

CANSO CYBERSECURITY RISK ASSESSMENT GUIDE

2023 Edition

SHAPING
OUR
FUTURE
SKIES

canso.org

Safety is the aviation industry’s number one priority. Air Traffic Management (ATM) faces many challenges including increasing traffic demand; the implementation of new technology; new entrants to airspace, such as unmanned aircraft; security threats from a dynamic threat landscape, and an increasing industry drive towards automation. The ATM industry must address these challenges while continuing to maintain and improve safety.

The Cyber Safety Task Force (CSTF) was created in 2019 to develop a cybersecurity maturity model that focuses on how the ATM service provider prepares for, detects, responds, and recovers from a cybersecurity incident. That work included revising the existing CANSO emergency response planning guide and cybersecurity risk assessment guidance.

ACKNOWLEDGEMENTS

This publication was produced by the CSTF of the Civil Air Navigation Services Organisation (CANSO) Safety Standing Committee. We particularly thank the following organisations which contributed an enormous amount of time and effort, without which this document would not have been possible.

- > Egis
- > Avinor
- > Frequentis
- > Eurocontrol
- > NATS
- > Park Air Systems
- > CAAS

CONTENTS

	EXECUTIVE SUMMARY	4
1.	PURPOSE AND SCOPE	5
2.	THREAT LANDSCAPE	6
3.	RISK ASSESSMENT FRAMEWORK	9
3.1.	Risk Assessment Scope	10
3.2.	Risk Assessment	10
3.3.	Risk Mitigation and Monitoring	16
3.4.	Risk Acceptance	17
3.5.	Risk Communication and Consultation	17
4.	CONCLUSIONS AND RECOMMENDED PRACTICES	18

EXECUTIVE SUMMARY

Air Navigation Service Providers (ANSPs) are a high value target for certain advanced persistent threats (APTs) as they are classified as critical national infrastructure (CNI) service providers. Criminals are constantly evolving into a more professional and organised threat to aviation, particularly as aviation continues its digital transformation which increases the attack potential. This highlights the need for aviation stakeholders to protect their systems and operation, as an inability to do so can lead to unacceptable impacts on safety.

This guide provides a common risk assessment framework consistent with the ISO 27001 series of standards which allows ANSPs to identify, analyse, evaluate and mitigate cybersecurity risks. It highlights how cybersecurity and safety barriers should work together to mitigate risk. This common approach to risk management also facilitates an integrated approach to managing risk across different connected undesirable outcomes, e.g., cybersecurity, safety, business, or environmental impacts.

To effectively secure assets against relevant cybersecurity threats, ANSPs should perform cybersecurity risk assessments to be able to identify the most effective controls to mitigate risk. A risk assessment can also serve as a tool to promote awareness to risk owners, which is necessary to obtain resources for mitigating efforts. This document provides a guide aviation stakeholders to achieve this. ANSPs should consult various frameworks and choose a methodology that meets their need to identify, assess and mitigate risk in their organisation.

This document should be used alongside the CANSO Standard of Excellence in Cybersecurity and the CANSO Emergency Response Planning Guide to enable a holistic and comprehensive approach to managing cybersecurity in the ATM domain.

1. PURPOSE AND SCOPE

The purpose of this document is to enable the ATM community to develop and/or improve cybersecurity risk assessment practices into their existing risk assessment processes and practices to address cybersecurity risks.

The scope of this document is limited to operational ATM systems, but includes the general considerations and best practices required to undertake effective risk assessment activities. The risk assessment process described is not unique, but the application differs as it is focused on the ATM domain. The differentiation is achieved by providing relevant examples of domain specific assets, risks, impacts and mitigations.

This guidance complements the CANSO Standard of Excellence in Cybersecurity, which helps ANSPs assess, develop, and improve their cybersecurity to provide safe and resilient air navigation services. The guidance in this document expands on the Cybersecurity Standard of Excellence's advice on cybersecurity risk assessment.

In some industries, the concept of threat assessment is replacing the more traditional measure of probability/likelihood within the risk assessment process. However, for ANSPs to adopt the cybersecurity risk assessment alongside existing risk management processes, there is a need for a clear and commonly agreed risk assessment guide to be available. Recognising this need, CANSO created this document.

This guide should also be seen in the context of overall risk management which encourages an integrated approach to management of risk, particularly safety risk and security risk. This risk assessment guide provides a discussion of this topic and a recommended approach to safety and security risk management, recognising the commonalities between each topic as well as the trade-offs that must be considered to achieve effective integrated risk management.

