UK
Civil Aviation
Authority

Guidance on Cyber Security Strategies for applicants and licensees.

CAP 2535

Published by the Civil Aviation Authority, 2024

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

First published April 2023
Second edition November 2024

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/CAP2535

Contents

Introduction

As the regulator, the CAA is responsible for licensing all spaceflight activities within the UK. We enable space activities which are safe for the public, in line with UK national security and interests and meet the UK's international obligations. 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).

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 as well as the process for how monitoring activities relating to cyber security will take place.

For applicants, 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 granted. 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 licensees, this document serves as information on how the CAA will conduct any cyber security related monitoring activities after a licence has been granted. Please refer to licences and permissions for definitions of licence types under the Space Industry Act.

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.

Cyber Security Regulation

Spaceflight Cyber Security - 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 (R185), 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 licensed activity. The loss of which would cause significant impact to or failure of the licensed activity

In addition to these defined key terms, and for further clarity, the CAA has provided the following definitions to 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.

Prior to Application

Cyber Security Strategy Guidance

To make clear what we expect, and to ensure consistency in licence application assessment, we have developed a process for applicants to help in the development of their cyber security strategy. This process is a method by which an acceptable cyber security strategy can be created, and comprises 3 activities which should form the basis of your cyber security strategy:

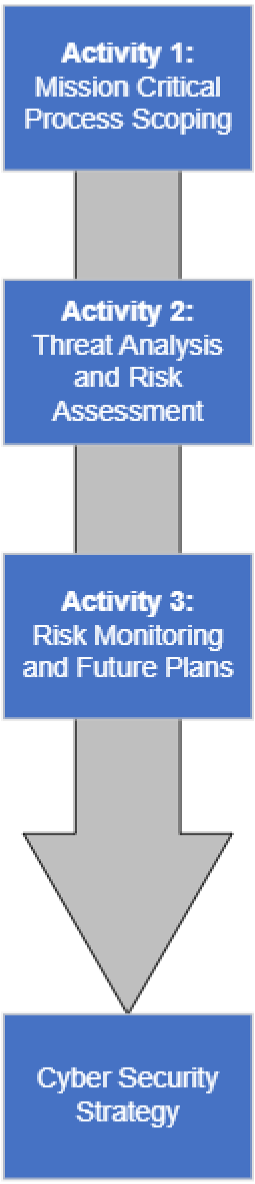
Activity 1:
Mission Critical Process Scoping
Activity 2:
Threat Analysis and Risk Assessment
Activity 3:
Risk Monitoring and Future Plans
Cyber Security Strategy

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.

The Cyber Security 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. Please email Cyber@caa.co.uk with any questions.

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 application. 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.

During Application

Once your cyber security strategy and accompanying risk assessment have been produced, they must be submitted to the CAA. After submission we will perform an initial check of the documentation to make sure that we have all the required information to begin a full assessment of the material.

During full assessment we will look to identify cyber security controls in place to protect your spaceflight activity, and to determine if any safety risks that could arise from a cyber security incident have been mitigated to a level of As Low As Reasonably Practicable (ALARP). This forms part of the wider safety test for Orbital, Spaceport, and Launch, and forms a part of the technical test for range applications. 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. 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.

Post Licence Grant

Once an applicant has been granted a licence, they will be subject to a monitoring regime. As part of this, licensees will be audited by the Cyber Security team to confirm compliance with the Regulations. The following sections will set out details surrounding the resubmission of your cyber security strategy, how the monitoring assessment will take place, and the objectives licensees will be assessed against.

Cyber Security Monitoring Process

The CAA has developed 35 objectives with which licensees will be assessed against. These have stemmed from analysis of international standards, and the needs of the regulations. Licensees are encouraged to utilise whichever best practice works for them and their operations, and evidence that has been used to achieve compliance with other standards can also be used to meet the needs of the monitoring assessment.

