement a policy of 'least privilege'.

1. **Establish effective account management processes:** Manage user accounts from creation, through-life and eventually revocation when a member of staff leaves or changes role. Redundant accounts, perhaps provided for temporary staff or for testing, should be removed or suspended when no longer required.
2. **Establish policies and standards for user authentication and access control:** A corporate password policy should be developed that seeks an effective balance between security and usability as set out in our password guidance. For some accounts an additional authentication factor (such as a token) may be appropriate.
3. **Limit user privileges:** Users should be provided with the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role.
4. **Limit the number and use of privileged accounts:** Strictly control the granting of highly privileged system rights, reviewing the ongoing need regularly. Highly privileged administrative accounts should not be used for high risk or day to day user activities, for example web browsing and email. Administrators should use normal accounts for standard business use.
5. **Monitor:** Monitor user activity, particularly access to sensitive information and the use of privileged account actions. Respond where activities are outside of normal, expected bounds (such as access to large amounts of sensitive information outside of standard working hours).
6. **Limit access to the audit system and the system activity logs:** Activity logs from network devices should be sent to a dedicated accounting and audit system that is separated from the core network. Access to the audit system and the logs should be strictly controlled to preserve the integrity of the content and all privileged user access recorded.
7. **Educate users and maintain their awareness:** All users should be aware of the policy regarding acceptable account usage and their personal responsibility to adhere to corporate security policies.

5. User Education and Awareness ***[Return to Framework] [Return to Mapping Matrix]***

Summary
Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well helping to establish a security-conscious culture.

What is the risk?
Users have a critical role to play in helping to keep the organisation secure, but they must also be able to effectively do their jobs. Organisations that do not effectively support employees with the right tools and awareness may be vulnerable to the following risks:

- **Removable media and personally owned devices:** Without clearly defined and usable policies on the use of removable media and personally owned devices, staff may connect devices to the corporate infrastructure that might lead to the inadvertent import of malware or compromise of sensitive information
- **Legal and regulatory sanction:** If users are not aware and supported in how they handle particular classes of sensitive information, the organisation may be subject to legal and regulatory sanction
- **Incident reporting culture:** Without an effective reporting culture there will be poor dialogue between users and the security team. This is essential to uncovering near misses and areas where technology and processes can be improved, as well as reporting actual incidents.
- **Security Operating Procedures:** If security operating procedures are not balanced to support how users perform their duties, security can be seen as a blocker and possibly ignored entirely. Alternatively, if users follow the procedures carefully this might damage legitimate business activity.
- **External attack:** Since users have legitimate system accesses and rights, they can be a primary focus for external attackers. Attacks such as phishing or social engineering attempts rely on taking advantage of legitimate user capabilities and functions.
- **Insider threat:** Changes over time in an employee's personal situation could make them vulnerable to coercion, and they may release personal or sensitive commercial information to others. Dissatisfied employees may try to abuse their system level privileges or coerce other employees to gain access to information or systems to which they are not authorised. Equally, they may attempt to steal or physically deface computer resources.

How can the risk be managed?

1. **Produce a user security policy:** Develop a user security policy, as part of the overarching corporate security policy. Security procedures for all systems should be produced with consideration to different business roles and processes. A 'one size fits all' approach is typically not appropriate for many organisations. Policies and procedures should be described in simple business-relevant terms with limited jargon.

2. **Establish a staff induction process:** New users (including contractors and third party users) should be made aware of their personal responsibility to comply with the corporate security policies as part of the induction process. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action.
3. **Maintain user awareness of the security risks faced by the organisation:** All users should receive regular refresher training on the security risks to the organisation. Consider providing a platform for users to enquire about security risks and discuss the advice they are given. On the whole, users want to do the right thing, so giving them guidance to put security advice into practice will help.
4. **Support the formal assessment of security skills:** Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognised certification scheme. Some security related roles such as system administrators, incident management team members and forensic investigators may require specialist training.
5. **Monitor the effectiveness of security training:** Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training provided will allow for a two-way dialogue between the security team and users.
6. **Promote an incident reporting culture:** The organisation should enable a security culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, without fear of recrimination. This should be reciprocated with a culture where security professionals acknowledge that security-related effort by non-security staff is time away from their work, and is helping to protect the organisation.
7. **Establish a formal disciplinary process:** All staff should be made aware that any abuse of the organisation's security policies will result in disciplinary action being taken against them. All sanctions detailed in policy should be enforceable at a practical level.

6. Incident Management *[Return to Framework] [Return to Mapping Matrix]*

Summary
All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

What is the risk?
Security incidents will inevitably happen and they will vary in their level of impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking the organisation's business continuity or disaster recovery plans. Some incidents can, on further analysis, be indicative of more severe underlying problems.

If businesses fail to implement an incident management capability to detect, manage and analyse security incidents the following risks could be realised:

- **Managing business harm:** Failure to realise that an incident is happening or has occurred limits your ability to manage it effectively. This may lead to a much greater overall business impact, such as significant system outage, serious financial loss or erosion of customer confidence.
- **Continual disruption:** An organisation that fails to address the root cause of incidents (such as poor technology or weaknesses in the corporate security approach) could be exposed to repeated or continual compromise or disruption.
- **Failure to comply with legal and regulatory reporting requirements:** An incident resulting in the compromise of sensitive information covered by mandatory reporting requirements could lead to legal or regulatory penalties.

The organisation's business profile or role will determine the type and nature of incidents that could occur and the impact they might have, so a risk-based approach should be used to shape incident management plans.

How can the risk be managed?

1. **Establish an incident response capability:** Identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability. Resources could be in house or you might pre-establish a relationship with an specialist incident management company. This should address the full range of incidents that could occur and set out appropriate responses. The supporting policy, processes and plans should be risk based and cover any legal or regulatory reporting requirements.
2. **Provide specialist training:** The incident response team may need specialist knowledge and expertise across a number of technical (including forensic investigation) and non-technical areas. You should identify recognised sources (internal or external) of specialist incident management training and maintain the organisation's skill base.
3. **Define the required roles and responsibilities:** Appoint and empower specific individuals (or suppliers) to handle incidents and provide them with clear terms of reference to make decisions and manage any incident that may occur. Ensure that the contact details of key personnel are readily available to use in the event of an incident.
4. **Establish a data recovery capability:** Data losses can occur and so a systematic approach to the backup of essential data should be implemented. Where physical backup media is used this should be held in a physically secure location, ideally offsite. The ability to recover archived data for operational use should be regularly tested.
5. **Test the incident management plans:** All plans supporting security incident management (including business continuity and disaster recover plans) should be regularly tested. The outcome of the tests should be used to inform the future development of the incident management plans.

6. **Decide what information will be shared and with whom:** For services or information bound by specific legal or regulatory reporting requirements you may have to report incidents. All internal and external reporting requirements should be clearly identified in the incident management plan.
7. **Collect and analyse post-incident evidence**: The preservation and analysis of the sequence of events that led up to the incident is critical to identify and remedy the root cause. The collected evidence could also potentially support any follow on disciplinary or legal action and the incident management policy should set out clear guidelines to follow.
8. **Conduct a lessons learned review:** Log the actions taken during an incident and review the performance of the incident management process post incident (or following a test) to see what aspects worked well and what could be improved. Review the organisational response and update any relevant policies or user training that could have prevented the incident from occurring.
9. **User awareness:** Users should be aware of their responsibilities and how they can report and respond to incidents. Users should be encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination.
10. **Report criminal incidents to law enforcement:** It is important that potential or actual cyber crime is reported to Action Fraud or other relevant law enforcement agency.

7. Malware Prevention *[Return to Framework] [Return to Mapping Matrix]*

Summary

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by implementing appropriate security controls as part of an overall 'defence in depth' approach.

What is the risk?

Malware infections can cause material harm to your systems. This might include disruption of business services, unauthorised export of sensitive information or loss of access to critical data (eg caused by ransomware).The range, volume and source of information exchanged (as well as the technologies used) provide a range of opportunities for malware to be imported. Examples include:

- **Email:** Email still provides a primary path for internal and external information exchange. Malicious email attachments can cause their payload to be executed when the file is opened or otherwise processed. Email with malicious content may be specifically targeted at known individuals (known as spear phishing) with access to sensitive information, or at roles with elevated privileges. Alternatively malicious email may include embedded links that direct users to websites hosting malicious content.

