Space

Guidance on Cyber Security Strategies for applicants and licensees.

CAP2535

Published by the Civil Aviation Authority, 2023

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published April 2023
First edition

Enquiries regarding the content of this publication should be addressed to: **Cyber@caa.co.uk**

The latest version of this document is available in electronic format at: www.caa.co.uk

Contents

Introduction

As the regulator, the CAA is responsible for licencing all spaceflight activities within the UK. We aim to have an appropriate and proportionate response to licensing spaceflight, and this is reflected within the CAA's approach to granting licences. We wish to promote a scalable method by which organisations of all sizes are capable of implementing a cyber security strategy and to promote cyber security best practices. A Cyber Security Strategy is required for all licence types under the Space Industry Regulations 2021. Further requirements are set out in the Regulator's Licensing Rules (RLRs), known as CAP2221.

This document is intended to serve as guidance material for applicants drafting cyber security strategies when applying for a licence under the Space Industry Act. The guidance supplied will allow an applicant to have a clearer understanding of the required information when it comes to submitting a Cyber Security Strategy as part of their application to the CAA. It will cover activities that the applicant should utilise to develop the basis of a Cyber Security Strategy. Use of this document in development of a strategy does not indicate that a licence will be issued. It sets out what the CAA expects to see in an acceptable Cyber Security Strategy and describes a method for demonstrating compliance with that legal requirement. This guidance material intends to further the information provided within CAP2217, Guidance on security matters for applicants and licensees.

For definitions of licence types please see: https://www.caa.co.uk/space/the-role-of-the-caa/types-of-licence/

Cyber Security Strategy Regulation

Spaceflight Cyber Security Strategy - Regulation 185 of the Regulations

The Space Industry Regulations 2021 (the Regulations) detail the requirements for those intending to conduct spaceflight activities within the UK. Part 11 of the Regulations covers security.

Under Regulation 185, an applicant must draw up and maintain a cyber security strategy for the network and information systems used in relation to spaceflight operations for which it is responsible.

This regulation applies directly to **all licensees** under the Space Industry Act.

A Cyber Security Strategy is a plan of actions intended to improve the resilience and security of IT infrastructures and services.

The strategy must:

- be kept up to date,
- be reviewed—
  - no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and
  - upon any upgrades made to the systems,
- be sent to the regulator following a review
- be proportionate and appropriate for the type of systems operated,
- comply with international obligations of the United Kingdom and be consistent with such obligations,
- be based on a security risk assessment which—
  - has been carried out by the licensee, and
  - is reviewed no more than 12 months after the date on which the licence was granted and, subsequently, at intervals not exceeding 12 months, and upon any upgrades made to the systems,
- ensure the security of the systems managed by employees or agents of the licensee,
- ensure that the systems are protected from—
  - unauthorised access or interference,
  - other unlawful occurrences, and
  - cyber threat, and
- ensure that the licensee’s suppliers and their supply chain specify in their security protocols how they will achieve the cyber security requirements set out in the strategy.

A draft cyber security strategy (and the cyber security risk assessment it is based upon) should be submitted as part of the licence application.

Definitions and Key Terms

Under the Regulations, there are several definitions and key terms specific to cyber security:

Cyber Threat anything capable of compromising the security of, or causing harm to, information systems and internet connected devices including hardware, software and associated infrastructure, the data on them and the services they provide, primarily by cyber means;

Jamming a deliberate blocking or interference with a wireless communication system by transmission of radio signals that disrupt information flow in wireless data networks by decreasing the signal to noise ratio.

Spoofing a technique used to gain unauthorised access to computers whereby an intruder sends messages to a computer indicating that the message is coming from a trusted source.

Unauthorised Access or Interference in connection with the security of systems relating to spaceflight operations includes hacking, jamming, or spoofing of services or other recognised cyber threats;

Unlawful Occurrences includes theft of data

Network and Information Systems In connection with spaceflight operations means –

(a) an electronic communications network within the meaning of section 32 of the Communications Act 2003(55),

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data,

(c) digital data stored, processed, retrieved, or transmitted by elements covered under subparagraphs (a) or (b) for the purposes of their operation, use, protection, and maintenance, or

(d) a flight safety system

Notifiable Incident Any event of a type that has been determined by the regulator and the licensee as having an adverse effect on the security of the network and information systems used in relation to spaceflight operations and that may have a significant impact on future essential services provided by the licensee

Security In connection with the network and information systems means the ability of the network and information systems to resist any action that compromises the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or the related services offered by, or accessible via, the systems.