As part of the review, the CAA will utilise evidence supplied at application stage to complete as much of the assessment as possible, before communicating any information requests to licensees. 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.

This assessment should not be viewed by licensees as certification that their business is fully protected against a cyber incident. Should the licensee have concerns about their cyber security maturity, they should seek an external, independent audit of their business by an accredited industry body.

The CAA also wishes to make clear to licensees that adherence to the CAA's regulatory framework does not imply compliance with the referenced international standards.

Section 1 – Tiering

The first stage of the assessment will be tiering licensees. These tiers will be based on a variety of areas, such as mission operation, flight heritage, and the licence type. The resulting tier will determine the level of cyber security compliance that is deemed acceptable for that licensee. Where a licensee has multiple licences, the CAA will use the highest resulting tier from the selection of licences.

Section 2 – The Framework

The 35 objectives developed by the CAA have resulted from a comprehensive analysis of ISO27001, NIST Cyber Security Framework V2.0 (CSF), and NCSC's Cyber Assessment Framework (CAF). Alongside this analysis, we have also utilised the requirements of the Regulations to ensure that meeting the objectives ensures regulatory compliance. As mentioned in the introduction, licensees are not expected to use the objectives as a way to determine the overall health of their cyber security, rather they are for the CAA to determine regulatory compliance. The objectives are detailed below in Section 2a, and any links to Regulation and the above standards have been identified in Annex B.

2a – Objectives

Governance

- G1 - Demonstrate effective implementation, enforcement, and documentation of relevant and up-to-date cyber security governance controls.
- G2 - Cyber security (including supply chain) informs organisational governance and risk management, ensuring effective procedures are in place and used to address risks across the board.
- G3 - Cyber Security training is implemented across the organisation.

Identity Management

- IM1 - Appropriate level of access control applied through organisation and spaceflight operations, and users have correct roles assigned to limit access (including physical environment), and reviewed and revoked as required.
- IM2 - Roles and responsibilities are defined, and all employees assigned roles and understand their roles as well as the access that comes with it.

Incident Detection and Response

- IDR1 - Incident Response (IR) plan created, tested, implemented, and continuously improved (created, implemented, executed, lessons learnt).
- IDR2 - Recovery Plan implemented as part of IR plan (created, tested, implemented, executed, lessons learnt).
- IDR3 - Logs are in place to enable monitoring and analysing of events - these logs must then be stored securely and never modified or deleted unless post retention period.
- IDR4 - Effective monitoring and detection controls are in place to identify all types of attacks across the entire network.
- IDR5 - Alerts are generated when a potential security event takes place and appropriate actions take place where required.

Risk Identification and Management

- RIM1 - Vulnerabilities affecting critical assets are identified, documented, and managed in accordance with a vulnerability management plan.
- RIM2 - Risk tolerance is clearly defined, documented, and communicated.
- RIM3 - Tailored threat intelligence from multiple sources is used to support risk management and inform decision making.
- RIM4 - Use organisationally defined risk management framework/methodology to determine overall risk.
- RIM5 - Both internal and external threats relating to spaceflight operations are identified and documented.
- RIM6 - Impacts to spaceflight operation and safety have been identified and documented.
- RIM7 - All risks have been assigned an inherent and post mitigation value.
- RIM8 - Risk identified and mitigated with an action timeline and prioritisation assigned.

Secure Architecture

- SA1 - Configuration management processes are documented and implemented effectively.
- SA2 - Appropriate protections are in place across corporate and operational networks, and any connections to internal operational networks are verified and authenticated.
- SA3 - Corporate and operational networks are effectively segregated.