- **Web browsing:** Users could browse (or be directed to) websites that may contain malicious content which seeks to compromise applications (such as the browser) that interact with that content
- **Web services:** User access to social media and other web based services could provide an ability for users to import a variety of data formats
- **Removable media and personally owned devices:** Malware can be transferred to a corporate system through the uncontrolled introduction of removable media or the direct connection of untrusted devices. This might include (for example) connecting a smartphone via a USB port, even if intended only to charge the device.

How can the risk be managed?

1. **Develop and implement anti-malware policies:** Develop and implement corporate anti-malware policies and standards and ensure that they are consistently implemented across your infrastructure. The approach should be applicable and relevant to all business areas.
2. **Manage all data import and export:** All data should be scanned for malicious content at the network perimeter, whether that's internet gateways or facilities to introduce removable media.
3. **Blacklist malicious web sites:** Ensure that the perimeter gateway uses blacklisting to block access to known malicious web sites.
4. **Provide dedicated media scanning machines:** Stand-alone workstations can be provided and equipped with appropriate anti-virus products. The workstation should be capable of scanning the content contained on any type of media and inspect recursive content within files. Ideally every scan should be binded to a known user.
5. **Establish malware defences:** Malware can attack any system process or function so a technical architecture that provides multiple defensive layers (defence in depth) should be considered. This should include the following controls.
    a) End user device protection: On many platforms host based malware protection is provided by using antivirus applications. However several platforms (such as some smartphones) meet the need to protect against malware using other mechanisms such as application whitelisting. For further information see the NCSC End User Device guidance.
    b) Deploy antivirus and malicious code checking solutions to scan inbound and outbound objects at the network perimeter. Where host based antivirus is used it may be sensible to use different products to increase overall detection capability. Any suspicious or infected malicious objects should be quarantined for further analysis.
    c) Deploy a content filtering capability on all external gateways to try to prevent attackers delivering malicious code to common desktop applications such as the web browser.
    d) Install firewalls where appropriate, configuring them to deny traffic by default.

e) If the business processes can support it, consider disabling certain browser plugins or scripting languages.

f) Where possible, disable the *autorun* function to prevent the automatic execution of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content.

g) Ensure systems and components are well configured according to the secure baseline build and kept up to date.

6. **User education and awareness**: Users should understand the risks from malware and the day-to-day processes they can follow to help prevent a malware infection from occurring. The user instructions should contain the following:

a) Try to stop and think *before* clicking on links, but don't worry if you think you've clicked on something harmful. Tell your security team as soon as possible and they will help.

b) Do not connect any unapproved removable media or personally owned device to the network.

c) Report any strange or unexpected system behaviour to the appropriate security team.

d) Maintain awareness of how to report a security incident.

8. Monitoring *[Return to Framework] [Return to Mapping Matrix]*

Summary

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

What is the risk?

Monitoring provides the means to assess how systems are being used and whether they are being attacked. Without the ability to monitor your systems you may not be able to:

- **Detect attacks:** Either originating from outside the organisation or attacks as a result of deliberate or accidental user activity. Attacks may be directly targeted against technical infrastructure or against the services being run. Attacks can also seek to take advantage of legitimate business services, for example by using stolen credentials to defraud payment services.
- **React to attacks:** An effective response to an attack depends upon first being aware than an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused.
- **Account for activity:** You should have a complete understanding of how systems, services and information are being used by users. Failure to monitor systems and their use could lead to attacks going unnoticed and/or non-compliance with legal or regulatory requirements.

How can the risk be managed?

1. **Establish a monitoring strategy and supporting policies:** Develop and implement a monitoring strategy based on business need and an assessment of risk. The strategy should include both technical and transactional monitoring as appropriate. The incident management plan as well as knowledge of previous security incidents should inform the approach.
2. **Monitor all systems**: Ensure that all networks, systems and services are included in the monitoring strategy. This may include the use of the use of network, host based and wireless Intrusion Detection Systems (IDS). These solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour.
3. **Monitor network traffic**: Inbound and outbound traffic traversing network boundaries should be monitored to identify unusual activity or trends that could indicate attacks. Unusual network traffic (such as connections from unexpected IP ranges overseas) or large data transfers should automatically generate security alerts with prompt investigation.
4. **Monitor user activity:** The monitoring capability should have the ability to identify the unauthorised or accidental misuse of systems or data. Critically, it should be able to tie specific users to suspicious activity. Take care to ensure that all user monitoring complies with all legal or regulatory constraints.
5. **Fine-tune monitoring systems**: Ensure that monitoring systems are tuned appropriately to only collect events and generate alerts that are relevant to your needs. Inappropriate collection of monitoring information and generation of alerts can mask the detection of real attacks as well as be costly in terms of data storage and investigatory resources required.
6. **Establish a centralised collection and analysis capability:** Develop and deploy a centralised capability that can collect and analyse information and alerts from across the organisation. Much of this should be automated due to the volume of data involved, enabling analysts to concentrate on anomalies or high priority alerts. Ensure that the solution architecture does not itself provide an opportunity for attackers to bypass normal network security and access controls.
7. **Provide resilient and synchronised timing:** Ensure that the monitoring and analysis of audit logs is supported by a centralised and synchronised timing source that is used across the entire organisation to support incident response and investigation.
8. **Align the incident management policies:** Ensure that policies and processes are in place to appropriately manage and respond to incidents detected by monitoring solutions.
9. **Conduct a 'lessons learned' review:** Ensure that processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability.

9. Removable Media Controls *[Return to Framework] [Return to Mapping Matrix]*

Summary
Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

What is the risk?
Removable media introduces the capability to transfer and store huge volumes of sensitive information as well as the ability to import malicious content. The failure to manage the import and export of information using removable media could expose you to the following risks:

- **Loss of information:** Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information stored on it. Some media types will retain information even after user deletion, placing information at risk where the media is used between systems (or when the media is disposed of)
- **Introduction of malware:** The uncontrolled use of removable media can increase the risk of introducing malware to systems.
- **Reputational damage:** The loss of media can result in significant reputational damage, even if there is no evidence of any specific data loss.

How can the risk be managed?

1. **Produce corporate policies:** Develop and implement policies and solutions to control the use of removable media. Do not use removable media as a default mechanism to store or transfer information. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms.
2. **Limit the use of removable media:** Where the use of removable media is required to support the business need, it should be limited to the minimum media types and users needed. The secure baseline build should deny access to media ports by default, only allowing access to approved users.
3. **Scan all media for malware:** Removable media should be automatically scanned for malware when it is introduced to any system. The removable media policy could also require that any media brought into the organisation is scanned for malicious content by a standalone machine before any data transfer takes place.
4. **Formally issue media to users:** All removable media should be formally issued to individual users who will be accountable for its use and safe keeping. Users should not use unofficial media, such as USB sticks given away at conferences.
5. **Encrypt information held on media:** Sensitive information should be encrypted at rest on media. If encryption is not employed then appropriate physical protection of the media is critical.
6. **Actively manage the reuse and disposal of removable media:** Where removable media is to be reused or destroyed then appropriate steps should be taken to ensure that

previously stored information will not be accessible. The processes will be dependent on the value of the information and the risks posed to it and could range from an overwriting process to the physical destruction of the media by an approved third party. For more information refer to Secure sanitisation of storage media.

7. **Educate users and maintain awareness:** Ensure that all users are aware of their personal responsibilities for following the removable media security policy.

10. Home and Mobile Working *[Return to Framework] [Return to Mapping Matrix]*

Summary

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

What is the risk?

Mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft/loss of devices. Organisations that do not establish sound mobile working and remote access practices might be vulnerable to the following risks:

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.
- **Being overlooked:** Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.
- **Loss of credentials:** If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.
- **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

How can the risk be managed?

1. **Assess the risks and create a mobile working policy**: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed.