Mission Critical A process, system, or asset that performs a function that is essential to the licenced activity. The loss of which would cause significant impact to or failure of the licenced activity

In addition to these defined key terms, and for further clarity, the CAA hereby provides definitions to the following terms in Regulations 185 and 186:

Cyber Security	Refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.
Upgrades	Any change in mission critical process, or system; addition or change of hardware, software or process that changes the fundamental functionality of the network and information systems, or mission operation.
Security Risk Assessment	A cyber security risk assessment that has been carried out either internally or externally, encompassing all aspects of an organisation’s IT, assets, physical security, and mission operation to identify the likelihood and severity of a risk, the mitigations relating to this risk. Resulting in an overall risk score before and after mitigations. Where risks have a potential safety impact, this should be clearly documented.

Cyber Security Strategy Guidance

To provide clarity of expectations to applicants, and to ensure consistency in licence application assessment, the CAA have developed the following process for applicants to use to assist in the development of their cyber security strategy. This process is a method by which an acceptable Cyber Security Strategy can be created. This process comprises of 3 activities which should form the basis of an applicant's cyber security strategy:

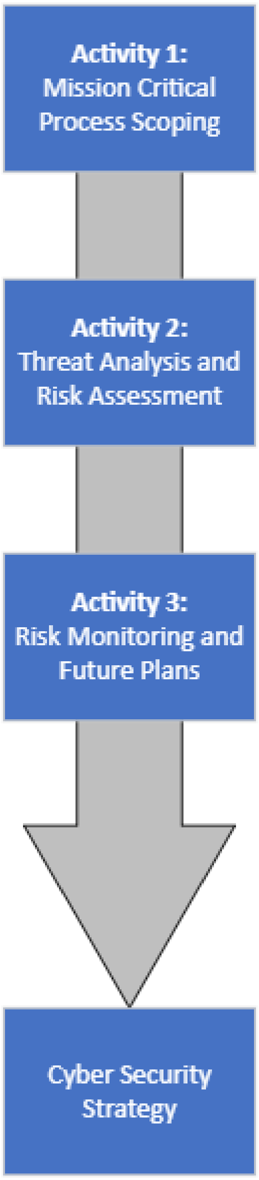
Activity 1:
Mission Critical Process Scoping
Activity 2:
Threat Analysis and Risk Assessment
Activity 3:
Risk Monitoring and Future Plans
Cyber Security Strategy

Figure 1: Cyber Security Strategy Development Process

The processes outlined in this guidance should provide an applicant with the relevant mission critical cyber security risks to be included in their wider cyber security strategy. The wider strategy should include further information regarding an applicant's network and information security, as well as broader organisational processes and policies. Annex A provides information on these wider considerations that should be included within the draft cyber security strategy.

Activity 1 – Mission Critical Process Scoping

Activity 1 requires an applicant to perform a mission critical process scoping activity that is intended to assist in the identification and documentation of cyber related mission critical processes, and the associated assets and services which support these processes, that would impact safety. This activity will aid in applying comprehensive, appropriate, and proportionate cyber security measures. Appropriate personnel should be included in the scoping activity to ensure complete coverage of spaceflight systems and processes, for example, Subject Matter Experts within Safety, Security, and Engineering.

When identifying the scope of mission critical processes, the CAA expect the applicant to make an informed and competent consideration of reasonable and expected impacts. The CAA does not expect the applicant to consider implausible scenarios or highly complex chains of events or failures — a reasonable worst-case scenario should be used.

The applicant is ultimately responsible for their own risks and the identification and validation of their mission critical process scope. Whereby an applicant is utilising third party systems to perform part of their mission function, this should be clearly documented within the strategy. To ensure that the scope is accurate and includes mission critical processes that would reasonably be considered in scope, the applicant should be able to demonstrate that a logical method was followed and included all stakeholders deemed relevant by the organisation (e.g., workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc). The applicant should ensure that all identified processes, systems, or assets identified are sufficiently detailed to perform the other activities within this guidance.

