AtkinsRéalis

Cyber Security Strategy

April 2024

FUTURE OF FLIGHT CHALLENGE PHASE 3

Notice

This document and its contents have been prepared and are intended solely as information and use in relation to cyber security research and findings for the Future of Flight Challenge.

AtkinsRéalis assumes no responsibility to any other party in respect of or arising out of or in connection with this document and/or its contents.

This document has 46 pages including the cover.

Document history

Document title: Cyber Security Strategy

Document reference: Revision	Purpose description	Originated	Checked	Reviewed	Authorised	Date
0.4	First Draft	KW/AH	CH	-	-	30/06/2023
0.5-9	Updates after internal review	KW/AH	-	-	-	-
1.1	Release to FFC project	KW/AH	PW	CH		31/07/2023

Contents

Acronyms

Acronym	Description
AAM	Advanced Air Mobility
AGL	Aeronautical Ground Lighting
ANSP	Air Navigation Service Providers
BMS	Building Management Systems
CAA	Civil Aviation Authority
CAF	Cyber Assessment Framework
CS	Certification Specification
DfT	Department of Transport
DPA	Data Protection Act
EASA	European Union Aviation Safety Agency
ENISA	European Union Agency for Cyber Security
eVTOL	Electric Vertical Take-off and Landing
FFC	Future of Flight Challenge
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation and Air Conditioning
IACS	Industrial Automation and Control Systems
ICAO	International Civil Aviation Organisation
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
ISMS	Information Security Management System
NASP	National Aviation Security Program
NATS	National Air Traffic Services
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NPA	Notice of Proposed Amendment
OT	Operational Technology
SARP	Standards and Recommended Practices
SUC	System under Consideration
UAM	Urban Air Mobility
UKRI	UK Research and Innovation

Definitions

Term	Definition
Advanced Air Mobility (AAM)	A safe, automated air transportation system for passengers and cargo in urban and rural locations.
Aerodromes	A location from which aircraft flight operations take place, regardless of whether they involve air cargo, passengers, or neither, and regardless of whether it is for public or private use.
Air taxi	A small commercial airplane used for short flights between localities not served by scheduled airlines.
Civil Aviation Authority (CAA)	The statutory corporation which oversees and regulates all aspects of civil aviation in the United Kingdom
Cyber Resilience	The ability to deliver the required outcome for the organisation despite adverse conditions caused by a cyber security attack.
Cyber Security	The application of people, processes, and technology to reduce the risk from cyber-attack.
Cyber Threat Landscape	The global, regional and sector specific threat environment including potential and identified cyber security threats.
Cyber-attack	Malicious activity intended to affect the Confidentiality, Integrity or Availability of technical resources such as Information Technology Systems (IT) or Operational Technology Systems (OT).
e-VTOL	A type of manned or unmanned aircraft that uses electric power to hover, take-off and land vertically, without the use or need for a runway.
Industrial Automation and control Systems (IACS)	In cyber security context, process control and safety systems are referred to as Industrial Automation and Control Systems or Operational Technology (OT) or Industrial Control System (ICS). This document uses the term OT.

INTRODUCTION

1. Background

Advanced Air Mobility (AAM) represents the next frontier in aviation, combining electric propulsion, autonomous systems, and vertical take-off and landing capabilities. As a revolutionary concept, AAM envisions a future where fast, efficient, reliable and sustainable means of passenger and cargo transportation become part of everyday life. With the potential to revolutionise urban transportation, connect remote areas, and alleviate ground congestion, AAM holds the promise of redefining how we travel and reshape the transportation landscape. By leveraging cutting-edge technologies and innovative aircraft designs, AAM aims to unlock new possibilities, offering faster, cleaner, and more accessible aerial transportation solutions for the future.

From world leading technical companies needing to protect their intellectual property (IP) and Flight Operators entrusted with personal data, though to Aerospace Management providers needing to ensure stable and uninterrupted operations, it is clear that cyber security and cyber resilience are crucial to the safe, stable, and reliable development and operation of AAM in the UK.

Currently AAM in the UK is in the Initial State as illustrated in the diagram below developed by NASA and Deloitte as part of UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4 Version 1.0[1]

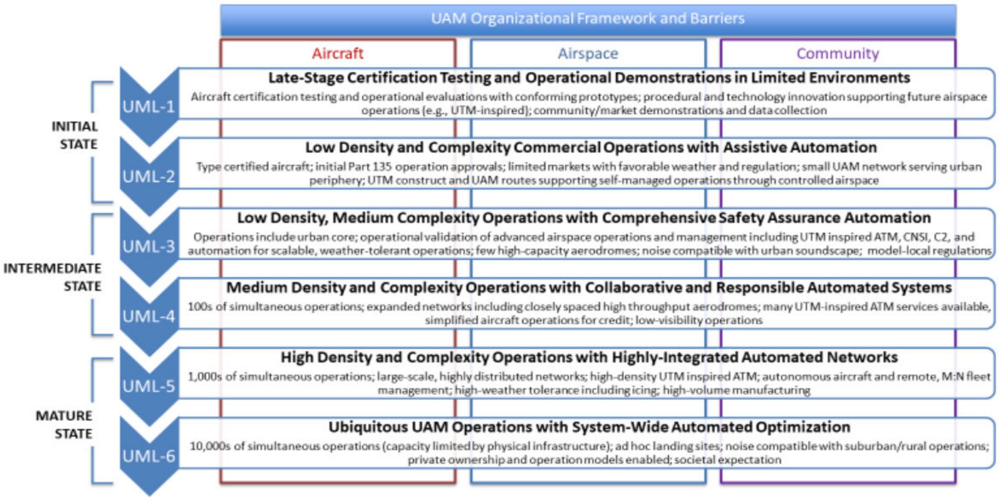

UAM Organizational Framework and Barriers
Aircraft
Airspace
Community
INITIAL STATE
INTERMEDIATE STATE
MATURE STATE
UML-1
Late-Stage Certification Testing and Operational Demonstrations in Limited Environments
Aircraft certification testing and operational evaluations with conforming prototypes; procedural and technology innovation supporting future airspace operations (e.g., UTM-inspired); community/market demonstrations and data collection
UML-2
Low Density and Complexity Commercial Operations with Assistive Automation
Type certified aircraft; initial Part 135 operation approvals; limited markets with favorable weather and regulation; small UAM network serving urban periphery; UTM construct and UAM routes supporting self-managed operations through controlled airspace
UML-3
Low Density, Medium Complexity Operations with Comprehensive Safety Assurance Automation
Operations include urban core; operational validation of advanced airspace operations and management including UTM inspired ATM, CNSI, C2, and automation for scalable, weather-tolerant operations; few high-capacity aerodromes; noise compatible with urban soundscape; model-local regulations
UML-4
Medium Density and Complexity Operations with Collaborative and Responsible Automated Systems
100s of simultaneous operations; expanded networks including closely spaced high throughput aerodromes; many UTM-inspired ATM services available, simplified aircraft operations for credit; low-visibility operations
UML-5
High Density and Complexity Operations with Highly-Integrated Automated Networks
1,000s of simultaneous operations; large-scale, highly distributed networks; high-density UTM inspired ATM; autonomous aircraft and remote, M:N fleet management; high-weather tolerance including icing; high-volume manufacturing
UML-6
Ubiquitous UAM Operations with System-Wide Automated Optimization
10,000s of simultaneous operations (capacity limited by physical infrastructure); ad hoc landing sites; noise compatible with suburban/rural operations; private ownership and operation models enabled; societal expectation

Figure 1-1 – NASA Maturity Model

The cyber security threats, impacts and risks will change over time as the development of AAM progresses from its current Initial State through to ubiquitous operations in its Mature State.

Over this time the quantity of systems employed will increase, new technology will be developed, and the threat landscape will evolve. To manage risk within acceptable limits, it is important that cyber security is considered at this early stage and a strategy

[1] [1] UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4 Version 1.0:

developed that considers the unique challenges of AAM and provides a series of approaches for dealing with cyber security risk in this complex and evolving environment.

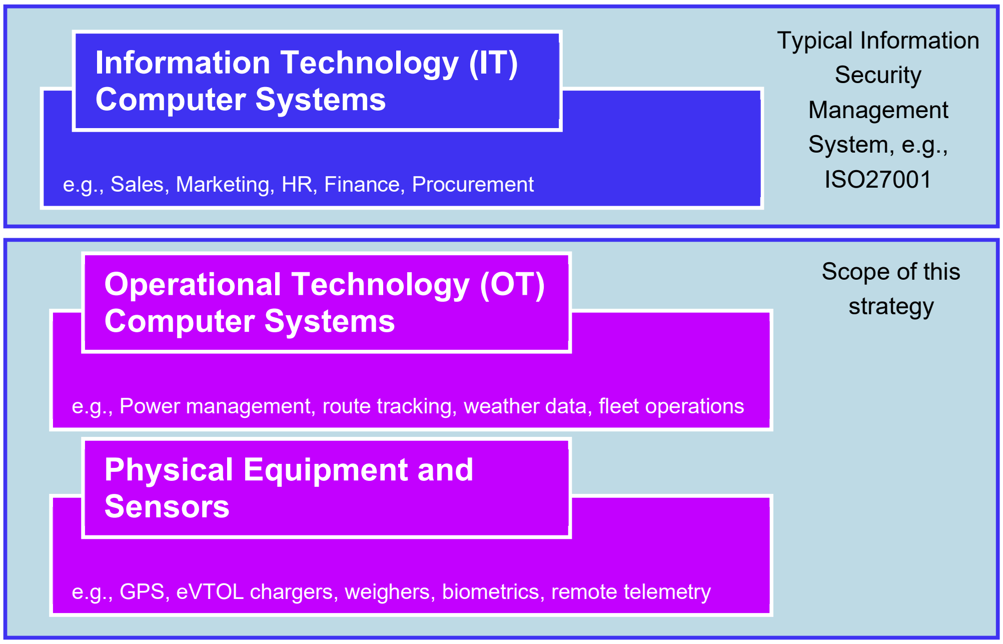
1.1 Scope of Work

The scope of work is the delivery of a Cyber Security Strategy for Future of Flight Challenge (FFC) for the Operational Technology (OT) Computer Systems and Physical Equipment and Sensors and their integration.

This scope of work does not include the specific cyber security requirements for the airworthiness certification and validation of the aircraft, the existing Civil Aviation Authority (CAA) regulations apply and further information on developments in this area should be sought from the CAA.

Cyber security and cyber resilience are wide ranging topics and organisations will have additional cyber security requirements to support the Information Technology (IT) systems used to support their day-to-day business operations, e.g., customer or investor requirements for accreditation, compliance with financial and data protection regulations, etc., these general business systems are also outside of the scope of this document.