2. **Educate users and maintain awareness:** All users should be trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate securely by following clear procedures. This should include direction on:
   - secure storage and management of user credentials
   - incident reporting
   - environmental awareness (the risks from being overlooked, etc.)
3. **Apply the secure baseline build:** Develop and apply a secure baseline build and configuration for all types of mobile device used by the organisation. Consider integrating the security controls provided in the End User Device guidance into the baseline build for mobile devices.
4. **Protect data at rest:** Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.
5. **Protect data in transit:** If the user is working remotely the connection back to the corporate network will probably use the Internet. All information exchanged should be appropriately encrypted. See Using IPsec to Protect Data and Using TLS to protect data.
6. **Review the corporate incident management plans**: Mobile working attracts significant risks and security incidents will occur even when users follow the security procedures. The incident management plans should be sufficiently flexible to deal with the range of security incidents that could occur, including the loss or compromise of a device. Ideally, technical processes should be in place to remotely disable a device that has been lost or at least deny it access to the corporate network.

5. GDPR-ICO (Target Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Source: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

A) Manage security risk

You have appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to personal data

A.1 Governance *[Return to Framework] [Return to Mapping Matrix]*
You have appropriate data protection and information security policies and processes in place. If required, you ensure that you maintain records of processing activities, and have appointed a Data Protection Officer.

A.2 Risk management *[Return to Framework] [Return to Mapping Matrix]*
You take appropriate steps to identify, assess and understand security risks to personal data and the systems that process this data.

GDPR emphasises a risk-based approach to data protection and the security of your processing systems and services. You must take steps to assess these risks and include appropriate organisational measures to make effective risk-based decisions based upon:

- the state of the art [of technology]
- cost of implementation
- the nature, scope, context and purpose of processing', and
- the severity and likelihood of the risk being realised.

Beyond this, where the processing is likely to result in a high risk to the rights and freedoms of individuals, you must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, you need to have a process in place to consult with the ICO before you start the processing.

A.3 Asset management *[Return to Framework] [Return to Mapping Matrix]*
You understand and catalogue the personal data you process and can describe the purpose for processing it. You also understand the risks posed to individuals of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data.

The personal data you process should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary.

A.4 Data processors and the supply chain *[Return to Framework] [Return to Mapping Matrix]*

You understand and manage security risks to your processing operations that may arise as a result of dependencies on third parties such as data processors. This includes ensuring that they employ appropriate security measures.
In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.

B) Protect personal data against cyber attack

You have proportionate security measures in place to protect against cyber attack which cover:

- the personal data you process and
- the systems that process such data

B.1 Service Protection Policies and Processes *[Return to Framework] [Return to Mapping Matrix]*

You should define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems involved in the processing of personal data.

You should also consider assessing your systems and implementing specific technical controls as laid out in appropriate frameworks (such as Cyber Essentials).

B.2 Identity & Access Control *[Return to Framework] [Return to Mapping Matrix]*

You understand, document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

You should appropriately authenticate and authorise users (or automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.

You should prevent users from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. You should appropriately constrain legitimate access ensure there is an appropriate audit trail.

You should have a robust password policy which avoids users having weak passwords, such as those trivially guessable. You should change all default passwords remove or suspend unused accounts.

B.3 Data Security *[Return to Framework] [Return to Mapping Matrix]*

You implement technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.

B.4 System Security *[Return to Framework] [Return to Mapping Matrix]*

You implement appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber attack.

Whilst the GDPR requires a risk-based approach, typical expected examples of security measures you could take include:

- Tracking and recording of all assets that process personal data, including end user devices and removable media.
- Minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity.

- Actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching) and taking other mitigating steps, where patches can't be applied.
- Managing end user devices (laptops and smartphones etc) so that you can apply organisational controls over software or applications that interact with or access personal data.
- Encrypting personal data at rest on devices (laptops, smartphones, and removable media) that are not subject to strong physical controls.
- Encrypting personal data when transmitted electronically.
- Ensuring that web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications such as the OWASP Top 10.
- Ensuring your processing environment remains secure throughout its lifecycle.

You also undertake regular testing to evaluate the effectiveness of your security measures, including virus and malware scanning, vulnerability scanning and penetration testing as appropriate. You record the results of any testing and remediating action plans.

Whatever security measures are put in place, whether these are your own or whether you use a third party service such as a cloud provider, you remain responsible both for the processing itself, and also in respect of any devices you operate.

B.5 Staff awareness & training *[Return to Framework] [Return to Mapping Matrix]*
You give staff appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data.
Staff should be provided with support to ensure that they do not inadvertently process personal data (eg by sending it to the incorrect recipient).

C) Detect security events

You can detect security events that affect the systems that process personal data and you monitor authorised user access to that data

C.1 Security monitoring *[Return to Framework] [Return to Mapping Matrix]*
You appropriately monitor the status of systems processing personal data and monitor user access to that data, including anomalous user activity.

You record user access to personal data. Where unexpected events or indications of a personal data breach are detected, you have processes in place to act upon those events as necessary in an appropriate timeframe.

D) Minimise the impact

You can:
- minimise the impact of a personal data breach
- restore your systems and services

- manage the incident appropriately
- learn lessons for the future

D.1 Response and recovery planning *[Return to Framework] [Return to Mapping Matrix]*
You have well-defined and tested incident management processes in place in case of personal data breaches. You have mitigation processes are in place that are designed to contain or limit the range of personal data that could be compromised following a personal data breach.

Where the loss of availability of personal data could cause harm, you have measures in place to ensure appropriate recovery. This should include maintaining (and securing) appropriate backups.

D.2 Improvements *[Return to Framework] [Return to Mapping Matrix]*
When a personal data breach occurs, you take steps to:

- understand the root cause
- report the breach to the Information Commissioner and, where appropriate, affected individuals
- Where appropriate (or required), report other relevant bodies (for example, other regulators, the NCSC and/or law enforcement) and
- take appropriate remediating action.

6. PSN (Target Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Source: Cabinet Office, PSN Code of Connection, Version 1.31, March 2017, 8pp.
https://www.gov.uk/government/publications/psn-code-of-connection-coco

1. Operational security

You will have appropriate policies, processes and procedures in place to ensure the operational security of your infrastructure.

a. Vulnerability management (patch management) *[Return to Framework] [Return to Mapping Matrix]*

You must ensure that any exploitable vulnerability is managed. You must have a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities. Your policy will specify specific patch application periods and a process for auditing compliance.

This typically will be of the order of: Critical vulnerabilities patched within 14 days, important vulnerabilities patched within 30 days and all others patched within 60 days.

Where you know that a vulnerability is being actively exploited then mitigating action (eg patch applied) should be taken immediately.

Where a patch is not deployed (or available) within the timescales above then there must be alternative mitigating action, such as disabling or reducing access to the vulnerable service.

b. Secure configuration *[Return to Framework] [Return to Mapping Matrix]*

You must ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. In particular, you will have ensured that applications, services, processes and ports not required are disabled by default. Default passwords will be changed, especially for any administrative functions.

You will keep configuration control of applications installed and technology that you use. All changes and new applications will be recorded and managed (including a formal approval and documentation process) by the enterprise.

You will ensure that devices, systems and services have the capability to detect, isolate and respond to malicious software.

c. Physical security *[Return to Framework] [Return to Mapping Matrix]*

You will ensure that appropriately secure accommodation and appropriate policies and practices governing its use are in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise.

d. Protective monitoring and intrusion detection *[Return to Framework] [Return to Mapping Matrix]*

You will collect and retain event data and undertake activities that will help you detect actual or potential security incidents. You must have a protective monitoring policy that describes the use cases you are aiming to detect, which can be used to define event data collection.

Your policy must include both detection of technical attacks as well as important abuses of business processes. These conditions do not describe any specific events to collect or incidents to detect. The requirement is that the business has thought about and documented its collection and analysis requirements and that this has led to your approach to protective monitoring and intrusion detection.

If you are using cloud services: Cloud Security Principle 5.3 *Protective Monitoring* should be factored into your overall monitoring strategy. Note that a cloud service will only provide monitoring with respect to the service provisioned. If you consume Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), you are responsible for monitoring of capability deployed onto the infrastructure. If you are consuming Software as a Service (SaaS), you should consider how you will be able to monitor for any potential abuse of business process or privilege.

End user devices: The capability associated with EUD Security Principle 11 *Event Collection for Enterprise Analysis* should form part of your overall monitoring strategy.

e. Security incident response ***[Return to Framework] [Return to Mapping Matrix]***

Even within well-secured and well-managed IT services, incidents will happen. You must be prepared for incidents so that when they do occur you act quickly to contain the incident, limit harm, ensure appropriate escalation and learn lessons for the future.