Applicants should include data flow diagrams within their strategies, for example, relating to the applicant’s network and information systems, and showing the traffic between an applicant’s systems and spacecraft.

Examples of mission critical processes that could form a part of an applicant’s scoping activity includes remote connections to a satellite, network and information systems used by the business, the software development process, or mission rules verification and validation.

Some examples of information that should be included in a cyber security strategy include the command & control software utilised, network diagrams, how traffic is protected across the TT&C network, how commands to the spacecraft are sent, authenticated, and received, at what stages the data is encrypted, and the standards of encryption utilised. Wider mission critical processes that are vital for the overall business, but do not result in a safety risk (such as emails), should be excluded from this activity.

Where applicants have achieved relevant cyber security certifications, these should be provided, and the evidence may be re-submitted to the CAA as part of the application process, provided it is still in date.

Activity 2 – Threat Analysis and Risk Assessment

This activity requires an applicant to undertake a risk assessment which has been informed by threat analysis. Both the assessment and analysis should have a focus on both the applicant's cyber security policies and plans, as well as the mission critical process and operational environment.

2a - Threat Analysis

Activity 2a requires an applicant to have conducted a cyber threat analysis for the applicant's mission critical processes and assets. Applicants should demonstrate how they maintain an up-to-date threat understanding that is relevant to their organisation and spaceflight activities through systematic and evidencable approaches for analysing threats such as STRIDE, TVRA, and more.

The threat landscape constantly evolves, with the number of new threats growing exponentially. It is therefore imperative that applicants have an approach to evaluate the threat at appropriate intervals or as an ongoing task. Applicants may wish to use external organisations to perform threat analysis if they do not possess the knowledge to perform this internally.

The National Cyber Security Centre – the UK's Technical Authority for cyber - provide weekly threat reports as well as sector specific threat reports. The CAA encourages applicants to engage with the NCSC to better understand the threat and to receive any other cyber security support. The latest threat reports can be found on the NCSC's website.

2b - Risk Assessment

The threat analysis above, alongside Activity 1 will provide the fundamental information an applicant will require to undertake a thorough cyber risk assessment. The identified cyber risks should be documented in a stand-alone document or located within the Cyber Security Strategy.

The risk assessment should classify the risk in likelihood and severity or impact levels and should have a named individual assigned as an owner, to each individual risk.

It's highly likely that there will be crossovers between safety risks and security risks. It is important that an applicant clearly documents the relationships between these risks. Where these risks are already identified in a safety case, the link to the cyber event should be clearly identified in the cyber security risk assessment.

Risks should be calculated to understand historic, current, and residual risks. Applicants should also consider the controls that are in place for each risk, and these should be documented in the risk assessment. Where there is a control, a residual risk column should be included to indicate how the implemented control reduces the risk scores. If a control is currently not in place but is to be implemented before commencement of spaceflight activities, this should be noted as a control with a clear implementation date. Controls beyond this timeframe should be included as part of Activity 3.

Where an applicant is considering using third-party technologies, software, or services, consideration around the security impact and associated risks of such suppliers ought to be taken into account throughout the creation of a cyber security strategy and clearly documented within the risk assessment. Further guidance around supply chain security is available from NCSC.

2c - Risk Response

Based on an applicant's risk assessment, each risk should have 1 of 4 risk responses:

- Treat
- Tolerate
- Transfer
- Terminate

Should an applicant have risk responses of terminate, tolerate, or transfer the applicant should provide reasoning as to why that particular risk response has been selected. Should risk transfer be used as a risk response, the applicant should detail who the risk is being transferred to and why, alongside any formal agreements that detail this risk transfer. The applicant should provide evidence that the risk has been accepted by the transferee for this risk response. Where treat is used as a response, the appropriate evidence should be documented in the controls column of the risk assessment.