> **“This is an evolving area of regulation, and the aviation organisation is responsible for staying abreast of regulatory requirements which may change from time to time.**
>
> **The CAA recommend that regardless of the level of our regulatory involvement, aviation organisations should proactively apply appropriate and proportionate cyber security good practice into their operations.”**
>
> ***CAP1753: The Cyber Security Oversight Process for Aviation***



Information Technology (IT) Computer Systems

e.g., Sales, Marketing, HR, Finance, Procurement

Typical Information Security Management System, e.g., ISO27001

Operational Technology (OT) Computer Systems

e.g., Power management, route tracking, weather data, fleet operations

Physical Equipment and Sensors

e.g., GPS, eVTOL chargers, weighers, biometrics, remote telemetry

Scope of this strategy

1.2 Purpose

The purpose of this document is to define a Cyber Security Strategy for FFC to provide strategic direction for cyber security decision making throughout the evolution of AAM.

This document is not intended to prescribe solutions or specific implementation methods, although examples will be given. Given the complex and evolving landscape internationally of both cyber security standards and regulations, its intent is to provide an overarching approach to cyber security and examples of relevant tools and techniques and how they can be applied in an AAM context.

1.3 Introduction

While AAM operations share some characteristics with traditional aviation, there are many challenges and opportunities that differentiate it from existing models and necessitate the revaluation of proportionate controls from the bottom up.

One of the technological examples of this differentiation is the ambition to develop an automated AAM service without an onboard pilot, this would require a number of new technologies being evaluated, tested and ultimately approved by the relevant regulators which would require high levels of cyber resilience due to the significant safety implications that could result in a cyberattack.

Another example is the passenger experience at one of the many Vertiports planned for the UK. In order to provide a service much more like a taxi than traditional aviation, new and existing technology would be utilised to provide a secure and efficient experience for users, minimising physical checks and providing a seamless experience for passengers. This technology is expected to use biometric data, automated measurement equipment, mobile applications and contactless security checks, all of which need to be secured to protect personally identifiable information and ensure the secure operation of the service.

To understand the regulatory environment in which this project will operate, a separate piece of work has been carried out to identify and review relevant legislation, regulations and standards, the output of this work can be found in AMEC document: D3.5 Cyber Security Standards and Regulations.

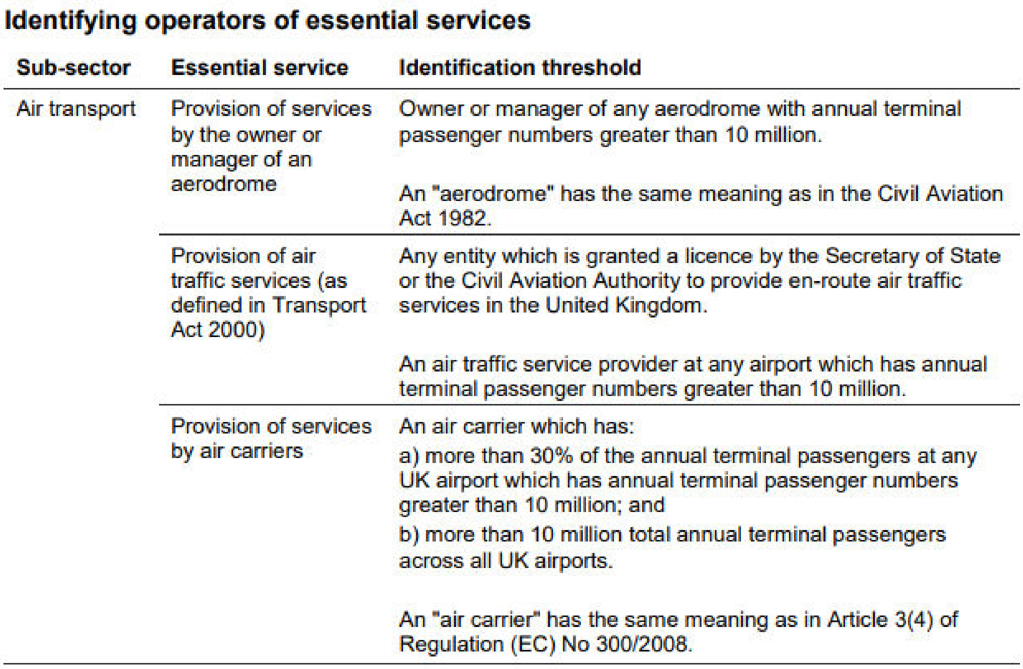
It should be noted that the CAA recognises the continuous evolution of cyber resilience in the aviation sector and provides this guidance in their publication CAP1753: The Cyber Security Oversight Process for Aviation[2].

The CAA has developed a number of documents supporting organisations in demonstrating compliance with the Network and Information Systems (NIS) Regulations, which are useful when considering cyber resilience in the AAM space.

CAP1850: Cyber Assessment Framework (CAF) for Aviation[3] is based on the Cyber Assessment Framework published by the National Cyber Security Centre (NCSC) and provides a framework for carrying out cyber resilience assessments, CAP 1850 is supported by CAP 1849: Cyber Security Critical Systems Scoping Guidance[4].

Vertiports and eVTOL Air Carriers do not reach the threshold of an Essential Service as defined in the Department of Transport Implementation of the NIS Directive DfT Guidance[5] and, as such, are not currently required to comply with the NIS Regulations.

[2] The Cyber Security Oversight Process for Aviation (caa.co.uk)
[3] Cyber Assessment Framework (CAF) for Aviation (caa.co.uk)
[4] Cyber Security Critical Systems Scoping Guidance (caa.co.uk)
[5] Implementation of the NIS directive: DfT guidance version 1.1 (publishing.service.gov.uk)



Identifying operators of essential services

Sub-sector	Essential service	Identification threshold
Air transport	Provision of services by the owner or manager of an aerodrome	Owner or manager of any aerodrome with annual terminal passenger numbers greater than 10 million. An "aerodrome" has the same meaning as in the Civil Aviation Act 1982.
	Provision of air traffic services (as defined in Transport Act 2000)	Any entity which is granted a licence by the Secretary of State or the Civil Aviation Authority to provide en-route air traffic services in the United Kingdom. An air traffic service provider at any airport which has annual terminal passenger numbers greater than 10 million.
	Provision of services by air carriers	An air carrier which has: a) more than 30% of the annual terminal passengers at any UK airport which has annual terminal passenger numbers greater than 10 million; and b) more than 10 million total annual terminal passengers across all UK airports. An "air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008.

Figure 1-1 – Department of Transport Criteria for Operators of Essential Air Transport Services

Although there is no regulatory requirement at this time to reach any specific level of compliance with the Objectives and Principles laid out in the NIS Regulations, CAP1850 and CAP1849 provide a useful framework with which to establish the organisation's own cyber security targets.

While CAP1849 and CAP1850 provide an assessment framework and an approach for scoping and grouping systems, the CAA recommends that aviation organisations select a cyber security risk assessment methodology themselves.

"There are many cyber risk assessment methodologies to choose from when conducting a risk assessment.

Aviation organisations are responsible for selecting a suitable cyber risk assessment methodology…"

UK CAA

The CAA recommends that the following areas are considered when conducting cyber risk assessments:

- Threats
- Vulnerabilities
- Impact (e.g., potential safety impacts)
- Likelihood
- Mitigations and existing controls.

The IEC 62443 series of technical specifications[6] and international standards were developed to address cyber security for Industrial Automation and Control systems (IACS) or OT systems.

The term OT Systems is used in this document rather than IACS, as OT systems recognise the wider application of such technologies outside the limited scope of Industrial Control.

OT systems provide the technology that interfaces computer systems with the physical world[7], which is the developing area that will drive the simplification and automation of AAM services.

eVTOL operations and vertiports are anticipated to utilise a wide range of systems that would be classified as 'OT', such as navigation systems, weather sensors, camera systems, weighers, battery chargers and cooling systems. For this reason, the IEC 62443 is particularly suited as a set of requirements and processes to support the cyber resilience of complex AAM systems.

Within the IEC 62443 set of standards IEC 62443 3-2 Security risk assessment for system design[8] provides an approach to risk assessment for complex OT systems that is directly relevant to FFC and AAM in general.

The cyber security risk assessment process lifecycle of IEC 62443 3-2 can be found in appendix D.5.

[6] Understanding IEC 62443 | IEC
[7] Operational technologies - NCSC.GOV.UK
[8] IEC 62443-3-2:2020 | IEC Webstore

CYBER SECURITY CONTEXT

2. Cyber Security Context

2.1 Recent growth in cyber security incidents

In recent years, there has been an upsurge in cyber security incidents encountered globally resulting in, but not limited to, data breaches, reputational damage, financial loss, disruption of services, and also impacting critical national infrastructure.

In 2022/23, 20% of businesses in the UK reported having had a cyber-attack that resulted in a material impact[9]. Should this continue, for any business operating over a five-year period, the likelihood of not having a cyber-attack that results in a material income is very low unless stronger than average controls are put in place.

A number of high-profile cyber-attacks on systems across several sectors that have led to physical effects have also been reported, with impacts ranging from loss of power and fuel supply to significant fires.

Such incidents have the potential of causing major accidents, potentially resulting in fatalities.

2.2 History of cyber security events in aviation

The following table provides some examples of cyber security incidents in the aviation industry:

Figure	Organisation	Description
2023	Aer Lingus	5,000 Aer Lingus staff have personal data stolen attributed to Russian gang.
2022	Spice Jet	In May 2022, Spice Jet systems impacted by an attempted ransomware attack resulting in passengers being stranded at airports.
2020	Easy Jet	Easy Jet revealed that email addresses, credit card information of nearly 9 million customers were stolen by cyber criminals.
2019	Air New Zealand	Air New Zealand had 120,000 Air-points members' personal data stolen after two staff user accounts had been breached in a phishing attack.

[9] NCSC Annual Review 2022

2018	Bristol Airport	Bristol airport – UK experienced lengthy disruptions over two days in 2018, due to a ransomware attack affecting flight information systems.
2018	British Airways	The Information Commissioner's Office (ICO) fined British Airways £20 million ($26 million) for a data breach that affected both the personal and credit card data of more than 400,000 customers.