You must have a security incident management plan, which you should test periodically. This will include named responsible owners and pre-defined processes to respond to common forms of attack.

For incidents that impact on the PSN, you must report them to the PSN team and other entities (GovCertUK, for example) as required.

In the event of an incident, and where it is appropriate to do so, you will provide the PSN team with audit logs holding user activities, exceptions and information security events to assist in investigations.

End user devices: EUDs must form part of the incident response plan. Mobile devices especially will get lost or stolen and your response plans should include how to manage (eg remotely wipe) such devices. Refer to EUD Security Principle 12 *Incident Response*.

2. Authentication and access control ***[Return to Framework] [Return to Mapping Matrix]***

Accounts must be provisioned with privileges appropriate for the user need. Administrator (or other high privilege) accounts should only be provisioned to users who need those privileges. Administrators must not conduct 'normal' day-to-day business from their high privilege account. Privileges should be periodically reviewed and removed where no longer required.

Users must identify and authenticate to devices and services. For passwords, you must:

- ensure that ALL passwords are changed from defaults
- not allow password/account sharing
- ensure that high-privilege users (ie administrators) use different passwords for their high-privilege and low-privilege accounts
- combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication
- ensure that passwords are never stored as plain text, but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a salt before hashing passwords.

CESG has published best practice in its Password Guidance: Simplifying Your Approach document.

End user devices: Users will identify and authenticate to devices and services. Additionally only appropriately authorised devices will be provided with access to services. See EUD Security Principle 3 *Authentication*.

If you are using cloud services: Users, administrators and service providers must identify and authenticate to all services. See Principle 9, *Secure Consumer Management*, and Principle 10 *Identity and Access Control*.

3. Boundary protection and interfaces *[Return to Framework] [Return to Mapping Matrix]*

You will ensure that your network has appropriately configured boundary protection between your network/services and the internet or any other network.

Network traffic, services and content should be limited to that required to support your business need (for example, by setting effective firewall rule sets).

Services presented outside of the protected enterprise (online services for staff, mobile working etc), should be delivered from an appropriate architecture, with access to any core information or services constrained.

The architecture will include services to identify malware at the gateway. Where encryption prevents this, the organisation shall implement an equivalent level of protection at the end point.

If you are using cloud services: You may consider procurement of services which respond to different business needs and therefore have different security attributes. It is important that any interfaces between services are within scope.

Unmanaged devices: must not have access to the PSN. Where a corporate service contains information that has been sent over the PSN, you should have the data owner's permission before allowing unmanaged devices to access that data. Additionally, you must ensure that an unmanaged device:

- Is not able to use the corporate service to access the PSN in an unmediated fashion
- Accesses the corporate service through an appropriately secured connection
- For example, at the network layer via a VPN, or at the application layer via a protocol that implements TLS.
- Is authenticated prior to the information being accessed with a mechanism that does not solely rely on a username and password.

4. Protecting data at rest and in transit *[Return to Framework] [Return to Mapping Matrix]*

Data will be protected by default whilst at rest and in transit. Protection can take many forms ranging from physical protection (eg when hosted within a secure data centre) to encryption (eg when data is vulnerable at rest or in transit).

Where data is released via vulnerable channels (eg unprotected email, or removable media) the user must make an active decision and pay due regard to any applicable handling instructions for that information.

5. User and Administrator separation of data *[Return to Framework] [Return to Mapping Matrix]*

Appropriate separation should exist between multiple users of corporate IT services. There should be capability to mediate user access to data and limit access to sensitive data (such as personal data) to the minimal amount necessary to support the business. There should be separation (however it is achieved) between users who have access to information sent over the PSN and users with no access to that information.

If you are using cloud (or shared) services: Separation should exist between consumers of the service to prevent a malicious or compromised user from affecting another. See Principle 3 *Separation between consumers*. Users must be separately authenticated to more privileged access services (i.e. management interfaces). See Cloud Security Principle 9 *Secure Consumer Management*.

6. Users *[Return to Framework] [Return to Mapping Matrix]*

For users who have administrative privileges (for example, users who are able to reconfigure your network or system administrators) you should implement pre-employment checks which are aligned with the Baseline Personnel Security Standard (BPSS). Your users should be trained to understand their obligations with regards to system security, data handling, and acceptable use.

7. Testing your security *[Return to Framework] [Return to Mapping Matrix]*

You must implement regular IT Health Checks (ITHCs) to seek evidence that any security mechanisms put in place are ongoing and effective and identify any current vulnerability. ITHCs should normally be conducted annually, but the PSN team may specify a different frequency of ITHCs where appropriate.

It is important that issues identified in the ITHC (including systemic issues) are addressed. Critical and High risks should either be resolved immediately or else a viable plan for resolution must be agreed with the PSN team. Medium and Low risks may be accepted or subject to remedial action plans.

7. PCI (Target Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Source: PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard version 3.2.1, July 2018, 39pp.

Build and Maintain a Secure Network

In the past, theft of financial records required a criminal to physically enter an organization's business site. Now, many payment card transactions (such as debit in the U.S. and "chip and pin" in Europe) use PIN entry devices and computers connected by networks. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing cardholder data.

Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data *[Return to Framework] [Return to Mapping Matrix]*

1.1 Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify *all* connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and stipulate a review of configuration rule sets at least every six months.

1.2 Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.4 Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.

1.5 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters *[Return to Framework] [Return to Mapping Matrix]*

The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, merchants do not change default passwords or settings upon deployment. This is akin to leaving your store physically unlocked when you go home for the night. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task – if you have failed to change the defaults.

2.1 Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts *before* installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

2.3 Using strong cryptography, encrypt all non-console administrative access.

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

2.5 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A1: "Additional PCI DSS Requirements for Shared Hosting Providers.")

Protect Cardholder Data

Cardholder data refers to any information printed, processed, transmitted or stored in any form on a payment card. Entities accepting payment cards are expected to protect cardholder data and to prevent their unauthorized use – whether the data is printed or stored locally, or transmitted over a public network to a remote server or service provider.

Requirement 3: Protect stored cardholder data ***[Return to Framework] [Return to Mapping Matrix]***

Cardholder data should not be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable (see 3.4, and table below for guidelines).

3.1 Limit cardholder data storage and retention time to that which is required for business, legal, and/ or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See table below. Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt.

3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index

tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

3.5 Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.

3.6 Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

3.7 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorisation (even if encrypted).
[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Requirement 4: Encrypt transmission of cardholder data across open, public networks
[Return to Framework] [Return to Mapping Matrix]

Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view this data. Encryption is one technology that can be used to render transmitted data unreadable by any unauthorized person.

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission.

4.2 Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

4.3 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain a Vulnerability Management Program

Vulnerability management is the process of systematically and continuously finding weaknesses in an entity's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Requirement 5: Use and regularly update anti-virus software or programs *[Return to Framework] [Return to Mapping Matrix]*

Malicious software (a.k.a "malware") exploits system vulnerabilities after entering the network via users' e-mail and other online business activities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may supplement (but not replace) anti-virus software.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.

5.2 Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

5.4 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 6: Develop and maintain secure systems and applications *[Return to Framework] [Return to Mapping Matrix]*

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed.

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.

6.2 Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

6.3 Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party.

6.4 Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.

6.5 Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.

6.6 Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

6.7 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Implement Strong Access Control Measures

Access-controls allow merchants to permit or deny the use of physical or technical means to access PAN and other cardholder data. Access must be granted on a business need-to-know basis. Physical access controls entail the use of locks or other means to restrict access to computer media, paper-based records or system hardware. Logical access controls permit or deny use of payment devices, wireless networks, PCs and other computing devices, and also controls access to digital files containing cardholder data.

Requirement 7: Restrict access to cardholder data by business need-to-know ***[Return to Framework] [Return to Mapping Matrix]***

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

7.3 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 8: Assign a unique ID to each person with computer access ***[Return to Framework] [Return to Mapping Matrix]***

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative

capabilities and all accounts with access to stored cardholder data. Requirements do not apply to accounts used by consumers (e.g., cardholders).

8.1 Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components. Assign all users a unique user name before allowing them to access system components or cardholder data.

8.2 Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

8.3 Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity's network.

8.4 Develop, implement, and communicate authentication policies and procedures to all users.

8.5 Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.

8.6 Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.