- SA4 - Implement user authentication techniques, such as Multi-Factor Authentication (MFA), across operational networks to secure user logins effectively.
- SA5 - Implement device authentication techniques across operational networks to ensure secure authentication between devices, enhancing overall network security.
- SA6 - Operational data is protected at all times (protected at rest, in-transit etc).
- SA7 - Testing environment separate from operational networks.
- SA8 - Backups in place that are maintained and tested.
- SA9 - Design processes include checks to ensure no malicious input.
- SA10 - Regularly conduct vulnerability scans, adjusting the frequency based on the criticality of systems and the associated risk.
- SA11 - Create, implement, and adhere to secure configuration and management procedures, ensuring that security requirements are identified and integrated into the design and lifecycle of systems and services.

Spaceflight Ops

- SFO1 - Assets (including software, applications, and networks) utilised for spaceflight operations are inventoried and managed throughout their lifecycle.
- SFO2 - Organisational networks are mapped and data flows between them are understood.
- SFO3 - Dependencies and critical functions relating to the delivery of essential spaceflight services have been identified, categorised, and their impact to operation incorporated into risk management.
- SFO4 - Adequate capacity to ensure spaceflight operations are uninterrupted (resiliency).

Supply Chain Management

- SCM1 - Supply chain and risks derived from third-party partners are identified and listed.
- SCM2 – Supply chain management processes including supplier assurance activities are in place to ensure a suitable level of cyber security is maintained.

Section 3 – The Assessment

The assessment will begin immediately after a licence is granted. Documentation that has been submitted throughout the course of the application process will initially be used to provide evidence against the objectives. Should there be any points for follow up, the licensee will receive an Information Requirement detailing any points that require clarification or further documentation. This initial part of the monitoring assessment will take approximately one month to perform, and the licensee will have 28 days from receiving the Information Requirement to supply the requested evidence.

After further evidence has been received, we will then utilise the new information to finalise the assessment by updating any areas where there has been extra evidence and filling any gaps. Each objective will receive a score based on the evidence that you have submitted. These scores are based on good practice requirements from industry standards. Whereby an objective is not suitable for your operation, we will award the objective a score of N/A which will remove the objective from the score that determines your final outcome. Licensees will then receive a final Conclusion Report, which will contain one of 4 outcomes and a breakdown of the score by objective groups. These outcomes have been detailed below.

Overall, we expect this assessment to take 3 months post licence. This monitoring assessment does not affect the requirement set out by R185 whereby you must submit an updated cyber security strategy within 12 months of licence date.

Section 4 – Outcomes

After the assessment has been completed, licensees will be given a report containing a final overall score, a breakdown of the group scores, and any areas for improvement. The scores that a licensee can receive are as follows:

Fully Compliant – This score denotes that you have exceeded the expected cyber security requirements of the CAA with regards to the Space Industry Regulations 2021. Whilst the final result determines the overall compliance of your approach to cyber security in relation to regulatory requirements, specific groups may have room for further improvement - the specific group scores may be found below in the Detailed Assessment section of this report.

Compliant – Improvement Desirable – This score denotes that you are meeting the expected cyber security requirements of the CAA with regards to the Space Industry Regulations 2021. Whilst the final result determines the overall compliance of your approach to cyber security in relation to regulatory requirements, there is room for further improvement. The specific group scores may be found below in the Detailed Assessment section of this report. Further comments around specific objectives and suggested actions can be found in the Areas for Improvement section of this report.

Shortfall (Minor/Major) - This score denotes that you are not meeting the expected cyber security requirements of the CAA with regards to the Space Industry Regulations 2021. This could mean you are in breach of the regulations and enforcement action may be taken if contraventions identified in this report are not remedied in a suitable timescale. Specific groups requiring attention can be found in the Detailed Assessment section of the conclusion report, and further comments around specific objectives and suggested actions can be found in the Areas for Improvement section. You as the licensee will be responsible for the creation of a corrective action plan and associated timelines for completion utilising the identified areas for improvement. This should be shared with the CAA once complete.