2.3 Cyber-attacks in other sectors resulting in physical impact

While none of the above incidents in the aviation industry have yet been identified as affecting physical systems, many of the technologies and communication protocols used in AAM are common to a wide range of other sectors and physical attacks in those sectors have occurred in recent years as the examples below show:

Date	Organisation	Description
2023	Khouzestan Steel Company	Fire in Iranian steel plant attributed to hacking group Predatory Sparrow
2015-2022	Ukrainian power companies	Multiple attacks causing outages to the power grid in Ukraine
2021	Colonial Pipeline company	$4.4m paid in ransom to a hacker group and an emergency declaration in 17 states due to fuel shortages
2010	Iranian Govt.	Stuxnet malware damaged centrifuges in an Iranian nuclear plant

These attacks demonstrate hacking groups' abilities to infiltrate current OT systems and have impact on the physical environment where systems are not sufficiently protected.

As AAM systems become more complex and interconnected, strong governance, cyber security by design and carefully designed and executed control measures are required to ensure cyber resilience.

AAM ECOSYSTEM

3. AAM Ecosystem

3.1 AAM systems

The AAM ecosystem is complex with many interconnected systems required to support the passenger, aircraft and crew journeys along with supporting operational systems.

The diagram below represents some of the systems required for a AAM ecosystem. Each organisation would need to develop their specific diagrams and schedules based on their technical environment.

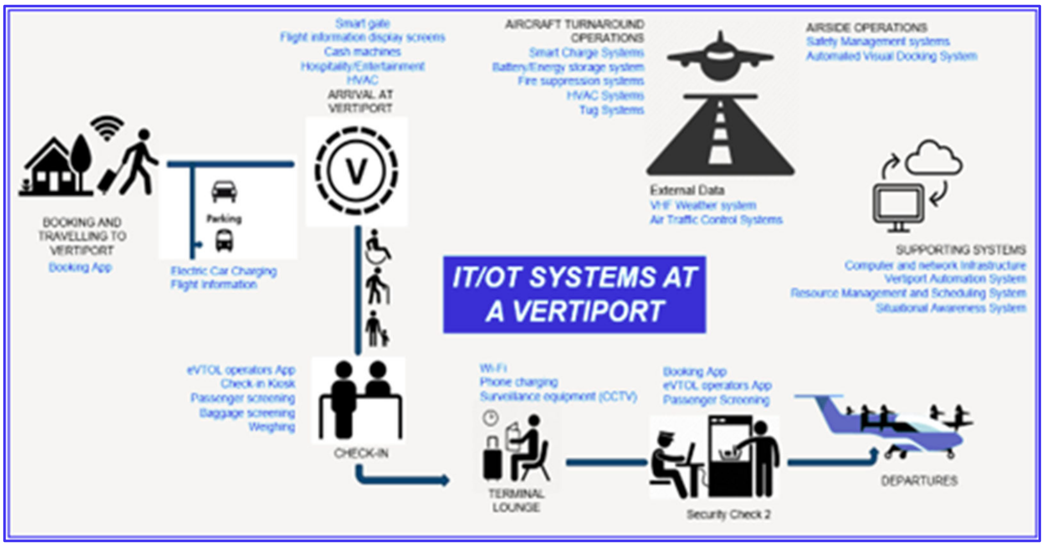
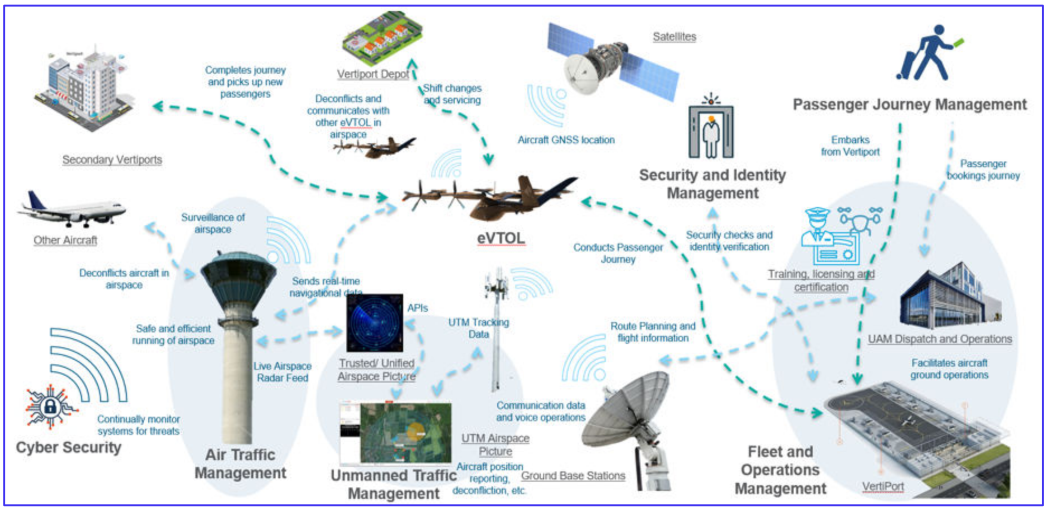


Figure 3-1 - Vertiport Systems Overview

While vertiports form an important part of the AAM infrastructure, their systems must be considered in the context of the wider AAM ecosystem.



Secondary Vertiports
Completes journey and picks up new passengers
Vertiport Depot
Deconflicts and communicates with other eVTOL in airspace
Shift changes and servicing
Satellites
Aircraft GNSS location
Passenger Journey Management
Embarks from Vertiport
Passenger bookings journey
Security and Identity Management
Other Aircraft
Surveillance of airspace
eVTOL
Conducts Passenger Journey
Security checks and identity verification
Training, licensing and certification
Deconflicts aircraft in airspace
Sends real-time navigational data
APIs
UTM Tracking Data
Route Planning and flight information
UAM Dispatch and Operations
Safe and efficient running of airspace
Live Airspace Radar Feed
Trusted/ Unified Airspace Picture
Facilitates aircraft ground operations
Communication data and voice operations
Continually monitor systems for threats
Cyber Security
Air Traffic Management
UTM Airspace Picture
Aircraft position reporting, deconfliction, etc.
Unmanned Traffic Management
Ground Base Stations
Fleet and Operations Management
VertiPort

Figure 3-1 - AAM systems overview

3.2 Operating environment

The AAM solutions will operate in a complex ecosystem with multiple customers interacting with multiple vertical service operators, each dealing with multiple vertiports and new eVTOL aircraft utilising dedicated airspace (Urban Operating Environment – UOE) and existing classes of airspace coordinated by traffic scheduling and tracking providers.

Each of these stakeholders will have differing existing and developing technical infrastructure and risks to consider throughout the AAM maturity journey.

For this reason, a generic solution to cyber resilience for AAM is not possible, and each organisation will need to assess their specific context and threats against their own risk appetite.

This document provides guidance to organisations in setting up their own processes.

CYBER SECURITY APPROACH

4. Cyber Security Approach

The following approach will guide organisations in establishing and maintaining a proportionate level of cyber resilience. It is essential that all parties maintain close contact with the CAA Cyber Security Oversight Team as the regulatory frameworks evolve, to ensure that they are ready to comply with requirements prior to them becoming mandatory.

It should be noted that if the CAA determines that an AAM organisation is in scope of CAP1753: The Cyber Security Oversight Process for Aviation[10], the organisation will be required to nominate a Cyber Security Responsible manager and provide their contact information to the CAA for an engagement phase to be initiated.

4.1 Cyber security governance

For cyber security risk management to be effective, the policy and approach for each organisation needs to be clearly defined.

Governance of cyber security is so critical to a successful cyber security programme that the CAA has directly followed the order of principles set out by the NCSC, and has selected it to be the first principle within the first Objective of the CAP1850 CAF for Aviation Guidance:

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

It is therefore essential that the organisation prioritises clear leadership of cyber security, the creation of necessary policies and procedures which are effectively deployed throughout the organisation and documented, risk-based decision making.

Governance is most effectively sustained thought the use of a formal cyber security programme, such as described in IEC62443 2-1[11].

In organisations where the OT assets form a small part of the overall IT/OT estate, the existing Information Security Management Systems (ISMS) may be extended to cover the OT estate, with appropriate OT specific modifications as identified in this strategy.

[10] The Cyber Security Oversight Process for Aviation (caa.co.uk),

[11] ISA-62443-2-1-2009, Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program

4.2 Cyber security vision

It is helpful for organisations to agree a high-level vision for cyber security risk management in order to communicate the outcome that the Policies and Procedures are set out to deliver.

The published vision for the CAA cyber programme is: **"To have a proportionate and effective approach to cyber security oversight that enables aviation to manage their cyber security risks without compromising aviation safety, security or resilience.**

To stay up to date, current and positively influence cyber within aviation to support the UK's National Cyber Security Strategy."

Using this vision statement as a benchmark, a suitable cyber security vision statement for an organisation in the AAM ecosystem could be:

"To have a proportionate and effective approach to cyber security oversight that enables {insert organisation name} to manage their cyber security risks without compromising safety, security, or resilience."

4.3 Planning

Ensuring that an organisation and its systems have a level of cyber resilience that matches its risk appetite is not a one-off activity, as it is unlikely that an organisation will reach its desired security posture in a single phase and, where that is possible, over time systems age, technology develops, and new threats emerge. For that reason, it is important that cyber security is embedded within the organisation in the same way as other improvement initiatives that need to become part of the business as usual processes.

A suitable approach would be to follow the PDCA Cycle (Plan, Do, Check, Act/Adjust) which is commonly used in a range of sectors[12].