8.7 All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).

8.8 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 9: Restrict physical access to cardholder data ***[Return to Framework] [Return to Mapping Matrix]***

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration – usually up to one day. "Media" is all paper and electronic media containing cardholder data.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.

9.3 Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled.

9.4 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.

9.5 Physically secure all media; store media back-ups in a secure location, preferably off site.

9.6 Maintain strict control over the internal or external distribution of any kind of media.

9.7 Maintain strict control over the storage and accessibility of media.

9.8 Destroy media when it is no longer needed for business or legal reasons.

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.

9.10 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Regularly Monitor and Test Networks

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities.

Requirement 10: Track and monitor all access to network resources and cardholder data
[Return to Framework] [Return to Mapping Matrix]

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 Implement audit trails to link all access to system components to each individual user.

10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or

administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.

10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.

10.4 Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.

10.5 Secure audit trails so they cannot be altered.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.

10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

10.8 Service providers must implement a process for timely detection and reporting of failures of critical security control systems.

10.9 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 11: Regularly test security systems and processes ***[Return to Framework] [Return to Mapping Matrix]***

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.

11.3 Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls.

11.4 Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data

environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

11.5 Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.

11.6 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an organization's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Requirement 12: Maintain a policy that addresses information security for all personnel ***[Return to Framework] [Return to Mapping Matrix]***

12.1 Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.

12.2 Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.

12.3 Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.

12.5 Assign to an individual or team information security responsibilities defined by 12.5 subsections.

12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

12.8 Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

12.9 Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of

the customer, or to the extent they could impact the security of the customer's cardholder data environment.

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.11 Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.

Compensating Controls for PCI DSS Requirements

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating controls. In order for a compensating control to be considered valid, it must be reviewed by an assessor. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a particular compensating control will not be effective in all environments.

8. NCSC – Cyber Assurance framework (CAF) (Advanced Progression Stage) *[Return to Framework] [Return to Mapping Matrix]*

Source: https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework

NCSC Guidance Objectives & Principles

The NCSC guidance has four objectives within which are 14 principles that define the security technical requirements, policies and procedures that must be in place to ensure compliance. The principles define a set of top-level outcomes that collectively describe the security requirements.

4 Objectives	14 Principles
Objective A. Managing security risk Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.	**A1. Governance** Putting in place the policies and processes which govern your organisations approach to the security of network and information systems. **A2. Risk Management** Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management. **A3. Asset management** Determining and understanding all systems and/or services required to maintain or support essential services. **A4. Supply chain** Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.
Objective B: Protecting against cyber attack Proportionate security measures are in place to protect essential services and systems from cyber attack.	**B1. Service protection policies and processes** Defining and communicating appropriate organisational policies and processes to secure systems and data that support the delivery of essential services. **B2. Identity and access control** Understanding, documenting and controlling access to essential services systems and functions. **B3. Data Security** Protecting stored or electronically transmitted data from actions that may cause disruption to essential services. **B4. System Security** Protecting critical network and information systems and technology from cyber attack. **B5. Resilient Networks & Systems** Building resilience against cyber attack. **B6. Staff Awareness & Training** Appropriately supporting staff to ensure they can support essential services' network and information system security.

Objective C: Detecting cyber security events Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.	**C1. Security Monitoring** Monitoring to detect potential security problems and track the effectiveness of existing security measures. **C2. Anomaly Detection** Detecting anomalous events in relevant network and information systems.
Objective D: Minimising the impact of cyber security incidents Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.	**D1. Response and Recovery Planning** Putting suitable incident management and mitigation processes in place. **D2. Improvements** Learning from incidents and implementing these lessons to make a more resilient service.

OBJECTIVE A

A1 Governance

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

Principle
The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A1.a Board direction *[Return to Framework] [Return to Mapping Matrix]*

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

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
The security of network and information systems related to the delivery of essential services is not discussed or reported on regularly at board-level. Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of networks and information systems supporting your essential services is not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies, or expect special accommodations to be made.	Your organisation's approach and policy relating to the security of networks and information systems supporting the delivery of essential services are set and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. Regular board discussions on the security of network and information systems supporting the delivery of your essential service take place, based on timely and accurate information and informed by expert guidance. There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level. Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential service.

A1.b Roles and responsibilities *[Return to Framework] [Return to Mapping Matrix]*

Your organisation has 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.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. Staff are assigned security responsibilities but without adequate authority or resources to fulfil them. Staff are unsure what their responsibilities are for the security of the essential service.	Necessary roles and responsibilities for the security of networks and information systems supporting your essential service have been identified. These are reviewed periodically to ensure they remain fit for purpose. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.

A1.c Decision-making *[Return to Framework] [Return to Mapping Matrix]*

You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of essential services are considered in the context of other organisational risks.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
What should be relatively straightforward risk decisions are constantly referred up the chain, or not made. Risks are resolved informally (or ignored) at a local level without a formal reporting mechanism when it is not appropriate. Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious". Organisational stovepipes result in risk decisions being made in isolation, for	Senior management have visibility of key risk decisions made throughout the organisation. Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential service, as set by senior management. Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.

example, engineering and IT don't talk to each other about risk.

Risk priorities are too vague to make meaningful distinctions between them, for example almost all risks are rated 'medium' or 'amber'.

Risk management decisions are periodically reviewed to ensure their continued relevance and validity.

A2 Risk Management

Principle
The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.

A2.a Risk management process [Return to Framework] [Return to Mapping Matrix]

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services, and communicating associated activities.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Risk assessments are not based on a clearly defined set of threat assumptions. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. Risk assessments for critical systems are a "one-off" activity (or not done at all). The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. There is no systematic process in place to ensure that identified security risks are managed effectively. Systems are assessed in isolation, without consideration of dependencies and interactions with other	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. You conduct risk assessments when significant events	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of disruption to your essential service, leading to a detailed understanding ofhow such disruption might arise as a consequence of possible attacker actions and the security properties of your networks and information systems. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service and your sector. Your risk assessments are informed by an understanding of the vulnerabilities in the

systems. (e.g. interactions between IT and OT environments.)

Security requirements and mitigation's are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential service.

Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.

potentially affect the essential service, such as replacing a system or a change in the cyber security threat.

You perform threat analysis and understand how generic threats apply to your organisation.

networks and information systems supporting your essential service.

The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security.

Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.

You conduct risk assessments when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat.

Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.

The effectiveness of your risk management process is reviewed periodically, and improvements made as required.

You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.

A2.b Assurance ***[Return to Framework] [Return to Mapping Matrix]***

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. Assurance is assumed because there have been no known problems to date.	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services. Your confidence in the security as it relates to your technology, people, and processes can be demonstrated to, and verified by, a third party. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

A3 Asset Management

Principle
Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A3.a Asset management *[Return to Framework] [Return to Mapping Matrix]*

Not Achieved	Achieved
At least one of the following statements is true	All the following statements are true
Inventories of assets relevant to the essential service are incomplete, non-existent, or inadequately detailed. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT). Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy. Knowledge critical to the management, operation, or recovery of essential services is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	All assets relevant to the secure operation of essential services are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. Dependencies on supporting infrastructure (eg. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the delivery of the essential service. You have assigned responsibility for managing the physical assets. Assets relevant to essential services are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

A4 Supply Chain

Principle

The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used. Regardless of your outsourcing model the OES remains responsible for the security of the service and therefore all requirements from NIS flow down.

A4.a Supply chain *[Return to Framework] [Return to Mapping Matrix]*

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for essential services are subcontracted and you have little or no visibility of the sub-contractors. Relevant contracts do not have security requirements. Suppliers have unrestricted or unmonitored access to critical systems, or access that bypasses your own security controls.	You understand the general risks suppliers may pose to your essential services. You know the extent of your supply chain for essential services, including sub-contractors. You engage with suppliers about security, and you set and communicate security requirements in contracts. You are aware of all third-party connections and have assurance that they meet your organisation's security requirements. Your approach to security incident management considers incidents that might arise in your supply chain.	You have a deeper understanding of your supply chain, including sub-contractors and the wider risks it faces. You take into account factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes. Your approach to supply chain risk management includes the risks to your essential services arising from supply chain subversion by capable and well-resourced attackers, if this is part of your threat model. You have confidence that information shared with suppliers that might be essential to the service is well protected. You can clearly express the security needs you place on suppliers in ways that are mutually understood, and are laid in contracts. There is a clear and documented shared-responsibility model.