Risk response should be clearly documented in its own column within the risk assessment. If an applicant has an incident response and recovery plan, this should be included in the documentation sent to the CAA during the application phase. Where risks are transferred, or not directly owned by the applicant, a statement of assurance from the third party organisation should be sought. Applicants should also ensure that the cyber security practices of third-party organisations utilised for spaceflight operations meet the applicant's minimum criteria.

Activity 3 – Risk Monitoring and Future Plans

The CAA accept that a risk assessment is for a specific snapshot in time. With this, an applicant is required to monitor risks to determine the risk response effectiveness. Also, applicants should conduct risk identification exercises periodically to identify and respond to evolving or new risks. As part of this activity, an applicant should document how they will manage and monitor the risks in the form of a risk management plan, which should be included within the Cyber Security Strategy.

The CAA recognises that multiple factors will affect risk responses, such as the implementation of mitigations. All risks should have – at minimum - an associated plan, should the risk response require it, regardless of organisational or spaceflight maturity. This should be documented within the strategy in the form of a future plan, as well as indicating future plans in the risk assessment where appropriate.

Working with the regulator

Sharing of Information Securely with the CAA

Any sensitive documentation including a Cyber Security Strategy with associated documentation should not be submitted via the Spaceflight online portal. Each application will be assessed on a case-by-case basis, and sensitive information submitted to the CAA will be stored securely. Please contact commercialspaceflight@caa.co.uk to arrange how your information will be delivered to the Cyber Security Certification Team.

Licence Application Assessment Phase

The Cyber Security Certification Team welcomes early engagement from an applicant to provide further steer on an applicant's cyber security strategy content and answer any questions an applicant may have.

During the assessment phase, the Cyber Security Certification Team shall keep open and regular communications with the applicant. Should the Cyber Security Certification Team receive inconsistent, insufficient, or missing information, this will be communicated at the earliest opportunity to allow the applicant to clarify or rectify this.

At this phase, we will utilise the submitted cyber security strategy to complete an assessment of an applicant's cyber security, with consideration placed on the wider safety risks posed by the spaceflight activities. It will also be used to satisfy the requirements indicated by Part 11, Chapter 3 of the Regulations. The submitted strategy will also be shared with other stakeholders involved in the licensing process, such as the United Kingdom Space Agency (UKSA), who are responsible for performing the national security assessment during the licensing process.

As with many legislative requirements, an audit of the applicant's cyber security strategy and associated processes shall be conducted. The duration and depth of the audit will be determined by the CAA, based upon the organisational complexity, spaceflight activities and associated risks. Expected duration, scope and dates will be discussed with applicants during the assessment phase.

After Licencing

Once a licence has been granted, the licensee will be expected to comply with any conditions set out in the licence, as well as comply with the Regulations. The continued periodicity by which a licensee is required to undergo cyber security oversight activities and regulatory audit is decided by the CAA in conjunction with the Regulations and the Oversight and Monitoring plan set out by the CAA. The factors used to determine frequency of audits could include:

- Any cyber security conditions on a licence
- Cyber security risk
- A licensee's complexity status
- Cyber security regulatory requirements

- Notifications of cyber security changes
- Cyber security maturity and future plans
- Cyber security incidents where relevant

The CAA will also consider the longevity of a licence such as those for spaceflight activities that are not enduring and last for a specific period of time.

Notification of a Cyber Security Change

Under the Regulations, a licensee is required to keep their cyber security strategy up to date. It also must be reviewed, no more than 12 months after licence grant date and subsequently at intervals not exceeding 12 months. A licensee's cyber security strategy must be sent to the CAA following each review.

A licensee should also communicate with the CAA, should there be a change to their:

- Mission Critical Process Scope
- Mission Critical Suppliers
- Cyber security controls which mitigate a safety risk, or
- A significant change to risk management or implementation plan

A Notification of Cyber Security Change should not include any sensitive information or attachments (i.e. network diagrams). The CAA accept no liability for sensitive information which is shared by your organisation non-securely or without prior agreement.

The notification email should include a high-level description of the nature of the change (i.e. change to mission critical suppliers, scope change) and the date the change was effective from. The CAA will then contact the licensee to discuss the change further and make appropriate arrangements for secure information sharing if required.