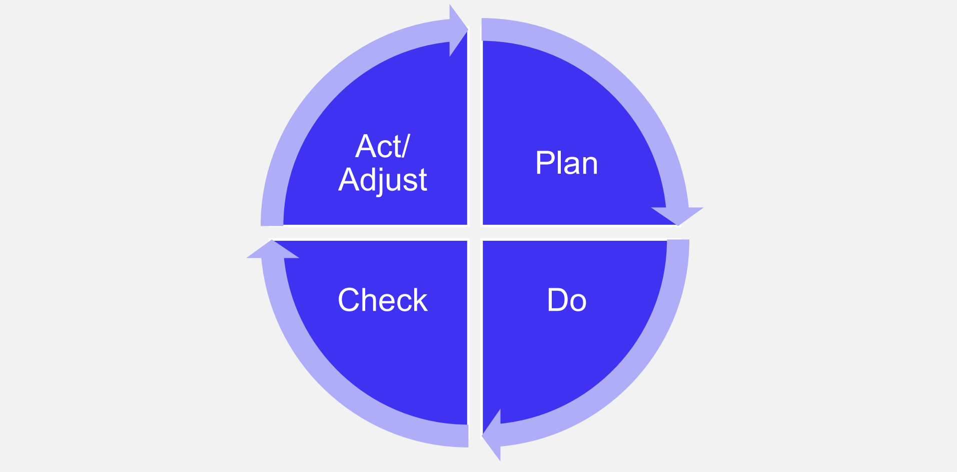


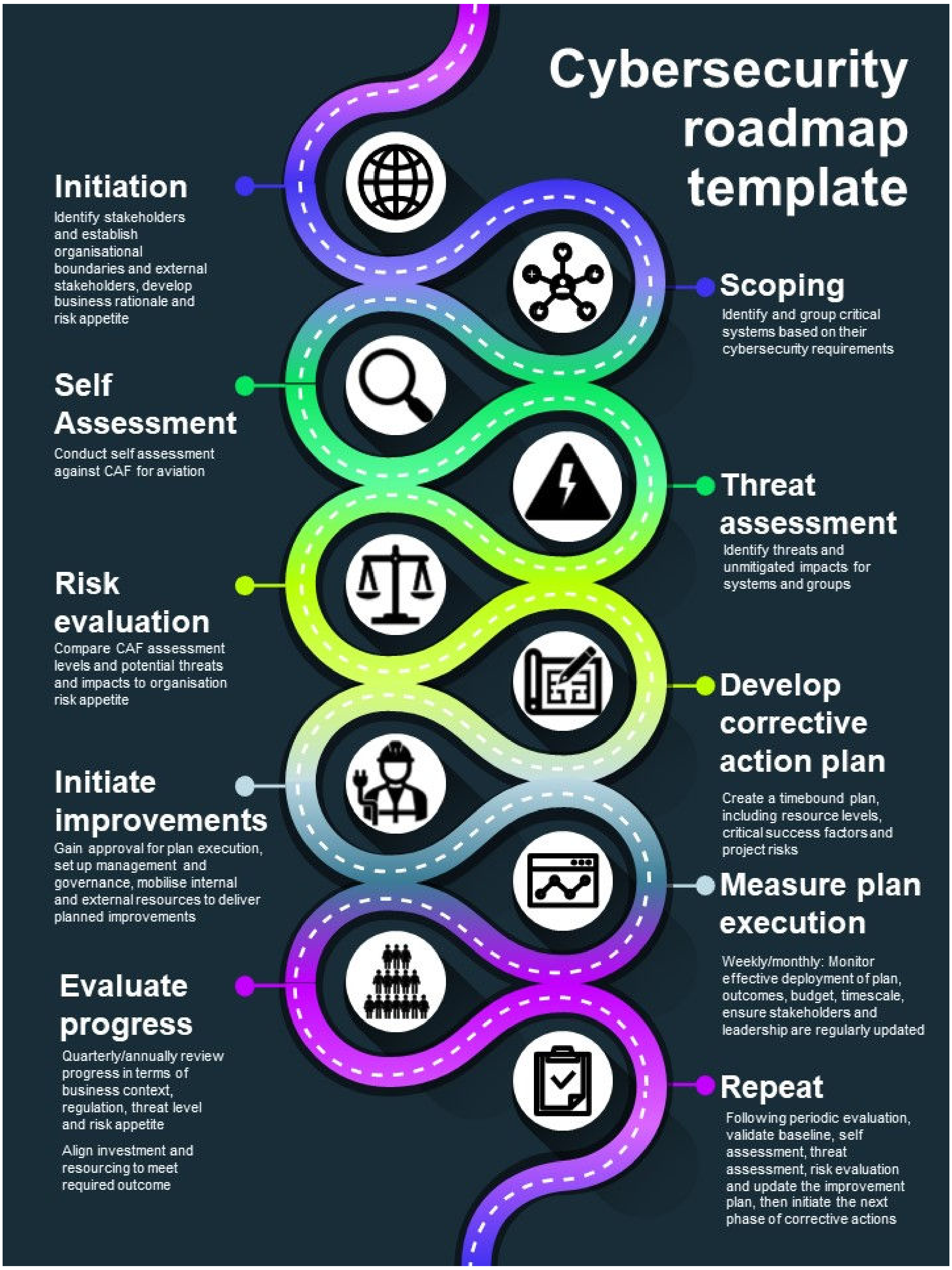
Figure 4-1 – PDCA Cycle

[12] PDCA - Wikipedia

CYBER SECURITY ROADMAP APPROACH

5. Cyber Security Roadmap Template

Achieving an appropriate level of cyber security for an organisation is a journey which is illustrated in the following roadmap template.



Cybersecurity roadmap template

Initiation
Identify stakeholders and establish organisational boundaries and external stakeholders, develop business rationale and risk appetite

Scoping
Identify and group critical systems based on their cybersecurity requirements

Self Assessment
Conduct self assessment against CAF for aviation

Threat assessment
Identify threats and unmitigated impacts for systems and groups

Risk evaluation
Compare CAF assessment levels and potential threats and impacts to organisation risk appetite

Develop corrective action plan
Create a timebound plan, including resource levels, critical success factors and project risks

Initiate improvements
Gain approval for plan execution, set up management and governance, mobilise internal and external resources to deliver planned improvements

Measure plan execution
Weekly/monthly: Monitor effective deployment of plan, outcomes, budget, timescale, ensure stakeholders and leadership are regularly updated

Evaluate progress
Quarterly/annually review progress in terms of business context, regulation, threat level and risk appetite

Align investment and resourcing to meet required outcome

Repeat
Following periodic evaluation, validate baseline, self assessment, threat assessment, risk evaluation and update the improvement plan, then initiate the next phase of corrective actions

Figure 5-1 – Cyber Security Roadmap Template

5.1 Initiation

5.1.1 Identify stakeholders

At the earliest stage of the cyber security management programme two roles are required as a minimum, firstly a suitably senior manager to be accountable for cyber security who has the necessary authority on behalf of the organisation to secure finance for the cyber security activities that are necessary; and secondly a manager responsible for the delivery of the cyber security activities.

The accountable manager may be a business executive with limited knowledge of cyber security; however, the 'cyber security responsible manager' needs to be a Suitably Qualified and Experienced Person (SQEP) to ensure compliance with cyber security regulations and management of cyber security risk.

5.1.2 Develop business rationale

The development of a business rationale for cyber security challenges senior decision makers to evaluate the relevance of cyber security in their business context.

The maturity and the financial stability of the organisation, the regulatory regimes it is operating within, the current credibility and reputation of the organisation are examples of factors that should be considered in developing the rationale.

The rationale uses the broad knowledge and assumptions of the organisation, to determine the level of resource and timescale provided to the cyber security accountable manager for the initiation of cyber security improvement activities.

Once the activities are underway, the assumptions can be validated, and the resourcing and timeline adjusted if required.

5.1.3 Determine risk appetite

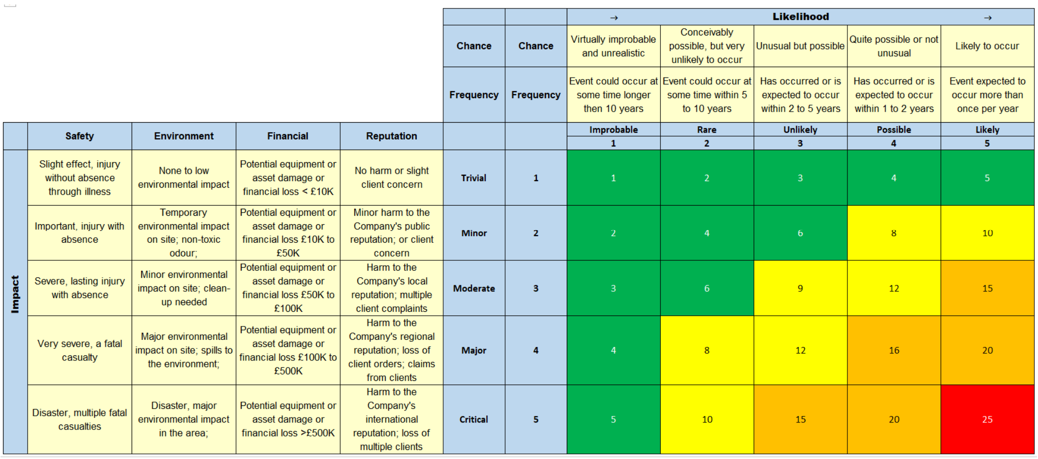
As stated in the cyber security vision, the required outcome is a proportionate response to cyber security risk. To achieve this, it is necessary for the risk appetite of the organisations to be determined (in line with business context and priorities, regulations, and legislation), then clearly articulated to decision makers at all levels within the organisations.

Risk appetite must consider a range of negative outcomes relative to each organisation such as safety, environment, regulatory, reputational, financial etc.

An effective way to evaluate and communicate risk appetite for these complex factors is via a risk matrix.

Risk matrices are individual to each organisation, with the acceptable level of loss for some factors, e.g., financial or reputational, varying by organisation. For other factors, such as environmental or safety risks, there may be a predetermined scale provided by a regulator that the organisations must comply with.

As part of the PDCA process it is important that this risk appetite is periodically reviewed to reflect changes in business context, threat levels and changes in technology.



							→		Likelihood		→
					Chance	Chance	Virtually improbable and unrealistic	Conceivably possible, but very unlikely to occur	Unusual but possible	Quite possible or not unusual	Likely to occur
					Frequency	Frequency	Event could occur at some time longer then 10 years	Event could occur at some time within 5 to 10 years	Has occurred or is expected to occur within 2 to 5 years	Has occurred or is expected to occur within 1 to 2 years	Event expected to occur more than once per year
	Safety	Environment	Financial	Reputation			Improbable 1	Rare 2	Unlikely 3	Possible 4	Likely 5
Impact	Slight effect, injury without absence through illness	None to low environmental impact	Potential equipment or asset damage or financial loss < £10K	No harm or slight client concern	Trivial	1	1	2	3	4	5
	Important, injury with absence	Temporary environmental impact on site; non-toxic odour;	Potential equipment or asset damage or financial loss £10K to £50K	Minor harm to the Company's public reputation; or client concern	Minor	2	2	4	6	8	10
	Severe, lasting injury with absence	Minor environmental impact on site; clean-up needed	Potential equipment or asset damage or financial loss £50K to £100K	Harm to the Company's local reputation; multiple client complaints	Moderate	3	3	6	9	12	15
	Very severe, a fatal casualty	Major environmental impact on site; spills to the environment;	Potential equipment or asset damage or financial loss £100K to £500K	Harm to the Company's regional reputation; loss of client orders; claims from clients	Major	4	4	8	12	16	20
	Disaster, multiple fatal casualties	Disaster, major environmental impact in the area;	Potential equipment or asset damage or financial loss >£500K	Harm to the Company's international reputation; loss of multiple clients	Critical	5	5	10	15	20	25

Figure 5-2 – Example Risk Matrix

5.2 Scoping

5.2.1 Scoping systems

To carry out an assessment of the threats that could impact an organisation delivering AAM, it is necessary to identify the critical systems and sub-systems that could be affected.