All network connectivity and data object exchange is appropriately managed.

Where appropriate, you offer support to suppliers to resolve incidents

OBJECTIVE B

B1 Service Protection Policies and Processes

Proportionate security measures in place to protect essential services and systems from cyber attack.

Principle
The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.

B1.a Policy and process development *[Return to Framework] [Return to Mapping Matrix]*

You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Your service protection policies and processes are absent or incomplete. Service protection policies and processes are not applied universally or consistently. People often or routinely circumvent service protection policies and processes to achieve business objectives. Your organisation's security governance and risk management approach has no bearing on your service protection policies and processes. System security depends upon users' careful and consistent application of manual security processes. Service protection policies and processes have not been reviewed in response to major	Your service protection policies and processes document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is often treated as a separate issue. You review and update service protection policies and processes in response to major cyber security incidents.	You document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management. Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies. Where your service protection policies and processes place requirements on people, e.g. changes in behaviour or activity, this is practical and they can do what is expected.

changes (e.g. technology or regulatory framework), or within a suitable period. Service protection policies and processes are not readily available to staff, too detailed to remember, or too hard to understand.		You review and improve policies and processes at suitably regular intervals to ensure they remain relevant to threats, the way people and systems work, adapt to lessons learned and remain appropriate and effective. This is in addition to reviews following a major cyber security incident. Your systems are designed with 'guard rails', so that they remain secure even when user security policies and processes are not always followed.

B1.b Policy and process implementation *[Return to Framework] [Return to Mapping Matrix]*

You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
None or only part of your service protection policies and processes are enacted. You do not have an understanding of the impact of your service protection policies and processes on your security. Some or all staff are unaware of their responsibilities under your service protection policies and processes. You do not detect breaches of service protection policies and processes.	All your service protection policies and processes are enacted and you assess their correct application. Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness. All staff are aware of their responsibilities under your service protection policies and processes. All significant breaches of service protection policies and processes are investigated; less significant breaches are	All your service protection policies and processes are enacted. You regularly evaluate the correct application and security effectiveness of your service protection policies. Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness. Your service protection policies and processes are effectively and appropriately communicated across all levels of the organisation. All staff are aware of their responsibilities

	tracked and assessed for trends or aggregation as a larger breach.	under your service protection policies and processes. Suitable action is taken to correct significant single or aggregated breaches of service protection policies and processes.

B2 Identity and Access Control

Principle
The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

B2.a Identity verification, authentication and authorisation [Return to Framework] [Return to Mapping Matrix]

You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You cannot individually identify all users (whether by user identifier or secondary means) with access to networks or information systems on which your essential service depends. Unknown or unauthorised users or devices can connect to your networks or information systems. User access is not limited to the minimum necessary.	You individually identify all the users that are granted access to your networks or information systems (both logically and physically), whether by user identifier or alternative / secondary means. User access to essential service networks and information systems is limited to the minimum necessary. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for access to sensitive systems such as operational technology. You individually authenticate and authorise all remote access to all your networks and information systems that support your essential service. The list of users with access to essential service networks and systems is reviewed on a regular basis, e.g. annually.	Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical accessrequire this individual authentication and authorisation. User access to all your networks and information systems supporting the essential service is limited to the minimum necessary. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for all systems that operate or support your essential service. You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote access to all your networks and information systems that support your essential service.

		The list of individuals with access to all your networks and systems supporting the essential service is reviewed on a regular basis, e.g. annually. The list of users with access to essential service networks and systems is reviewed on a regular basis, e.g. every 6 months.

B2.b Device management ***[Return to Framework] [Return to Mapping Matrix]***

You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Users are allowed to connect to your essential service's networks using personal devices. Administrators are able to perform administrative functions from non-corporately managed devices (such as remote access from personal devices). You have not gained assurance in the security of any third-party devices or networks connected to your systems. Physically connecting to your network gives a device access to systems without further authentication.	Only corporately-owned and managed devices are allowed to access your essential service's networks and information systems. All administrative access occurs from dedicated management devices. You have sought to understand the security properties of third-party devices and networks before they are allowed to be connected to your systems. You have taken appropriate steps to mitigate any risks identified. The act of connecting to a network port or cable does not grant access to any systems. You are able to detect unknown devices being connected to your network, and investigate such incidents.	Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email. You either obtain independent or professional assurance of the security of third-party networks, or you only allow third-party devices or networks dedicated to supporting your systems to connect. You perform certificate based device identity management, and only allow known devices to access essential services. You perform regular scans to detect unknown devices and investigate any findings.

B2.c Privileged user management [Return to Framework] [Return to Mapping Matrix]

You closely manage privileged user access to networks and information systems supporting the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
The identities of the individuals with privileged access to your essential services (infrastructure, platforms, software, configuration, etc.) are not known or not managed It is not known whether all privileged users are strongly authenticated when accessing the system. Privileged access is granted from remote sessions without additional validation. The list of system administrators has not been reviewed recently, e.g. within the last 12 months. Privileged user access is granted on a system-wide basis (as opposed to by specific roles). System administrators use generic (shared or default name) accounts to administer servers and devices. Where there are “always on” terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted. User roles are not suitably logically segregated, e.g. users have a single user identifier for	Privileged access requires additional validation, but this does not use a strong form of authentication (e.g. two-factor, hardware authentication or additional real-time security monitoring). The identities of the individuals with privileged access to your essential service systems (infrastructure, platforms, software, configuration, etc) are known and managed. This includes third parties. Activity by privileged users is routinely reviewed and validated (e.g. at least annually.) Privileged users are only granted specific privileged permissions and roles which are essential to their business function.	Privileged user access to your essential service systems is carried out from dedicated separate accounts that are closely monitored and managed. The issuing of temporary, time-bound rights for privileged user access and external third-party support access is either in place or you are migrating to an access control solution that supports this functionality. Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process. All privileged user access to your networks and information systems requires strong authentication, such as two-factor, hardware authentication, or additional real-time security monitoring. All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.

routine business activities and privileged or segregated roles.

B2.d IDAC management and maintenance *[Return to Framework] [Return to Mapping Matrix]*

You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Greater rights are granted to users than necessary. User rights are granted without validation of their identity and requirement for access. User rights are not reviewed when they move jobs. User rights remain active when people leave your organisation.	You have a robust procedure to verify each user and issue minimum required access rights. You regularly review access rights and those no longer needed are revoked. Your joiners, leavers and movers process ensures that user permissions are reviewed both when people change roles and at regular intervals. All access is logged and monitored.	Your procedure to verify each user and issue the minimum required access rights is robust and regularly audited. User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually. All user access is logged and monitored. You regularly review access logs and correlate this data with other access records and expected activity. Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated.

B3 Data Security

Principle
Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.

B3.a Understanding data [Return to Framework] [Return to Mapping Matrix]

You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing, or accessing data important to the delivery of essential services.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You have incomplete knowledge of what data is used by and produced in the delivery of the essential service. You have not identified the important data on which your essential service relies. You have not identified who has access to data important to the delivery of the essential service. You have not clearly articulated the impact of data compromise or inaccessibility.	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker. You have identified and catalogued who has access to the data important to the delivery of the essential service. You periodically review location, transmission, quantity and quality of data important to the delivery of the essential service. You have identified all mobile devices and media that hold data important to the delivery of the essential service. You understand and document the impact on your essential service of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data.	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker. You have identified and catalogued who has access to the data important to the delivery of the essential service. You maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service. You take steps to remove or minimise unnecessary copies or unneeded historic data. You have identified all mobile devices and media that may hold data important to the delivery of the essential service. You maintain a current understanding of the data links used to transmit data that is important to your essential service.

	You occasionally validate these documented impact statements.	You understand the context, limitations and dependencies of your important data. You understand and document the impact on your essential service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data. You validate these documented impact statements regularly, at least annually..