Please direct all cyber security change notifications to cyber@caa.co.uk.

Note: This is in addition to any change notification required under existing safety or security regulations.

Further Information

The CAA have the appetite to develop a Space Profile for the Cyber Assessment Framework (CAF), in collaboration with the National Cyber Security Centre (NCSC) and industry. Whilst in development, the CAA has published the CAF for Aviation which applicants and licensees may use as a guideline in the meantime. Annex B contains an excerpt from the CAF relating to good practice.

A Security Management System (SeMS) provides a formalised, risk-driven framework for integrating security into the daily operations and culture of an organisation. A Security Management System enables an organisation to identify and address security risks, threats, gaps, and weaknesses in a consistent and proactive way. In short, a SeMS provides the necessary organisational structure, accountabilities, policies, and procedures to ensure effective security oversight. Though a Security Management System is not a mandatory requirement to obtain a licence, it is likely to prove helpful to an applicant in ensuring they meet the requirements set out in the Space Industry Act 2018 and related security regulations. The CAA has issued guidance on how to implement Security Management Systems in CAPs 1223 and 1273.

Whilst the information in this document is intended to serve as guidance for cyber security strategies, licensees may wish to utilise other available frameworks or resources to further their strategy. Some of the available frameworks and resources include:

CQEST is a self-assessment questionnaire developed by the Bank of England in support of their CBEST scheme. The answers to this questionnaire provide a valuable snapshot of a firm's cyber resiliency capability and highlight any areas for development.

Introduction to Cybersecurity for Commercial Satellite Operations - NISTIR8270
Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control - NISTIR8401
Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models - ISA/IEC 62443 1-1
Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program - ISA/IEC 62443 2-1
Guide for Conducting Risk Assessments - NIST SP800-30
Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy - NIST SP800-37
Managing Information Security Risk: Organization, Mission, and Information System View - NIST SP800-39
Guide to Operational Technology (OT) Security - NIST SP800-82
CyBOK Risk Management & Governance Knowledge Area
Information technology — Security techniques — Information security risk management - ISO/IEC 27005:2022
Information security management - ISO/IEC 27001
Risk Management - ISO/IEC 31000

Annex A: Example Information

Applicants should look to include details relating, but not limited to, the information below within their strategies:

Orbital

- All systems related to mission operation including but not limited to:
  - Ground Stations Equipment (GSE)
  - Assets connected to the network
  - Connections from/to the spacecraft and ground systems
  - Software/Hardware on the spacecraft
  - Satellite/Mission Control Centres
  - Software to control spacecraft, hardware utilised etc
- The data that is to be transported to/from the spacecraft and how this is done
  - Encryption
  - Movement operations
- Network Security within the organisation
- Information Security Management within the organisation
- Cyber Security Culture/Policies within the organisation
  - Access control, physical security, etc
- Satellite state during Launch

Launch

- All systems related to mission operation including but not limited to:
  - Ground Stations Equipment (GSE)
  - Operational Technology
  - Industrial Control Systems/Fuelling Systems (where a cyber-attack can lead to a safety concern)
  - Mission Control Centres (MCC)
  - Assets connected to the network
  - Outbound Connections
  - Physical Security of IT
  - Launch Vehicle Systems
  - Connections
    - Launch Vehicle (LV) to GSE
    - GSE TO MCC
    - LV to MCC
  - (Autonomous) Flight Safety System
  - Safety Critical Telemetry
  - Links between payloads and LV if applicable
- Network security within the organisation
- Information Security Management within the organisation
- Cyber Security Culture/Policies within the organisation
  - Access control, physical security, etc

Spaceport

- All systems related to mission operation including but not limited to:
    - Ground Systems Equipment (GSE)
    - Operational Technology
    - Mission Control Centres (MCC)
    - Lighting
    - Monitoring
    - Connections
        - MCC to LVs
        - MCC to Range
    - Range Control, if provided by Spaceport
    - For Horizontal Spaceports
        - Runway Lighting
        - Air Traffic Control
        - Monitoring
        - Access Control
- Cyber Security Culture/Policies within the organisation
    - Access control, physical security, etc
- Information Security Management within the organisation