The CAA provides guidance on this topic in CAP:1849 Completing the Critical Systems Scoping Template.

The approach required is to break down all functions relating to passengers, baggage, aircraft, crew, and ancillary functions, e.g., passenger booking, baggage tracking, power systems, weight and balance, and identify all of the systems and sub-systems. This could include software, computer infrastructure, communications systems and data.

Where services are provided by external parties, the services provided by the first layer of suppliers should be considered.

To avoid misunderstanding, it is important that a diagram of the interconnected systems is created, and the boundary of the System Under Consideration (SUC) and the external connections are clearly defined.

5.2.2 Grouping systems

The assessment of threats and impacts on a sub-system by sub-system basis would be unnecessarily time consuming and inefficient; both the CAP1849 and IEC 62443 3-2 recognise the need to group systems.

In CAP1849 the guidance states:

> **“Critical systems can be grouped where the same cyber security controls have been applied to reduce duplication….”**

IEC 62443 goes into a great deal more detail on the grouping of assets and provides useful advice on how systems should be grouped to support risk assessment and application of cyber security controls, for this reason the process described in “IEC

62443 3-2 4.4 ZCR 3: Partition the System Under Consideration into Zones and Conduits” should be used.

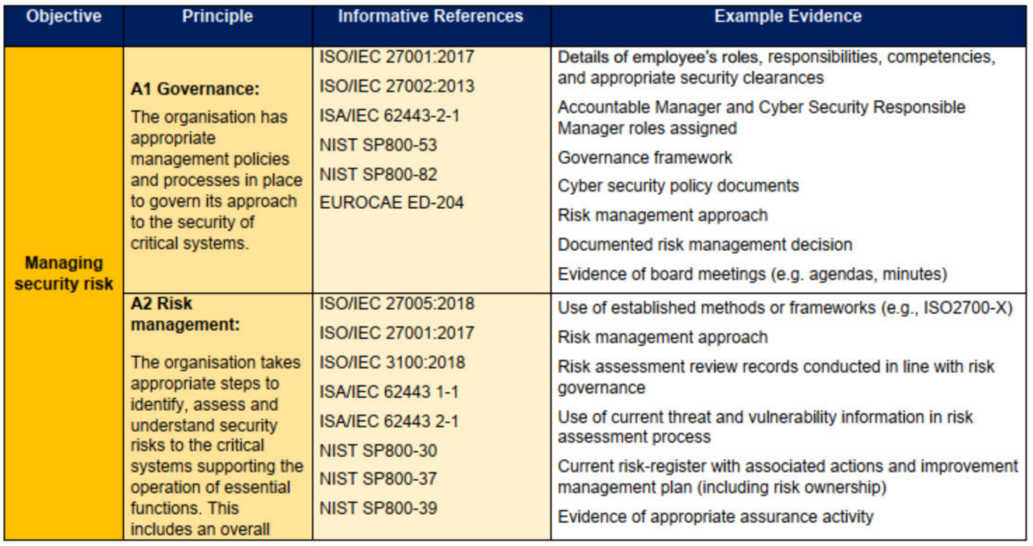
ZCR 3.1 requires that systems are grouped into zones and that the connections between them are identified and assessed separately, these are referred to as conduits:

> **“The intention of grouping assets into zones and conduits is to identify those assets which share common security requirements and to permit the identification of common security measures required to mitigate risk.”**

ZCR 3.2 to 3.6 give further advice on approaches to grouping and segmenting systems. The list of systems, subsystems and their respective zones and conduits should be recorded to support the self-assessment and threat assessment stages.

5.3 Self-assessment

To understand the current cyber security posture of the organisation the CAA CAP1850: Cyber Assessment Framework for Aviation Guidance should be used, as it provides clear example evidence to assist with assessment, as in the example below:



Objective	Principle	Informative References	Example Evidence
Managing security risk	**A1 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	Details of employee's roles, responsibilities, competencies, and appropriate security clearances Accountable Manager and Cyber Security Responsible Manager roles assigned Governance framework Cyber security policy documents Risk management approach Documented risk management decision Evidence of board meetings (e.g. agendas, minutes)
	A2 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	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	Use of established methods or frameworks (e.g., ISO2700-X) Risk management approach Risk assessment review records conducted in line with risk governance Use of current threat and vulnerability information in risk assessment process Current risk-register with associated actions and improvement management plan (including risk ownership) Evidence of appropriate assurance activity

Figure 5-2 – Example Objectives, Principles, and evidence from CAP1850

CAP1850: CAF for Aviation Guidance identifies the following Objectives:

- Objective A – Managing security risk (Manage)

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 functions.

- Objective B – Protecting against cyber-attack (Protect)

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber-attack.

- Objective C – Detecting cyber security events (Detect)

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

- Objective D – Minimising the impact of cyber security incidents (Respond)

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

NB. These four objectives are further broken down into 14 principles in Appendix D. The organisation should assess its achievement of outcomes identified in each principle as either ‘Achieved’, ‘Not Achieved’ or ‘Partially Achieved’.

The output of this process supports the Risk Evaluation Stage.

5.4 Threat assessment

Using the identified zones and conduits, an initial assessment of high-level threats and worst-case consequences will be carried out for each zone or conduit, at this stage likelihood will not be considered as the specific systems and their vulnerabilities will not yet be known.

The potential threats to each zone or conduit should be considered in the following format:

› “Due to {listed vulnerability}”
› “There is a risk of {listed threat}”
› “Causing {stated consequence}.”

An example of this could be:

› “Due to an insecure internet connection on the charging system”
› “There is a risk of a criminal threat actor forcing batteries to overcharge”
› “Causing thermal runaway in the batteries and an uncontrolled fire.”

5.4.1 Selecting threats

When selecting the threats for evaluation at this stage the CAA offers the following advice:

“The CAA expects an aviation organisation to make an informed and competent consideration of reasonable and expected impacts.
The CAA does not expect an aviation organisation to consider implausible scenarios or highly complex chains of events or failures – a reasonable worst-case scenario should be used.”

In addition to threats often associated with IT and OT systems – given the unique nature of AAM – a number of additional threat areas should also be considered.

The following list from NASA[13] illustrates some examples, but it is not comprehensive, and each organisation will need a range of subject matter experts to help them determine the potential threats to their specific systems:

- RF jamming (e.g., ground to air, air to satellite)
- Spoofing (e.g., GPS or ADS-B)
- Man-in-the-middle (Command and Control links)

[13] A Review of Cybersecurity Vulnerabilities for UAM (nasa.gov)

- De-authentication (Command and Control links)
- Eavesdropping (user or crew comms)
- Injection (e.g., Command and Control, ADS-B)
- DoS (e.g., Command and Control, GPS).

The threat landscape is continually evolving with new groups, tools, techniques and procedures being developed constantly. It is essential that organisations maintain awareness of the current heats to their sector and organisation.

To assist with the identification of potential threats, the Mitre ATT&CK Framework for ICS provides a useful reference[14].

A wide range of commercial solutions exist to support this activity and threat reports are routinely issued by the NCSC[15].

5.4.2 Recording threats and impacts per zone and conduit

Zones and conduits, and the relevant systems and sub-systems that are identified, should be recorded along with their associated threats and impacts on a threat assessment worksheet, an example is shown below.

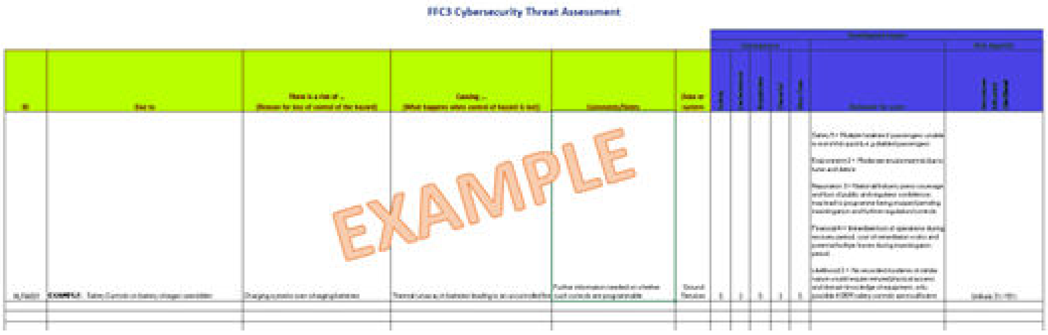

FFC3 Cybersecurity Threat Assessment
EXAMPLE

Figure 5-3 – Example Threat Assessment Worksheet

Each identified threat and consequence combination will be scored against criteria relevant to the organisation, such as safety, environmental, reputational or financial, with no additional mitigation being considered.

The consequences with the highest level of impact per zone should then be summarised for each zone and conduit.

5.4.3 Visualisation of controls using bowtie

The threat and impact assessment will generate a considerable amount of data which, when the existing controls are added, can be difficult to assess and review.

A technique that is commonly used by safety professionals to visualise threats leading to an unwanted consequence is the “bowtie method”.

[14] Matrix | MITRE ATT&CK®

[15] Threat reports - NCSC.GOV.UK

A diagram is constructed using threats on the left leading to a “top event” (which is the event that the organisation is seeking to avoid) and the controls that exist to reduce the risk of the top event occurring; on the right of the top event are the controls that mitigate the effect of the top event or support recovery to normal operation.