A robust approach to identifying, mitigating, and managing cybersecurity risks will help ANSPs to operate an acceptably secure system with the following characteristics:

- The system is able to reliably detect possible compromise of the system;
- The system can quickly respond to, and recover from, a compromise;
- The system can function in a degraded mode, i.e., the system can function despite part or parts of it being compromised/in a process of recovery after a compromise.

2. THREAT LANDSCAPE

The cyber threat landscape, the potential threats affecting a sector, has evolved in recent years. States and state-sponsored groups have grown into advanced persistent threats while the dangers of 'script kiddies' has diminished. Threat actors are becoming more organised, better funded, and more patient.

The aviation sector is an increasingly high-profile target for threat actors, and recent years have seen a gradual rise in attacks upon aviation. These have mainly been limited to the airline and manufacturing areas where personal data, including customer financial details is held. Cyber attacks on ATM systems have, so far, been limited, but the role of aviation as part of CNI makes it a prestigious target for would-be assailants and therefore it is likely that incidents affecting ATM will increase.

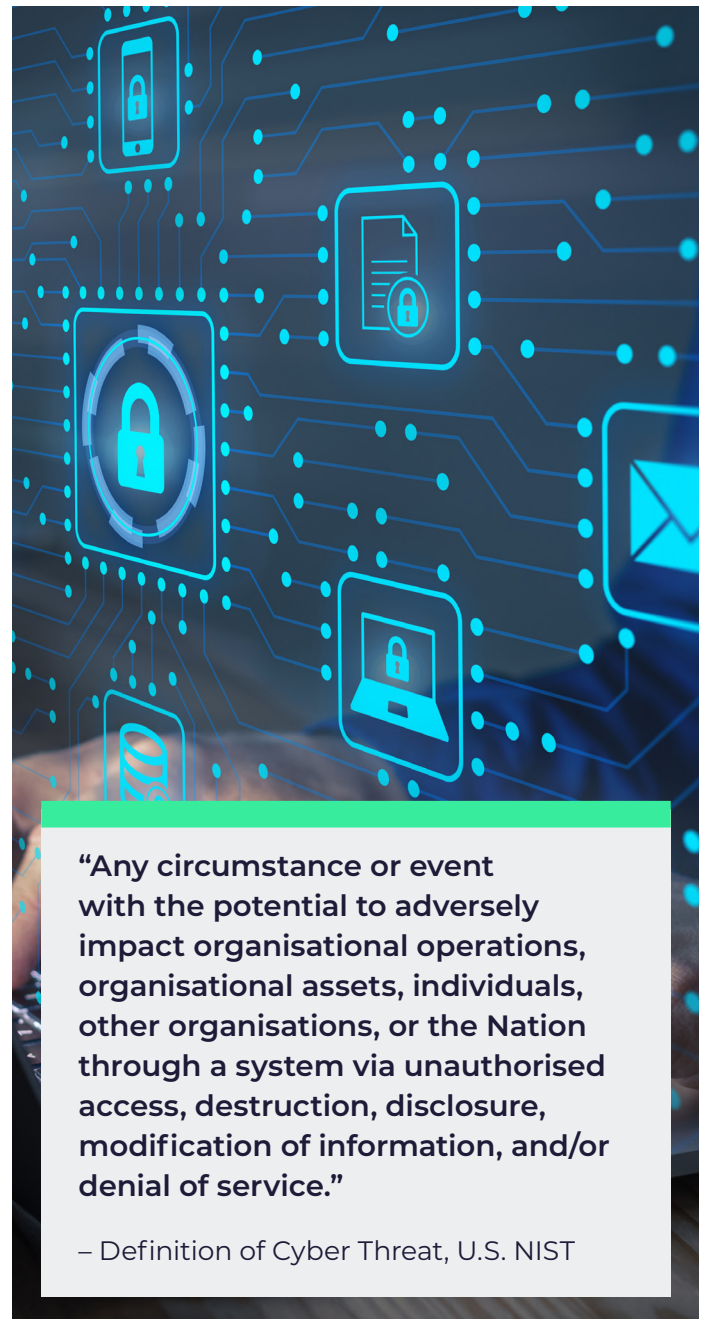
ATM networks continue their digital transformation, connecting to other organisations, and passing more data than ever before. Previously, networks were largely isolated, using telephony infrastructure, which limited risk from outside attack. With the increased connectivity and efficiencies from Internet Protocol (IP) networks, new technologies are taking over, cybersecurity is growing in risk, and is now playing an important role in safety within ATC.

A cybersecurity threat is intentional, may be targeted or non-targeted, and can come from a variety of sources. Figure 1 shows several possible threat actors, including their motivation: nations engaged in espionage and information warfare; criminals; hackers; virus writers; and disgruntled employees and contractors working within an organisation.