Alongside one of these outcomes, will be a breakdown by group. Each group will have a percentage and an outcome next to it to help you identify areas in which you should focus on to improve your compliance with the Regulations. These percentages align with the outcomes above and are as follows:

Major Shortfall – Below 30%

Minor Shortfall – Above 30% and Below 50%

Compliant (Improvement Desirable) – Above 50% and Below 75%

Fully Compliant – Above 75%

Section 5 – Corrective Action Plans and Timelines

This section only applies if you receive a score of Minor or Major Shortfall. As explained above, the score dictates that you are not meeting the requirements of the Regulations when it comes to cyber security. You must analyse the areas for improvement as noted on the Conclusion Report and devise a corrective action plan to remedy any deficiencies. The corrective action plan must include what you as the licensee plan to do, along with timelines that indicate when the control will be implemented. The CAA appreciates that actions may take a significant amount of time to implement. Where this is the case, the CAA will, at its discretion, determine whether or not the length of time is suitable.

Once the corrective action plan has been agreed, the CAA will determine a suitable schedule for meetings to be held to ensure progress is being made on the actions identified. When resubmitting a cyber security strategy as per R185 of the Regulations, the corrective action plan should be included with any appropriate updates around the actions.

Section 6 – Enforcement

If you are in contravention of the Regulations, enforcement action may be taken. The CAA’s Spaceflight Enforcement Policy lays out how this will occur.

Notification of a Cyber Security Change

Once your strategy has been created, sent to the CAA, and you have been granted a licence – the strategy will remain valid for 12 months. This in turn means that further applications within a 12 month period from the date of your first licence will not require a cyber security strategy to be sent each time, as long as there have been no changes to your cyber security since the original application. An updated risk assessment must still be submitted as part of your application, detailing any new or specific risks to that mission.

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,
- Systems (that introduces new risk),
- Cyber security controls which mitigate a safety risk, or
- A significant change to risk management or implementation plan

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. The CAA accepts no liability for sensitive information which is shared by your organisation non-securely.

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.

Reporting of a Notifiable Incident

The CAA determines a Notifiable Incident (as per R186(2) of the Regulations) as any event involving a cyber incident that has the potential to compromise or has compromised the security of the network and information systems utilised by the licensee.

In the above definition, “security” in connection with network and information systems has the meaning given in R186(2) of the Regulations;

“Network and Information Systems” has the meaning given in R185(3) of the Regulations.

Examples of potential cyber threats that lead to incidents can be found in R185(3) of the Regulations.

As per R186(1) of the Regulations, a licensee must report any notifiable incident to the regulator within 72 hours of the time at which you become aware of it. If you experience or suspect a cyber incident, please report it to the CAA using the online Occurrence Reporting Form as soon as possible, identifying it as a cyber incident.

If you have experienced any suspicious activity and are unsure as to whether or not it would be classed as a notifiable incident, please follow the above guidance and submit an occurrence report with as much information as possible.

You should also report any suspected cyber incident to the National Cyber Security Centre (NCSC) as soon as possible, using their reporting service.

Reporting incidents and suspicious activity helps improve the security of the space sector by ensuring that any relevant cyber security information is reported, collected, stored, protected, and analysed. It is not to attribute blame or liability but supports continued learning to ensure up to date threat analysis and improved cyber security.

Further Information

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.

Security and Privacy Controls for Information Systems and Organisations NIST 800-53 Rev 5

NIST Cybersecurity Framework – NIST CSF 2.0

National Cyber Security Centre’s Cyber Assessment Framework – NCSC CAF

Information Security, cybersecurity and privacy protections – Information security management systems – Requirements – ISO27001

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: Objectives and Informative References

This annex describes the links between the objectives and the Space Industry Regulations (SIR), and also shows the closest comparable objectives in other international standards (ISO27001, NIST CSF 2.0 (which incorporates references to NIST800-53 Rev 5)), alongside NCSC's CAF. Where applicable, a double star (**) implies relevance to all objectives within a group in the relevant standard.