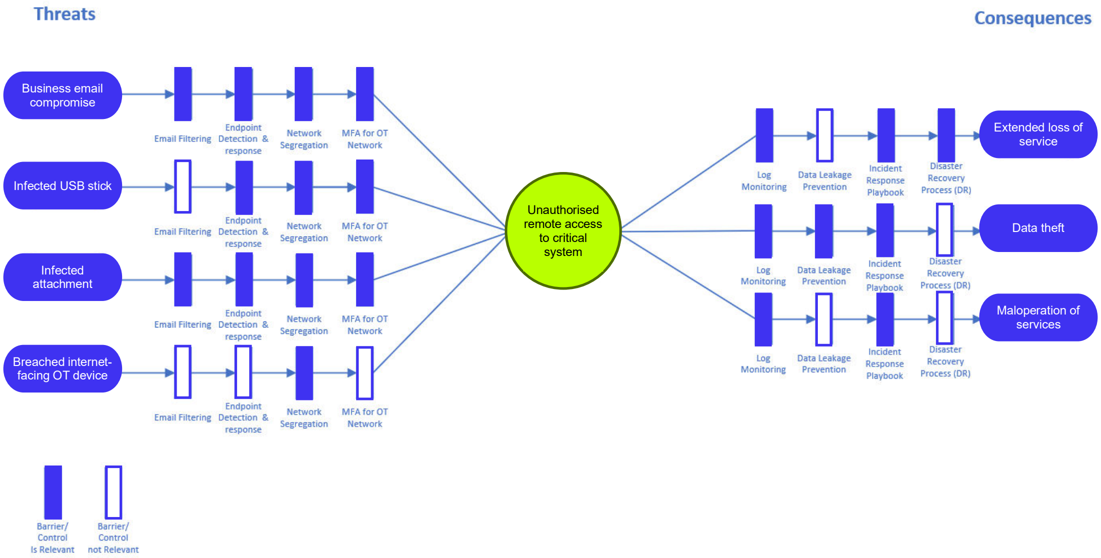

Threats
Consequences
Business email compromise
Email Filtering
Endpoint Detection & response
Network Segregation
MFA for OT Network
Infected USB stick
Email Filtering
Endpoint Detection & response
Network Segregation
MFA for OT Network
Infected attachment
Email Filtering
Endpoint Detection & response
Network Segregation
MFA for OT Network
Breached internet-facing OT device
Email Filtering
Endpoint Detection & response
Network Segregation
MFA for OT Network
Unauthorised remote access to critical system
Log Monitoring
Data Leakage Prevention
Incident Response Playbook
Disaster Recovery Process (DR)
Extended loss of service
Log Monitoring
Data Leakage Prevention
Incident Response Playbook
Disaster Recovery Process (DR)
Data theft
Log Monitoring
Data Leakage Prevention
Incident Response Playbook
Disaster Recovery Process (DR)
Maloperation of services
Barrier/ Control Is Relevant
Barrier/ Control not Relevant

Figure 5-4 – Example Cyber Security Bowtie Diagram

The bowtie technique provides a highly structured way of visualising threats, consequences and controls (usually referred to by safety specialists as barriers) in a single view.

Bowtie diagrams have been in use since the investigations following the Piper Alpha disaster in 1988, and have had widespread adoption in process industries such as oil and gas.

The CAA provides resources on the use of bowties in aviation on its website[16].

“Bowtie is one of many barrier risk models available to assist the identification and management of risk and it is this particular model we have found (and are still finding) useful.” – CAA

Bowtie diagrams are not commonly used in cyber security, potentially due to the perceived level of complexity, and also to the lack of quantitative data to use the bow tie in exactly the same manner as in safety disciplines.

The way the bowtie above has been developed sets out to tackle both of these challenges.

While not providing the full benefit of a quantitative bowtie, the cyber security bowtie shown above uses a binary selection of ‘relevant’ or ‘not relevant’ for each barrier that is in place that could potentially have an effect on the top event and hence outcome.

[16] Introduction to bowtie | Civil Aviation Authority (caa.co.uk)

In a complex system the number of potential barriers could be quite large, and the bowtie provides a means to quickly visualise which barriers are effective against each threat, or in mitigating each consequence.

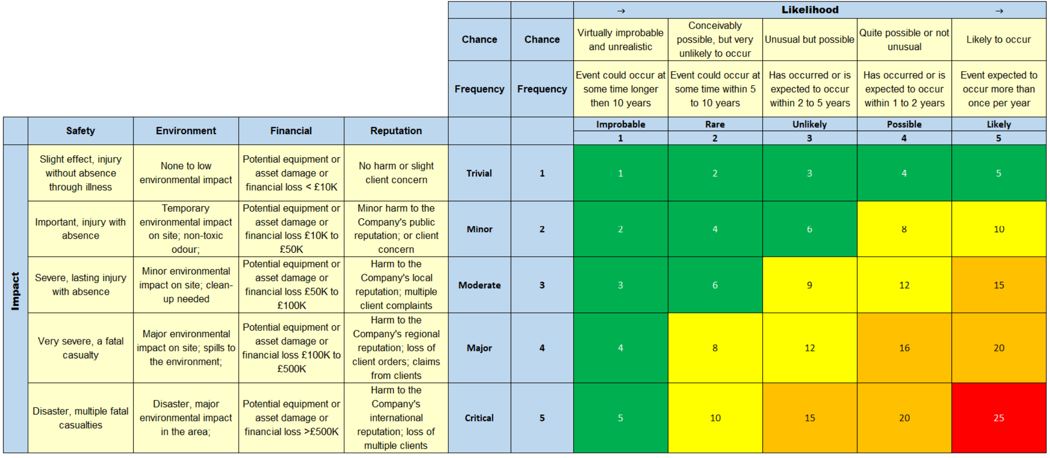
An additional benefit of this approach is that for a given organisation, a template prepopulated with all barriers can be quickly re-used, by adding the threats, top events and consequences from the threat assessment stage; then, following the identification of relevant barriers, any barriers that are found to be not relevant for any of the identified threats or consequences can be removed in order to simplify the finished diagram.

5.5 Risk evaluation

The Risk evaluation step is carried out by a group of domain and cyber security specialists working together.

For each threat identified in step 5.4.2, the controls identified in the self-assessment in step 5.3 are considered, and used to estimate the likelihood of each threat occurring with those controls in place.

The combination of consequence and likelihood for each threat are then plotted on the risk matrix, e.g., for risk 04, the consequence is >£500k, and the likelihood estimated to be ‘unusual but possible’.



							→		Likelihood		→
					Chance	Chance	Virtually improbable and unrealistic	Conceivably possible, but very unlikely to occur	Unusual but possible	Quite possible or not unusual	Likely to occur
					Frequency	Frequency	Event could occur at some time longer then 10 years	Event could occur at some time within 5 to 10 years	Has occurred or is expected to occur within 2 to 5 years	Has occurred or is expected to occur within 1 to 2 years	Event expected to occur more than once per year
	Safety	Environment	Financial	Reputation			Improbable	Rare	Unlikely	Possible	Likely
							1	2	3	4	5
Impact	Slight effect, injury without absence through illness	None to low environmental impact	Potential equipment or asset damage or financial loss < £10K	No harm or slight client concern	Trivial	1	🟩 1	🟩 2	🟩 3	🟩 4	🟩 5
	Important, injury with absence	Temporary environmental impact on site; non-toxic odour;	Potential equipment or asset damage or financial loss £10K to £50K	Minor harm to the Company's public reputation; or client concern	Minor	2	🟩 2	🟩 4	🟩 6	🟨 8	🟨 10
	Severe, lasting injury with absence	Minor environmental impact on site; clean-up needed	Potential equipment or asset damage or financial loss £50K to £100K	Harm to the Company's local reputation; multiple client complaints	Moderate	3	🟩 3	🟩 6	🟨 9	🟨 12	🟧 15
	Very severe, a fatal casualty	Major environmental impact on site; spills to the environment;	Potential equipment or asset damage or financial loss £100K to £500K	Harm to the Company's regional reputation; loss of client orders; claims from clients	Major	4	🟩 4	🟨 8	🟨 12	🟧 16	🟧 20
	Disaster, multiple fatal casualties	Disaster, major environmental impact in the area;	Potential equipment or asset damage or financial loss >£500K	Harm to the Company's international reputation; loss of multiple clients	Critical	5	🟩 5	🟨 10	🟧 15	🟧 20	🟥 25

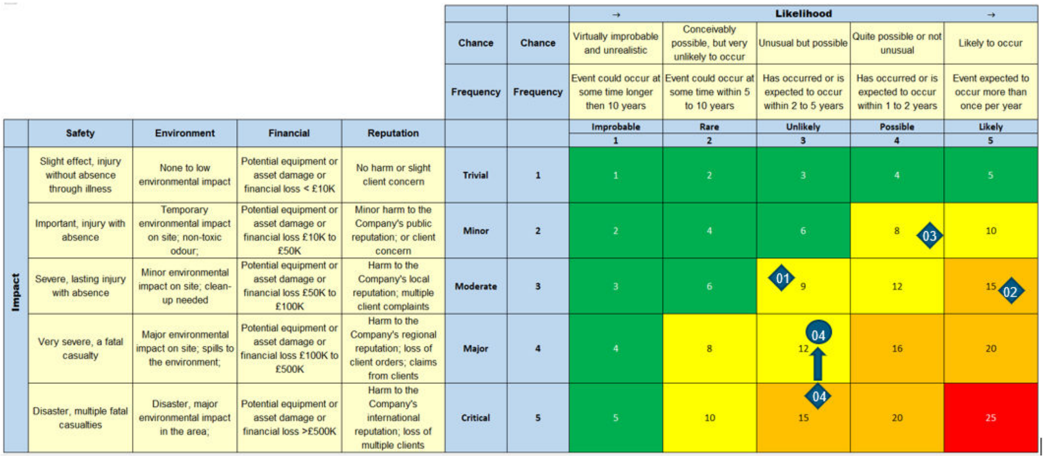
Figure 5-5 – Example Threat Matrix

At this point the Cyber Security Accountable Manager, (supported by the organisation's executive) will review each threat against the risk appetite illustrated by the zones of the risk matrix, and select the appropriate response to each threat:

- Avoid – This would involve the system or service being decommissioned or cancelled, e.g., no longer using an insecure online service
- Modify – This involves taking actions to either reduce the likelihood and/or the impact of the threat
- Share – This could be via insurance or other shared business arrangement
- Retain – Accept the risk in its current form.

5.5.1 Risk treatment

Where the option chosen is to avoid, modify or share, a new position on the risk matrix should be selected as a target.



							→		Likelihood		→
					Chance	Chance	Virtually improbable and unrealistic	Conceivably possible, but very unlikely to occur	Unusual but possible	Quite possible or not unusual	Likely to occur
					Frequency	Frequency	Event could occur at some time longer then 10 years	Event could occur at some time within 5 to 10 years	Has occurred or is expected to occur within 2 to 5 years	Has occurred or is expected to occur within 1 to 2 years	Event expected to occur more than once per year
	Safety	Environment	Financial	Reputation			Improbable	Rare	Unlikely	Possible	Likely
							1	2	3	4	5
Impact	Slight effect, injury without absence through illness	None to low environmental impact	Potential equipment or asset damage or financial loss < £10K	No harm or slight client concern	Trivial	1	1	2	3	4	5
	Important, injury with absence	Temporary environmental impact on site; non-toxic odour;	Potential equipment or asset damage or financial loss £10K to £50K	Minor harm to the Company's public reputation; or client concern	Minor	2	2	4	6	8 03	10
	Severe, lasting injury with absence	Minor environmental impact on site; clean-up needed	Potential equipment or asset damage or financial loss £50K to £100K	Harm to the Company's local reputation; multiple client complaints	Moderate	3	3	6	01 9	12	15 02
	Very severe, a fatal casualty	Major environmental impact on site; spills to the environment;	Potential equipment or asset damage or financial loss £100K to £500K	Harm to the Company's regional reputation; loss of client orders; claims from clients	Major	4	4	8	04 12 ↑	16	20
	Disaster, multiple fatal casualties	Disaster, major environmental impact in the area;	Potential equipment or asset damage or financial loss >£500K	Harm to the Company's international reputation; loss of multiple clients	Critical	5	5	10	04 15	20	25

Figure 5-7 – Example Threat Matrix Showing a Threat Reduction Target

In the diagram above, Risk 04 (with an initial risk score of 15) was assessed and a target of 12 has been set, requiring a reduction in the Impact from 5 to 4.