Threats can be exacerbated, and even realised by inattentive or poorly trained employees, weaknesses in operating/maintenance procedures, software upgrades, and equipment failures that inadvertently disrupt computer systems or corrupt data.

Threats include both targeted and non-targeted attacks. A targeted attack is when a group or individual specifically attacks a critical infrastructure system. A non-targeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target.

Threats generally include those specific to an individual company or organisation, wider reach threats intended to catch out as many companies or individuals as possible, and attacks that target the supply chain or infrastructure which makes companies (and individuals) unintended victims. Techniques used are varied and increasingly sophisticated including, but not limited to, virus, worm, or malware.



The most concerning threat for an organisation is that of the ‘insider’ – someone who has authorised and legitimate access to a system or network. Other malefactors (such as organised crime or a terrorist group) may make use of insiders, for example, by coercing a willing insider (such as a disgruntled employee), or making use of an unwitting insider (e.g., by influencing someone with authorised network access to insert a disk containing hidden code). However, insider threats can be guarded against and deterred by organisational (e.g.a policy), logical (e.g. authentication) and physical (e.g. restricted proximity card access) controls, and by training staff about the various cyber best practices to avert cyber-attack attempts (e.g. recognising phishing e-mails).

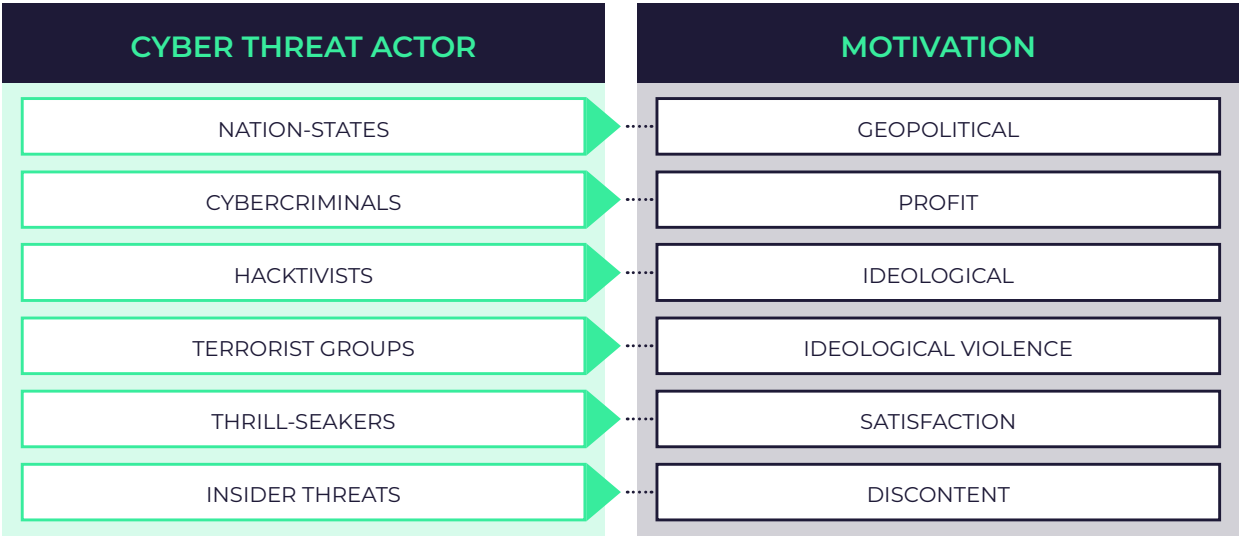


Figure 1 – Cyber threat landscape

Cyber attacks come in a number of forms, from advanced botnets to more simple phishing attacks. The primary goal is to breach security defences and create a foothold in the target network. From this command-and-control position, an attacker can move laterally within the network, gathering data, compromising systems and user accounts. This period has no time limit and depends on the assailant and their end goal, but could include the exfiltration of data, activation of a payload, or continued espionage.

The most common forms of cyber attack include:

Malware – Comes in many forms including ransomware, worms, trojans, adware, and spyware. The aim is to infiltrate, spy, or create a backdoor to control systems.

Phishing – Attempts to trick the target into performing an action. This can be opening a hyperlink to a website, downloading a file, or asking them to fill in a form. Phishing can be non-targeted (i.e., a random attempt to trick anyone), targeted on individuals in positions of authority (whale phishing/whaling) and targeted towards specific organisations and/or lower-level individuals with an email which appears to come from a known contact of the victim (spear phishing). Targeted phishing attacks require a period of reconnaissance from the attacker to perform an attack.