Governance

- G1:
  - SIR: Regulation 185 (1), (2)
  - NIST CSF V2.0: GV.PO-(01, 02), ID.IM-(02, 04), PR.DS-01, PR.PS-01
  - ISO27001: A5.1, A5.10, A5.19, A5.20, A5.30, A5.36, A5.37
  - NCSC CAF: B1.(a, b), B3.(c, d)
- G2:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: GV.OC-02, GV.RM-(01, 04, 06), GV.RR-(02, 03), GV.SC-02
  - ISO27001: A5.4
  - NCSC CAF: A1, A2, A4
- G3:
  - SIR: Regulation 188 (3, 4b) and 190(2)
  - NIST CSF V2.0: GV.RM-05, GV.RR-04, PR.AT-**
  - ISO27001: A5.34, A6.3
  - NCSC CAF: B6.b

Identity Management

- IM1:
  - SIR: Regulation 185 (2, h, i)
  - NIST CSF V2.0: GV.RR-04, ID.AM-08, PR.AA-(01, 02, 03, 05, 06), PR.IR-01
  - ISO27001: A6.1, A6.5, A8.3
  - NCSC CAF: A1.b, B2.(a, c, d)
- IM2:
  - SIR: Regulation 185 (2, h, i)
  - NIST CSF V2.0: PR.AT-02, GV.RR-02
  - ISO27001: A5.2, A5.3
  - NCSC CAF: A1.b

Incident Detection and Response

- IDR1:
  - SIR: Regulation 185 (2, g)
  - NIST CSF V2.0: RC.CO-(03, 04), RC.RP-(01, 02, 03, 04, 05, 06)
  - ISO27001: A5.24, A5.25, A5.26
  - NCSC CAF: B1.(a, b), D1.(b, c), D2.(a, b)
- IDR2:
  - SIR: Regulation 185 (2, g)
  - NIST CSF V2.0: RC.**.**
  - ISO27001: A5.26, A5.27
  - NCSC CAF: D1.(a, b, c)
- IDR3:
  - SIR: Regulation 185 (2, g)
  - NIST CSF V2.0: PR.PS-04, DE.CM-01
  - ISO27001: A5.28, A8.15, A8.16
  - NCSC CAF: C2.(a, b)

- IDR4:
  - SIR: Regulation 185 (2, g)
  - NIST CSF V2.0: ID.IM-(02, 03), DE.AE-(02 ,03 ,04, 06, 08), RS.**-**
  - ISO27001: A6.8
  - NCSC CAF: B1.(a, b), C1.(a, b, c, d, e), C2.(a, b), D1.(a, b, c), D2.b
- IDR5:
  - SIR: Regulation 185 (2, g)
  - NIST CSF V2.0: DE.CM-**, DE.AE-(06, 08), RS.MA-**
  - ISO27001: A5.26
  - NCSC CAF: C1.(c, d)

Risk Identification and Management

- RIM1:
  - SIR: Regulation 185 (2, f, i)
  - NIST CSF V2.0: ID.RA-(01, 04)
  - ISO27001: A8.8
  - NCSC CAF: A2.a, B4.d
- RIM2:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: GV.RM-(02, 04), ID.RA-06
  - ISO27001: A5.1
  - NCSC CAF: A2.a
- RIM3:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: ID.RA-02
  - ISO27001: A5.7
  - NCSC CAF: C2.b
- RIM4:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: ID.RA-05
  - ISO27001: A5.1
  - NCSC CAF: A2.a

- RIM5:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: ID.RA-04
  - ISO27001: A5.7
  - NCSC CAF: A1.c, B4.d
- RIM6:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: ID.RA-(03, 04, 05)
  - ISO27001: A5.36, A5.37
  - NCSC CAF: A2.a
- RIM7:
  - SIR: Regulation 185 (2,f)
  - NIST CSF V2.0: ID.RA-(04, 05)
  - ISO27001: A5.1
  - NCSC CAF: A2.a
- RIM8:
  - SIR: Regulation 185 (2, f)
  - NIST CSF V2.0: ID.RA-(01, 06), PR.PS-02
  - ISO27001: A5.1
  - NCSC CAF: A2.a