Range

- All systems related to mission operation including but not limited to:
    - Mission Control Centres (MCC)
        - Co-ordination Services
        - Notification Services
    - Boundary Control Systems
    - Monitoring Systems
    - Weather systems
    - Safety critical telemetry
    - Operational Technology
- Cyber Security Policies and Culture within the organisation
    - Access control, physical security, etc
- Network security
- Information Security Management within the organisation

Procurement Only

- All systems related to mission operation within the following phases:
    - Satellite Creation
    - Storage
    - Transportation
    - Integration with LV
    - Launch phase
- If procuring the launch of a UK based satellite, an assurance statement that proves an understanding of the cyber security risks relating to safety, and that these risks are at a negligible/ALARP level will suffice.

Annex B: Good Practice

The CAA recommend that regardless of the level of our regulatory involvement, space organisations should proactively apply appropriate and proportionate cyber security good practice into their operations. The represents the building blocks for cyber security and resilience, the relevant profiles set by the CAA will inform whether Contributing Outcomes should be "Achieved", "Partially Achieved" or in some cases "Not Achieved" for each aviation organisation.

The below extract of the CAF for Aviation provides an overview of good practice principles, and references associated standards and guidance. For further information and guidance on good practices please visit the NCSC website.

Objective	Principle	Informative References	Contributing Outcomes	Description
Managing security risk	**Governance:** The organisation has appropriate management policies and processes in place to govern its approach to the security of critical systems.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-82 Eurocae ED-204	Board Direction	You have effective organisational security management led at board level and articulated clearly in corresponding policies.
			Roles and Responsibilities	Your organisation has established roles and responsibilities for the security of critical systems at all levels, with clear and well-understood channels for communicating and escalating risks.
			Decision Making	You have senior-level accountability for the security of critical systems, and delegate decision-making authority appropriately and effectively. Risks to critical systems are considered in the context of other organisational risks.
	Risk management: The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	ISO/IEC 27005:2018 ISO/IEC 27001:2017 ISO/IEC 3100:2018 ISA/IEC 62443 1-1 ISA/IEC 62443 2-1 NIST SP800-30 NIST SP800-37 NIST SP800-39 NIST SP800-82 Eurocae ED202A, ED203A, ED204 & ED205 CyBOK Risk Management & Governance Knowledge Area	Risk Management Process	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems. This includes an overall organisational approach to risk management.
			Assurance	You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to critical systems.

	Asset management: Everything required to deliver, maintain, or support critical systems is determined and understood. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).	ISO/IEC 55001:2019 ISO/IEC27002: 2013 ISA 62443-1-1 NIST SP800-82 NIST SP800-53	Asset Management	Principle applies.
	Supply chain: The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	ISO/IEC 27002:2013 ISO/IEC 27036-2 ISO/IEC 27036-3 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-37 Eurocae ED201	Supply Chain	Principle applies.
Protecting against cyber-attack	**Function protection policies and processes:** The organisation defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing critical systems and data that support operation of essential functions.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISO/IEC 22301:2019 ISA/IEC 62443-1-1 NIST SP800-53 NIST SP800-82	Policy and Process Development	You have developed and continue to improve a set of cyber security and resilience policies and processes that manage and mitigate the risk of adverse impact on the critical system.
			Policy and Process Implementation	You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.
	Identity and access control: The organisation understands, documents, and	ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP800-53 NIST SP800-82	Identity verification, authentication, and authorisation	You robustly verify, authenticate, and authorise access to the critical systems.