B3.b Data in transit *[Return to Framework] [Return to Mapping Matrix]*

You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You do not know what all your data links are, or which carry data important to the delivery of the essential service. Data important to the delivery of the essential service travels without technical protection over untrusted or openly accessible carriers. Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.	You have identified and suitably protected all the data links that carry data important to the delivery of the essential service. You apply appropriate technical means (e.g. cryptography) to protect data that travels over an untrusted carrier, but you have limited or no confidence in the robustness of the protection applied.	You have identified and suitably protected all the data links that carry data important to the delivery of the essential service. You apply appropriate physical or technical means to protect data that travels over an untrusted carrier, with justified confidence in the robustness of the protection applied. Suitable alternative transmission paths are available where there is a risk of impact on the delivery of the essential service due to resource limitation (e.g. transmission equipment or service failure, or important data being blocked or jammed).

B3.c Stored data [Return to Framework] [Return to Mapping Matrix]

You have protected stored data important to the delivery of the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All of the following statements are true
You have no, or limited, knowledge of where data important to the delivery of the essential service is stored. You have not protected vulnerable stored data important to the delivery of the essential service in a suitable way. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	All copies of data important to the delivery of your essential service are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used, you apply suitable techical and procedural means, but you have limited or no confidence in the robustness of the protection applied. You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used you apply suitable techical and procedural means, and you have justified confidence in the robustness of the protection applied. You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies. Necessary historic or archive data is suitably secured in storage.

B3.d Mobile data [Return to Framework] [Return to Mapping Matrix]

You have protected data important to the delivery of the essential service on mobile devices.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You don't know which mobile devices may hold data important to the delivery of the essential service. You allow data important to the delivery of the essential service to be stored on devices not managed by your organisation, or to at least equivalent standard. Data on mobile devices is not technically secured, or only some is secured.	You know which mobile devices hold data important to the delivery of the essential service. Data important to the delivery of the essential service is only stored on mobile devices with at least equivalent security standard to your organisation. Data on mobile devices is technically secured.	Mobile devices that hold data that is important to the delivery of the essential service are catalogued are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place. Your organisation can remotely wipe all mobile devices holding data important to the delivery of essential service. You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.

B3.e Media / equipment sanitisation ***[Return to Framework] [Return to Mapping Matrix]***

You appropriately sanitise data from the service, media or equipment.

Not Achieved	Achieved
At least one of the following statements is true	All of the following statements are true
Some or all devices, equipment or removable media that hold data important to the delivery of the essential service are disposed of without sanitisation of that data.	You catalogue and track all devices that contain data important to the delivery of the essential service (whether a specific storage device or one with integral storage). All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal.

B4 System Security

Principle
Network and information systems and technology critical for the delivery of essential services are protected from cyber attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

B4.a Secure by design [Return to Framework] [Return to Mapping Matrix]

You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Systems essential to the operation of the essential service are not appropriately segregated from other systems. Internet access is available from operational systems. Data flows between the essential service's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic. Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential service.	You employ appropriate expertise to design network and information systems. You design strong boundary defences where your networks and information systems interface with other organisations or the world at large. You design simple data flows between your networks and information systems and any external interface to enable effective monitoring. You design to make network and information system recovery simple. All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	You employ appropriate expertise to design network and information systems. Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone. The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring. The networks and information systems supporting your essential service are designed to be easy to recover. Content-based attacks are mitigated for all inputs to operational systems that effect the essential service (e.g. via transformation and inspection).

B4.b Secure configuration [Return to Framework] [Return to Mapping Matrix]

You securely configure the network and information systems that support the delivery of essential services.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You haven't identified the assets that need to be carefully configured to maintain the security of the essential service. Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential service. Configuration details are not recorded or lack enough information to be able to rebuild the system or device. The recording of security changes or adjustments that effect your essential service is lacking or inconsistent.	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential service. Secure platform and device builds are used across the estate. Consistent, secure and minimal system and device configurations are applied across the same types of environment. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential service are approved and documented. You verify software before installation is permitted.	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice)the assets that need to be carefully configured to maintain the security of the essential service. All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. You regularly review and validate that your network and information systems have the expected, secured settings and configuration. Only permitted software can be installed and standard users cannot change settings that would impact security or business operation. If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.

B4.c Secure management ***[Return to Framework] [Return to Mapping Matrix]***

You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Essential service networks and systems are administered or maintained using non-dedicated devices. You do not have good or current technical documentation of your networks and information systems.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices. Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained. You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.

B4.d. Vulnerability management *[Return to Framework] [Return to Mapping Matrix]*

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements below are true	All the following statements are true
You do not understand the exposure of your essential service to publicly-known vulnerabilities. You do not mitigate externally-exposed vulnerabilities promptly.	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities. Announced vulnerabilities for all software packages, network equipment and	You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities. Announced vulnerabilities for all software packages, network equipment and operating

There are no means to check data or software imports for malware.

You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential service.

You have not suitably mitigated systems or software that is no longer supported. These systems may still be running, but not in operational use.

You are not pursuing replacement for unsupported systems or software.

operating systems used to support your essential service are tracked, prioritised and externally-exposed vulnerabilities are mitigated (eg by patching) promptly.

Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.

You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology.

You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service.

systems used to support your essential service are tracked, prioritised and mitigated (eg by patching) promptly.

You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service and verify this understanding with third-party testing.

You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service.

B5 Resilient Networks and Systems

Principle
The organisation builds resilience against cyber attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.

B5.a Resilience preparation [Return to Framework] [Return to Mapping Matrix]

You are prepared to restore your essential service following disruption.

Not Achieved	Partially Achieved	Achieved
Any of the following statements are true	All of the following statements are true	All of the following statements are true
You have limited understanding of all the elements that are required to deliver the essential service. You have not completed business continuity and/or disaster recovery plans for your essential service's networks, information systems and their dependencies. You have not fully assessed the practical implementation of your disaster recovery plans.	You know all networks, information systems and underlying technologies that are necessary to deliver the essential service and understand their interdependencies. You know the order in which systems need to be restored to efficiently and effectively restore the essential service.	You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g. manual failover, table-top exercises, or red-teaming. You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

B5.b Design for resilience [Return to Framework] [Return to Mapping Matrix]

You design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Operational networks and systems are not appropriately segregated. Internet services, such as browsing and email, are	Operational systems for your essential service are logically separated from your business systems, e.g. they reside on the same network as the rest of the organisation, but within a DMZ.	Your essential service's operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate

accessible from essential service operational systems. You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential service.	Internet access is not available from operational systems. Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	network and system infrastructure with independent user administration. Internet services are not accessible from operational systems. You have identified and mitigated all resource limitations, i.e. bandwidth limitations. You have identified and mitigated any geographical constraints or weaknesses. For example, systems that your essential service depends upon are duplicated to another location, important network connectivity has alternative physical paths and service providers. You review and update dependencies, resource and geographical limitation assessments and update mitigations when required.

B5.c Backups ***[Return to Framework] [Return to Mapping Matrix]***

You hold accessible and secured current backups of data and information needed to recover.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Backup coverage is incomplete in coverage and would be inadequate to restore your essential service. Backups are not frequent enough for your essential service to be restored within a suitable timeframe.	You have appropriately secured backups (including data, configuration information, software, equipment, processes and key roles or knowledge). These backups will be accessible to recover from an extreme event. You routinely test backups to ensure that the backup	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event. Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.

	process functions correctly and the backups are usable.	Backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.

B6 Staff Awareness and Training

Principle
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 delivery of essential services.

B6.a Cyber security culture [Return to Framework] [Return to Mapping Matrix]

You develop and pursue a positive cyber security culture.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the essential service. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting issues may get them into trouble. Your organisation's approach to cyber security doesn't reflect the way staff work to deliver the essential service. It is perceived by staff as being incompatible with the ability of the organisation to deliver the essential service.	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution they make to the essential service's cyber security. All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations. People in your organisation are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored. Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure. Your management is seen to be committed to and actively involved in cyber security. Your organisation communicates openly about cyber security, with any concern being taken seriously. People across your organisation participate in cyber security activities and improvements, building joint

		ownership and bringing knowledge of their area of expertise.