Secure Architecture

- SA1:
  - SIR: Regulation 185 (2, h)
  - NIST CSF V2.0: ID.AM-09, ID.RA-07, PR.PS-(01, 06)
  - ISO27001: A8.9, A8.10, A8.11, A8.12
  - NCSC CAF: B1.b, B4.c
- SA2:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.AA-(01, 03, 04)
  - ISO27001: A8.1, A8.2, A8.3, A8.5, A8.18, A8.20
  - NCSC CAF: B2.(a, b, c, d)

- SA3:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.IR-01
  - ISO27001: A8.21, A8.22
  - NCSC CAF: B4.(b, c), B5.b
- SA4:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.AA-03
  - ISO27001: A8.5, A8.6, A8.18
  - NCSC CAF: B2.(a, d)
- SA5:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.AA-(01, 05)
  - ISO27001: A8.5, A8.6, A8.18
  - NCSC CAF: B2.(a, b, c, d)
- SA6:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.DS-(01, 02, 10), DE.CM-(01, 09)
  - ISO27001: A8.11, A8.24
  - NCSC CAF: B3.(a, b, c, d)
- SA7:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.IP-01
  - ISO27001: A8.31
  - NCSC CAF: B4.b, B5.b
- SA8:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.DS-11
  - ISO27001: A8.13, A8.14
  - NCSC CAF: B5.c

- SA9:
    - SIR: Regulation 185 (2, g, h)
    - NIST CSF V2.0: DE.CM-(01, 09)
    - ISO27001: A8.25, A8.27, A8.28, A8.29
    - NCSC CAF: B3.a
- SA10:
    - SIR: Regulation 185 (2, g, h)
    - NIST CSF V2.0: ID.RA-01
    - ISO27001: A8.8
    - NCSC CAF: C2.b
- SA11:
    - SIR: Regulation 185 (2, g, h)
    - NIST CSF V2.0: PR.PS-01
    - ISO27001: A8.30, A8.32
    - NCSC CAF: B3.(a, b, c)

Spaceflight Ops

- SFO1:
    - SIR: Regulation 185 (2, g)
    - NIST CSF V2.0: ID.AM-(01, 02, 04, 08), PR.PS-03
    - ISO27001: A5.9, A5.11
    - NCSC CAF: A3, B4.d
- SFO2:
    - SIR: Regulation 185 (2, g, h)
    - NIST CSF V2.0: ID.AM-03
    - ISO27001: A8.20, A8.21, A8.22
    - NCSC CAF: A3
- SFO3:
    - SIR: Regulation 185 (2, g, h)
    - NIST CSF V2.0: GV.OC-(04, 05)
    - ISO27001: A7.12, A8.8
    - NCSC CAF: A2, A3

- SFO4:
  - SIR: Regulation 185 (2, g, h)
  - NIST CSF V2.0: PR.IR-(03, 04)
  - ISO27001: A5.29, A8.6
  - NCSC CAF: B5.a

Supply Chain Management

- SCM1:
  - SIR: Regulation 185 (2, i)
  - NIST CSF V2.0: GV.OC-02, ID.RA-10, GV.RM-05, GV.SC-(01, 03, 05, 06, 07, 09, 10)
  - ISO27001: A5.19, A5.20, A5.21, A5.22, A5.23
  - NCSC CAF: A2.a, A4
- SCM2:
  - SIR: Regulation 185 (2, i)
  - NIST CSF V2.0: GV.SC-07, ID.RA-10, DE.CM-(01, 03, 06, 09)
  - ISO27001: A5.19, A5.20, A5.51, A5.22
  - NCSC CAF: A4