	manages access to critical systems supporting the operation of essential functions. Users (or automated functions) that can access critical data or critical systems are appropriately verified, authenticated, and authorised.	Eurocae ED204 CyBOK Authentication, Authorisation and Accountability Knowledge Base	Device Management	You fully know and have trust in the devices that are used to access your critical systems and data.
			Privileged User Management	You closely manage privileged user access to critical systems supporting the essential functions.
			Identity and Access Management (IdAM)	You assure good management and maintenance of identity and access control for your critical systems.
	Data security: Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on critical systems. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of critical systems. It also covers information that would assist an attacker, such as design details of critical systems.	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP800-53 NIST SP800-82 Eurocae ED204 & ED205	Understanding Data	You have a good understanding of data important to the operation of the critical systems, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the critical systems. This also applies to third parties storing or accessing data important to the operation of critical systems.
			Data in Transit	You have protected the transit of data important to the operation of the critical systems. This includes the transfer of data to third parties.
			Stored Data	You have protected stored data important to the operation of the critical system.
			Mobile Data	You have protected data important to the operation of the critical system on mobile devices.
			Media / Equipment Sanitisation	You appropriately sanitise media and equipment holding data critical to the operation of the critical systems.
	System security: Critical systems and technology critical for the operation of essential functions are protected from cyber-attack. An organisational understanding of risk to the critical system	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP800-53 NIST SP800-82 Eurocae ED202A, ED203A, ED204 & ED205	Secure by Design	You design security into the critical systems. You minimise their attack surface and ensure that the operation of the critical system should not be impacted by the exploitation of any single vulnerability.
			Secure Configuration	You securely configure critical systems.

	informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.		Secure Management	You manage your organisation's critical systems to enable and maintain security.
			Vulnerability Management	You manage known vulnerabilities in your critical systems to prevent adverse.
	Resilient Networks and Systems: The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation, and management of critical systems.	ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-1-1 NIST SP800-53 NIST SP800-82	Resilience Preparation	You are prepared to restore the operation of your critical system following adverse impact.
			Design for Resilience	You design critical systems to be resilient to cyber security incidents. Critical systems are appropriately segregated, and resource limitations are mitigated.
			Backups	You hold accessible and secured current backups of data and information needed to recover operation of your critical system.
	Staff Awareness and Training: Staff have appropriate awareness, knowledge, and skills to carry out their organisational roles effectively in relation to the security of critical systems supporting the operation of essential functions.	NCSC 10 Steps: User Education and Awareness ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-82	Cyber Security Culture	You develop and pursue a positive cyber security culture.
			Cyber Security Training	The people who support the operation of your critical system are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.
Detecting cyber security events	**Security monitoring:** The organisation monitors the security status of the networks and systems supporting the operation of critical systems in order to detect potential security problems and to track the ongoing effectiveness of	NCSC Introduction to logging for security purposes NCSC 10 Steps: Monitoring CREST – Cyber Security Monitoring Guide ISO/IEC 27002:2019 ISO/IEC 27002:2013 ISO/IEC 27035:1-3 ISA/IEC 62443-2-1	Monitoring Coverage	The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your critical system.
			Securing Logs	You hold log data securely and grant read access only to accounts with business need. No employee should ever need to modify or delete log data within an agreed retention period, after which it should be deleted.

	protective security measures.	NIST SP 800-53 NIST SP800-82 NIST SP800-94	Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.
			Identifying Security Incidents	You contextualise alerts with knowledge of the threat and your systems to identify those security incidents that require some form of response.
			Monitoring Tools and Skills	Monitoring staff skills, tools, and roles, including any that are outsourced, 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 critical systems they need to protect.
	Proactive security event discovery: The organisation detects, within critical systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).	ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-2-1 NIST SP800-53	System Abnormalities for Attack Detection	You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.
			Proactive Attack Discovery	You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.
Minimising the impact of cyber security incidents	**Response and recovery planning:** There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit	NCSC 10 Steps: Incident Management ISO/IEC 27035 (all) ISO/IEC 22301:2019 ISO/IEC 27002:2013 NIST SP800-61 NIST SP800-53 NIST SP800-82 Eurocae ED204	Response Plan	You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential functions and covers a range of incident scenarios.
			Response and Recovery Capability	You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your critical systems. During an incident, you have access to timely information on which to base your response decisions.

	the impact of compromise are also in place.		Testing & Exercising	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.
	Lessons learned: 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.	NCSC 10 Steps: Incident Management ENISA Good Practice for Incident Management Guide ISO/IEC 27035:2-3 ISO/IEC 22301:2019 ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP800-61 NIST SP800-53	Incident Root Cause Analysis	When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.
			Using Incidents to Drive Improvements	Your organisation uses lessons learned from incidents to improve your security measures.