B6.b Cyber security training *[Return to Framework] [Return to Mapping Matrix]*

The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
There are teams who operate and support your essential service that lack any cyber security training. Cyber security training is restricted to specific roles in your organisation. Cyber security training records for your organisation are lacking or incomplete.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively. Cyber security information is easily available.	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths. Each individuals' cyber security training is tracked and refreshed at suitable intervals. You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective. You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

OBJECTIVE C

C1 Security Monitoring

Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

Principle
The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

C1.a Monitoring coverage *[Return to Framework] [Return to Mapping Matrix]*

The data sources that you include in your monitoring allow for timely identification of security events which might affect the delivery of your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Data relating to the security and operation of your essential services is not collected. You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential services, such as know malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed). You are not able to audit the activities of users in relation to your essential service. You do not capture any traffic crossing your network boundary including as a minimum IP connections.	Data relating to the security and operation of some areas of your essential services is collected. You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures. Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour. You monitor traffic crossing your network boundary (including IP address connections as a minimum).	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect your essential service. (e.g. presence of malware, malicious emails, user policy violations). Your monitoring data provides enough detail to reliably detect security incidents that could affect your essential service. You easily detect the presence or absence of IoCs on your essential services, such as know malicious command and control signatures. You have timely access to the data you need to use with IoCs. Extensive monitoring of user activity in relation to essential services enables you to detect

		policy violations and an agreed list of suspicious or undesirable behaviour. You have extensive monitoring coverage that includes host-based monitoring and network gateways. All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

C1.b Securing logs *[Return to Framework] [Return to Mapping Matrix]*

Logging data should be held securely and read access to it should be granted only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
It is possible for logging data to be edited or deleted. There is no controlled list of who can view and query logging information. There is no monitoring of the access to logging data. There is no policy for accessing logging data. Logging is not synchronised, using an accurate common time source.	Only certain staff can view logging data for investigations. Privileged users can view logging information. There is some monitoring of access to logging data. (e.g. copying, deleting or modification, or even viewing.).	The integrity of logging data is protected, or any modification is detected and attributed. The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it. Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered. Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways. Access to logging data is limited to those with business need and no others.

		All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user. Legitimate reasons for accessing logging data are given in use policies.

C1.c Generating alerts *[Return to Framework] [Return to Mapping Matrix]*

Evidence of potential security incidents contained in your monitoring data is reliably identified and alerted upon.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All the following are true	All of the following are true
Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers. Logs are distributed across devices with no easy way to access them other than manual login or physical action. The resolution of alerts to a network asset or system is not performed. Security alerts relating to essential services are not prioritised. Logs are reviewed infrequently.	Alerts from third party security software are investigated, and action taken. Some logging datasets can be easily queried with search tools to aid investigations. The resolution of alerts to a network asset or system is performed regularly. Security alerts relating to some essential services are prioritised. Logs are reviewed at regular intervals.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts. A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts. Alerts can be easily resolved to network assets using knowledge of networks and systems. Security alerts relating to all essential services are prioritised and this information is used to support incident management. Logs are reviewed almost continuously, in real time. Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

C1.d Identifying security incidents *[Return to Framework] [Return to Mapping Matrix]*

You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.

Not Achieved	Partially Achieved	Achieved
At least one of the following is true	All of the following are true	All of the following are true
Your organisation has no sources of threat intelligence. You do not apply intelligence updates (e.g. AV signature updates, other threat signatures or IoCs) in a timely way, after receiving them. You do not receive signature updates for all protective technologies (such as AV and IDS) or other software in use. You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	Your organisation uses some threat intelligence services, but you don't choose providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, antivirus providers, specialist threat intel firms). You apply some updates, signatures and IoCs in a timely way. You receive signature updates for all your signature-based protective technologies (e.g. AV, IDS). You are cognisant of how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong antivirus providers, sector and community-based infoshare). You are able to apply new signatures and IoCs within a reasonable (risk-based) time of receiving them. You receive signature updates for all your protective technologies (e.g. AV, IDS). You can track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).

C1.e Monitoring tools and skills *[Return to Framework] [Return to Mapping Matrix]*

Monitoring staff skills, tools and roles, including any that are out-sourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protect.

Not Achieved	Partially Achieved	Achieved

At least one of the following is true	All of the following are true	All of the following are true
There are no staff who perform a monitoring function. Monitoring staff do not have the correct specialist skills. Monitoring staff are not capable of reporting against governance requirements Monitoring staff lack the skills to successfully perform any part of the defined workflow. Monitoring tools are only able to make use of a fraction of logging data being collected. Monitoring tools cannot be configured to make use of new logging streams, as they come online. Monitoring staff have a lack of awareness of the essential services the organisation provides, what assets relate to those services and hence the importance of the logging data and security events.	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers). Monitoring staff are capable of following most of the required workflows. Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types. Your monitoring tools can work with most logging data, with some configuration. Monitoring staff are aware of some essential services and can manage alerts relating to them.	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance. Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process. Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external. Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data. Your monitoring tools make use of all logging data collected to pinpoint activity within an incident. Monitoring staff and tools drive and shape new log data collection and can make wide use of it. Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.

C2 Proactive Security Event Discovery

Principle
The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature based security prevent/detect solutions, or when it is not possible to use signature based detection, for some reason.

C2.a System abnormalities for attack detection [Return to Framework] [Return to Mapping Matrix]

You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

Not Achieved	Achieved
At least one of the following is true	All of the following are true
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity. You have no established understanding of what abnormalities to look for that might signify malicious activities.	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity. (e.g. You fully understand which systems should and should not communicate and when.) System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity. The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services. The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

C2.b Proactive attack discovery [Return to Framework] [Return to Mapping Matrix]

You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.

Not Achieved	Achieved
At least one of the following is true	All of the following are true
You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting your

essential service, generating alerts based on the results of such searches.

You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.

OBJECTIVE D

D1 Response and Recovery Planning

Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including, the restoration of those services, where necessary.

Principle
There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response plan [Return to Framework] [Return to Mapping Matrix]

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential service and covers a range of incident scenarios.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
Your incident response plan is not documented. Your incident response plan does not include your organisation's identified essential service. Your incident response plan is not well understood by relevant staff.	Your response plan covers your essential services. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only. Your response plan is understood by all staff who are involved with your organisation's response function Your response plan is documented and shared with all relevant stakeholders	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service. Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen Your incident response plan is documented and integrated with wider organisational business and supply chain response plans. Your incident response plan is communicated and understood by the business areas involved

	with the supply or maintenance of your essential services.

D1.b Response and recovery capability *[Return to Framework] [Return to Mapping Matrix]*

You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.

Not Achieved	Achieved
At least one of the following statements is true	All of the following statements are true
Inadequate arrangements have been made to make the right resources available to implement your response plan. Your response team members are not equipped to take good response decisions and put them into effect. Inadequate back-up mechanisms exist to allow the continued delivery of your essential service during an incident.	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available. You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available. Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out. Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable. Arrangements exist augment your organisation's incident response capabilities with external support (eg. specialist providers of cyber incident response capability).

D1.c Testing and exercising *[Return to Framework] [Return to Mapping Matrix]*

Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.

Not Achieved	Achieved
At least one of the following statements is true	All of the following statements are true

Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.

Incident response exercises are not routinely carried out, or are carried out in an ad-hoc way.

Outputs from exercises are not fed into the organisation's lessons learned process.

Exercises do not test all parts of the response cycle.

Exercise scenarios are based on incidents experienced by your and other organisations, or are composed using experience or threat intelligence.

Exercise scenarios are documented, regularly reviewed, and validated.

Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.

Exercises test all parts of your response cycle relating to particular services or scenarios (e.g. restoration of normal service levels).

D2 Lessons Learned

Principle
When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.

D2.a Incident root cause analysis [Return to Framework] [Return to Mapping Matrix]

Your organisation identifies the root causes of incidents you experience, wherever possible.

Not Achieved	Achieved
At least one of the following statements is true	All of the following statements are true
You are not usually able to resolve incidents to a root cause. You do not have a formal process for investigating causes.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident. Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software. All relevant incident data is made available to the analysis team to perform root cause analysis.

D2.b Using incidents to drive improvements [Return to Framework] [Return to Mapping Matrix]

Your organisation uses lessons learned from incidents to improve your security measures.

Not Achieved	Achieved
At least one of the following statements is true	All of the following statements are true
Following incidents, lessons learned are not captured or are limited in scope. Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems. You use lessons learned to improve security measures, including updating and retesting response plans when necessary.

Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.

Analysis is fed to senior management and incorporated into risk management and continuous improvement.

This document has been produced by the Scottish Government Cyber Resilience Unit to accompany the Public Sector Action Plan on Cyber Resilience.

Please send all comments, questions or suggested amendments to cyberresilience@gov.scot