As this process is carried out, a list of threats and their associated risk treatment requirements will be developed.

5.6 Develop improvement plan

In the previous stage '5.5 Risk Evaluation', a list of threats that require additional risk treatment will have been identified.

For each of those requirements, solutions will need to be defined which could be categorised as people, process, technical or a combination of all three.

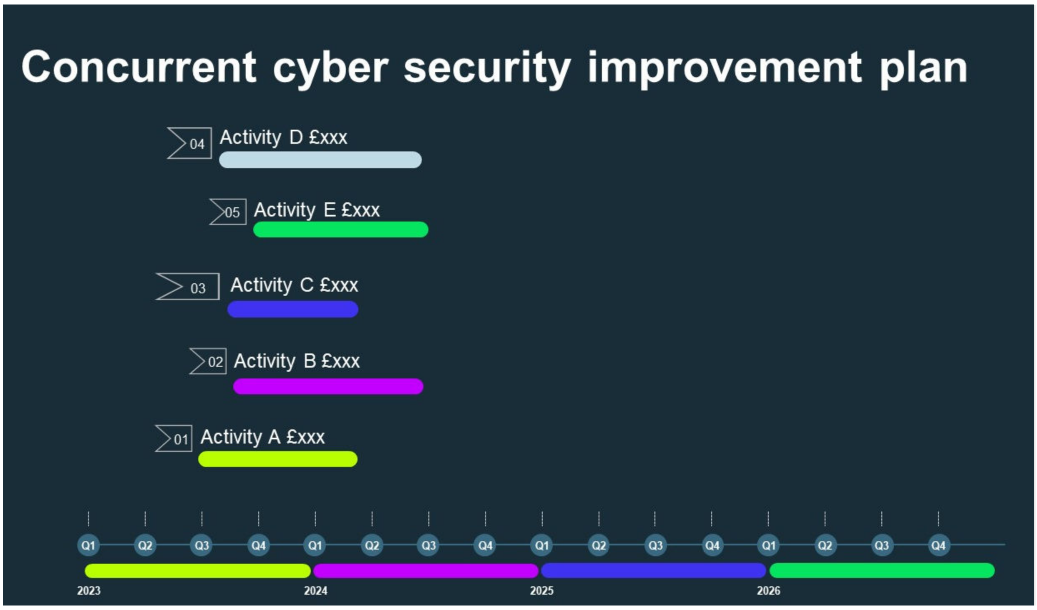
Some will be quick to define, and the necessary resource, timescale, critical success factors and risks will be understood, these can be added to the initial plan.

Other solutions will be complex to define and will need an investigation phase. For these activities, it is important that the investigation phase is clearly defined using the same measures, and that placeholders based on the best available information are used for the execution activity.

This ensures that investigations are not carried out into solutions that are unlikely to be appropriate, and conversely that solutions do not begin execution prior to being sufficiently defined.

This plan, like any other will be constrained by the triple constraints common to all projects which are scope, resource, and timescale for a given level of quality.

An unconstrained concurrent plan should first be developed to deliver all the identified activities within the minimum potential timeline.



Concurrent cyber security improvement plan

Figure 5-6 – Concurrent Cyber Security Improvement Plan

5.6.1 Balancing timescale vs risk

An initial plan to tackle all improvements concurrently is likely to require a level of resource, investment and disruption that the organisation is unwilling to accept.

As the scope was recently defined it should be regarded as fixed, allowing an optimal plan to be determined by the balance of resource/investment vs timescale.

Therefore, the next stage is to iteratively change the phasing of the various activities, until the executive leadership agree that the balance between the resource/investment and timescale meets the business risk appetite, while working within the operational constraints of the business.

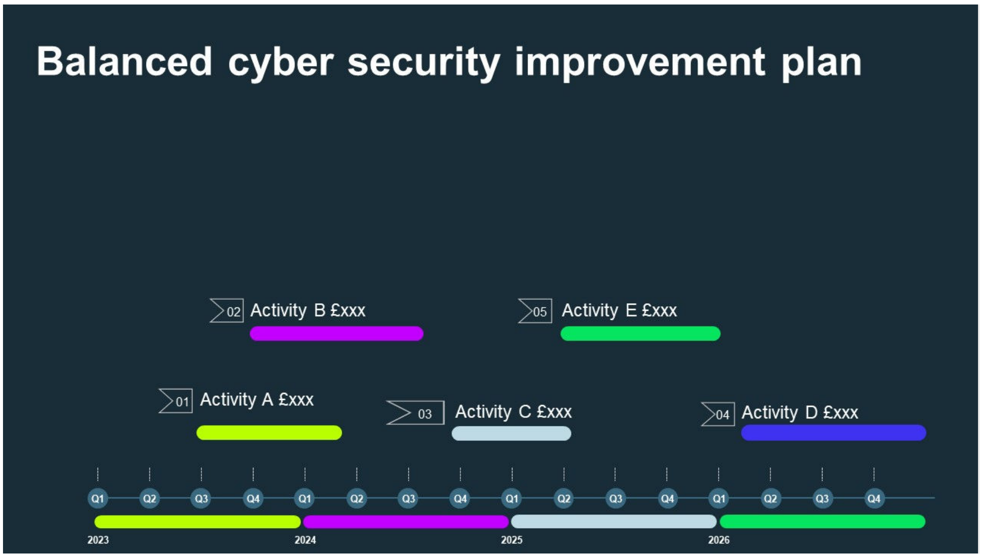

Balanced cyber security improvement plan

Figure 5-7 – Balanced Cyber Security Improvement Plan

5.7 Initiate improvements

Before being initiated, it is important that the Cyber Security Improvement Plan is approved by the organisation Executive Leadership team, to ensure that the resulting initiatives are adequately supported by the business.

While a cyber security programme may have many differences from other programmes being executed by the organisation, it is important that the programme sits within the existing portfolio and programme management processes, reporting structures and business governance and is not seen as an isolated technical activity, to ensure the necessary ongoing visibility and continuity of the programme.

Like any other project the Cyber Security Improvement Plan needs a number of elements in order to be successful:

- A visible senior sponsor to communicate the need for change to the organisation
- A clear scope and set of deliverables
- An appropriate level of resource with the necessary skills to manage and execute the improvement activities
- A schedule that recognises critical success factors such as external dependencies and maintenance windows
- A quantified log of project risks reviewed and accepted by the executive leadership
- Clearly defined measures to assess progress and completion along with cost and timescale
- Clear acceptance criteria of all objectives and deliverables.

Once these items in place the Cyber Security Improvement Plan can be communicated to the necessary stakeholders, the resource mobilised, and any necessary procurement initiated.

5.8 Measure plan execution

Once execution of the Cyber Security Improvement Plan is underway, an appropriate level of oversight is required. This could take the form of scheduled weekly/monthly checkpoints with appropriate levels of staff reporting and monitoring progress.

Areas to review include:

- Progress against objectives
- Timescale
- Budget
- Project Risks.

The outcome of each review should be published to the relevant stakeholders and the Cyber Security Accountable Manager kept up to date on progress, risks, and barriers.

5.9 Evaluate progress

On a quarterly or six-monthly basis, a strategic review of the progress of the plan against the objectives for the period should be carried out.

This review should consider whether the current rate of progress is in line with the expectations of the business to meet the selected objectives.

It should also consider any high-level changes to regulation, business context, threat level, organisation or technology that would necessitate a review of the plan.

At the end of the project phase, and at least annually, the steps that were used to develop the Cyber Security Improvement Plan, i.e., scoping, self-assessment, threat assessment, risk evaluation, should be revalidated and, if necessary, the plan adjusted to reflect the revised information.

The revised plan should then be approved by the organisation’s executive leaders and a new phase of work initiated.

CONCLUSION

6. Conclusion

The AAM market is still at an early stage of development, but the pace of development is increasing rapidly, and it is important that cyber security risks are recognised, and managed, throughout all stages of the lifecycle.

The regulatory frameworks around AAM are still developing, and the CAA also recognises that cyber security regulation for aviation is evolving and that organisations should stay abreast of changes.

Existing NIS Regulations for aerodromes, air traffic services and air carriers do not apply to organisations at the current AAM scale, but may apply to larger existing organisations seeking to operate within the AAM ecosystem. For this reason, we have recommended that the existing "**CAP1850: CAF for Aviation Guidance**" is used as a framework for self-assessment of cyber resilience.

AAM systems are becoming increasingly complex and cloud-dependent, using a wide range of communication technology and smart sensors, all of which share many important characteristics with OT systems. For this reason, we have recommended that the general approach within the IEC 62443 3-2 standard should be used as a basis for segmenting and risk assessing the complex technical infrastructure and systems of an AAM solution, as this is also aligned to the guidance in CAP1849.

An organisation needs to have a readily understood way of communicating its risk appetite to a range of technical and non-technical stakeholders, and we recommend that this is done via a risk matrix. The risk matrix should be approved by the organisation's executive leaders and shared with all relevant decision makers within the business.

Once the organisation has identified the gaps between the current people, processes and technology and the target, a Cyber Security Improvement Plan is developed to address the gaps with regard to the necessary resources, critical success factors and risks.

This plan should then be approved by the organisation's executive and visibly launched to the whole organisation by a senior sponsor.

The improvement programme, once underway, should be monitored and adjusted over the short term and, periodically, strategic reviews should be used to ensure that the Cyber Security Improvement Plan continues to be aligned to ensure people, processes and technology meet the business risk appetite over a longer time horizon.

APPENDICES

Appendix A.

A1. Example Systems in AAM

IT Systems

- Air Traffic Control Systems
- Air Traffic Deconfliction Systems
- Passenger Booking Systems
- Passenger Identity Systems
- Baggage Tracking Systems
- Crew Identification and Scheduling Systems
- Aircraft Planning and Scheduling Systems
- Data storage
- Other Application Software
- Computer Equipment
- Software Licenses
- Cloud Services
- Network Equipment
- Communication Equipment
- Passenger information Systems

OT Systems

- CCTV Cameras
- Baggage Scanners
- Baggage Handling
- Weighing Systems
- Power Systems
- Battery Charging & Monitoring Systems
- Security Scanning Technology
- Fire Alarm monitoring
- Heating, Ventilation and Air Conditioning (HVAC)
- Restricted Access Control
- Aeronautical Ground Lighting
- Building Management Systems (BMS)
- GPS positioning Systems
- Vertiport Surveillance Radar
- Passenger information Screens

Appendix B.

B1. Data Protection Act Principles

The first data protection principle

Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’).

The second data protection principle

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’).

The third data protection principle

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

The fourth data protection principle

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’).

The fifth data protection principle

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’).

The sixth data protection principle

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

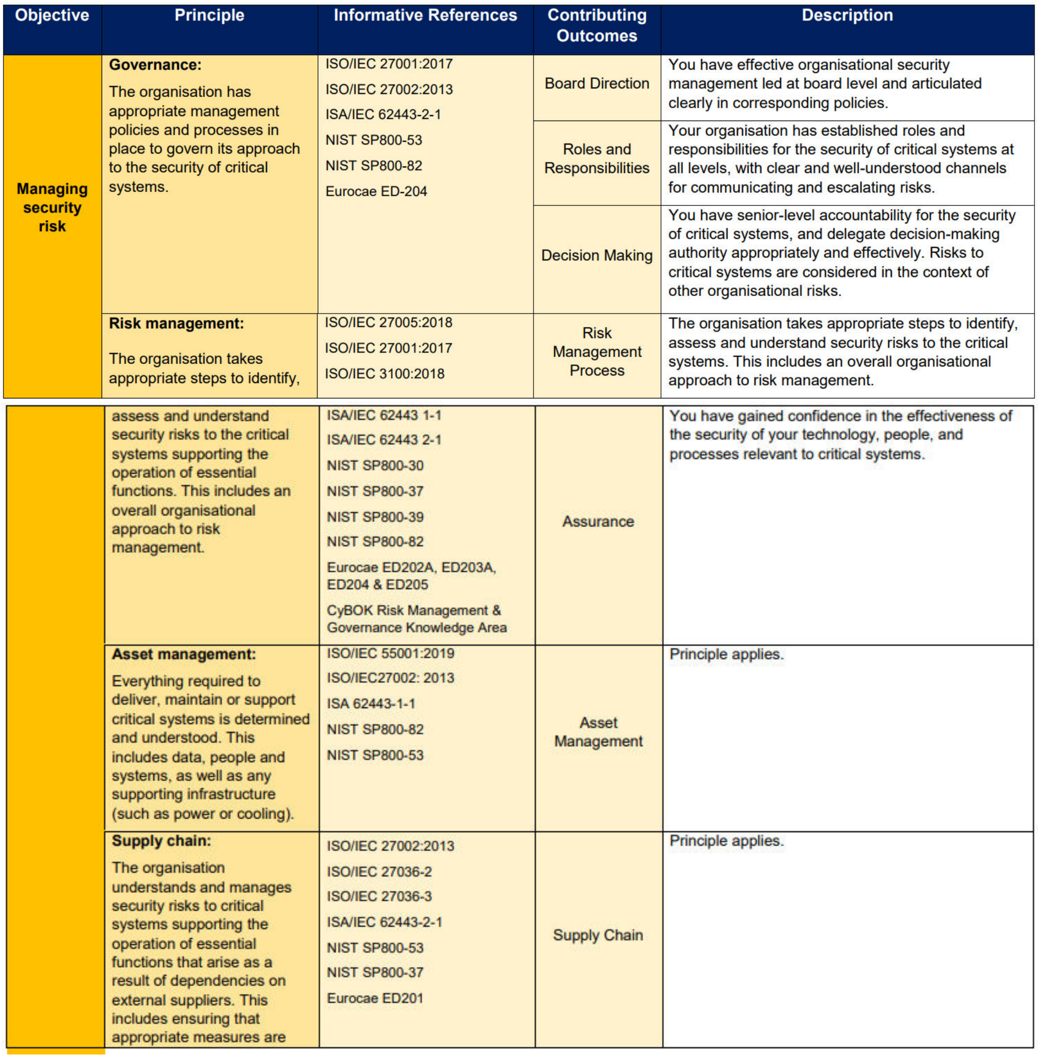
There is stronger legal protection for more sensitive information, such as: race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health, sex life or orientation.

There are separate safeguards for personal data relating to criminal convictions and offences.

Appendix C.

C1. CAF for Aviation Good Practice

The below extract of the 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 refer to CAP 1753, CAP1850 and NCSC's 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,	ISO/IEC 27005:2018 ISO/IEC 27001:2017 ISO/IEC 3100:2018	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.
	assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	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	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	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.

	employed where third party services are used.			
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 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.	ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP800-53 NIST SP800-82 Eurocae ED204 CyBOK Authentication, Authorisation and Accountability Knowledge Base	Identity verification, authentication and authorisation	You robustly verify, authenticate and authorise access to the critical systems.
			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 informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and 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 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.
			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 protective security measures.	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.
			Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.
		NIST SP 800-53 NIST SP800-82 NIST SP800-94	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 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 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	NCSC 10 Steps: Incident Management ISO/IEC 27035 (all) ISO/IEC 22301:2019 ISO/IEC 27002:2013 NIST SP800-61 NIST SP800-53	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.

	designed to contain or limit the impact of compromise are also in place.	NIST SP800-82 Eurocae ED204	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.

Appendix D.

D1. Regulatory References

- CAP1753: CAA Cyber security oversight process for aviation
  The Cyber Security Oversight Process for Aviation (caa.co.uk)

- CAP1849: Cyber Security Critical System Scoping Guidance
  Cyber Security Critical Systems Scoping Guidance (caa.co.uk)

- CAP 1850: Cyber Assessment Framework (CAF) for Aviation Guidance
  Cyber Assessment Framework (CAF) for Aviation (caa.co.uk)

- IEC62443 3-2
  IEC 62443-3-2:2020 | IEC Webstore

Appendix E.

E1 Cyber Security Risk Assessment Process

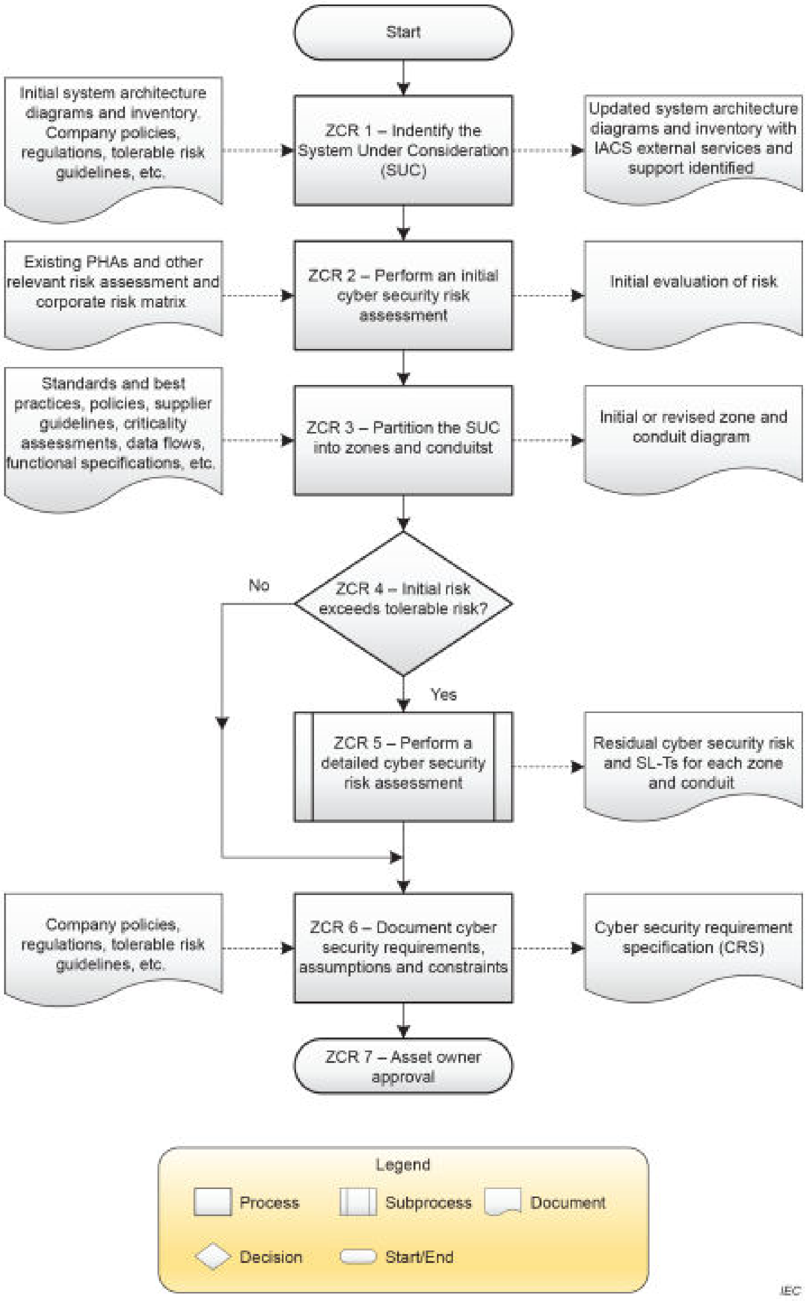

Start
Initial system architecture diagrams and inventory. Company policies, regulations, tolerable risk guidelines, etc.
ZCR 1 – Indentify the System Under Consideration (SUC)
Updated system architecture diagrams and inventory with IACS external services and support identified
Existing PHAs and other relevant risk assessment and corporate risk matrix
ZCR 2 – Perform an initial cyber security risk assessment
Initial evaluation of risk
Standards and best practices, policies, supplier guidelines, criticality assessments, data flows, functional specifications, etc.
ZCR 3 – Partition the SUC into zones and conduitst
Initial or revised zone and conduit diagram
No
ZCR 4 – Initial risk exceeds tolerable risk?
Yes
ZCR 5 – Perform a detailed cyber security risk assessment
Residual cyber security risk and SL-Ts for each zone and conduit
Company policies, regulations, tolerable risk guidelines, etc.
ZCR 6 – Document cyber security requirements, assumptions and constraints
Cyber security requirement specification (CRS)
ZCR 7 – Asset owner approval
Legend
Process
Subprocess
Document
Decision
Start/End
IEC

Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk

Figure E-1 – Cyber Security Risk Assessment Process (IEC 62443 3-2)

AtkinsRéalis

Kevin White / Aysha Hydros
AtkinsRéalis
Nova North

kevin.white@atkinsrealis.com
aysha.hydros@atkinsrealis.com

Future of Flight Challenge Phase 3:
Cyber Security Strategy
April 2024