Denial of Service (DoS) – Attacks that attempt to use all of the resources of a system causing it to fail. This can include congesting all available system bandwidth, using all the memory or processors, or simply filling the device storage. Distributed Denial of Service (DDoS) is a type of DoS attack that uses botnets, a number of remotely controlled systems, to bring the bandwidth of many systems to bear upon the target system often used to knock websites offline by bombarding them with requests.

Man in the Middle – The interception and sometimes manipulation of data between systems. Often used to steal or redirect information including directing victims to fake

websites and then harvesting their information. Man in the Middle attacks are harder to execute and are therefore less commonly used by attackers.

Brute Force – Cycling through numerous attempts to finally breach a system. Password lists are often used to perform attacks on accounts to gain access to information. Such lists are readily available online and used by attackers to perform a lengthy attack on targeted systems.

Structured Query Language (SQL) Injection – Malformed insertion of an SQL query via the input data. A successful attack can allow the reading or modifying of database data or allow a malicious actor to administer the database service. This type of attack is commonly used against websites to gain access to data.

Cross-site Scripting (XSS) – XSS uses third-party web resources to run scripts on the victim's system. The attacker injects a payload onto a vulnerable webserver, which then harvests user data or steals their session to take over their account.

The methods of attack are forever changing and evolving with more complex and diverse attacks taking place. Nation states and state-sponsored groups are becoming more meticulous in their planning and delivery which means organisations must become more resilient in their defence.

3. RISK ASSESSMENT FRAMEWORK

A *risk* is a combination of the severity and likelihood of an undesirable outcome typically expressed using a risk classification matrix.

Cybersecurity risk means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of a cybersecurity event. Cybersecurity risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets. The impact such an exploit potentially may cause to information assets in ATM, should at least be derived considering what impact it can cause to *safety*. In this regard ANSPs may take advantage of the corresponding safety assessment since the impact on the level of Air Traffic Service (ATS) is often already identified as part of the safety process.

Considering both safety events and cybersecurity events, the impact on the level of ATS may be the same although the event leading up to the event is different. This alignment may be called *cyber safety* and address the safety impact a potential cybersecurity event may cause to ATS. Similarly, safety and cybersecurity barriers should be considered to work together for mitigating cybersecurity risks with a potential to impact safety.

However, cybersecurity and safety can have conflicting needs. An example of this is the comprehensive software assurance processes required for safety critical systems. The assurance level often demands a significant reliability test period before the system, or a new software release is put into operation. This practice conflicts with having a dynamic patch management process. In these cases, the risks must be benchmarked against each other and a practical approach involving the least risk must be opted for. For example, the corresponding Common Vulnerability Scoring System (CVSS) for a given published vulnerability may serve as an input to a risk-based decision. Alternatively, a process where the needs from both fields are addressed in an adequate manner must be developed. However, it is recognised that safety is the absolute priority in the ATM domain.

To quantitatively and/or qualitatively identify, assess, and mitigate the risk, a cybersecurity risk assessment should be performed.

The output of the risk assessment should be a set of risk mitigating measures to effectively control the identified risks. The identified risks with the associated risk mitigating measures, should be prioritised and communicated to stakeholders. To achieve this, “a *risk acceptance* criterion in line with the organisation’s policies, goals, objectives, and interests of stakeholders, must be defined¹”. In aviation, the thresholds dividing the level of defined risk should, as a minimum, relate to *aviation safety risk* where different thresholds define what scope of actions is required to mitigate the risk.

If risk acceptance thresholds exist at three separate levels of risk, i.e: *Unacceptable, tolerable, and acceptable*, the risk acceptance criterion may be:

The risk introduced by cybersecurity threats, shall be no greater than **tolerable**.

A more conservative and risk averse approach might be to rule out the possibility to accept risk at the **tolerable** and **unacceptable** thresholds therefore leaving the acceptance criterion as:

The risk introduced by cybersecurity threats, shall be no greater than **acceptable**.

1 As quoted in ISO 27005

3.1. RISK ASSESSMENT SCOPE

The first step in conducting a risk assessment consists of understanding the general mission of the organisation. The mission is a high-level description of the purpose of the organisation aimed at aligning all stakeholders involved in the risk assessment activity. The mission for an ANSP may be: “to provide a safe and efficient air traffic service to airspace users”.

Once the high-level mission is identified and agreed, the underlying set of services supporting the mission shall be identified. The services may be provided to internal and external stakeholders and enable the achievement of the mission.

When identifying the services supporting the mission, specific care shall be given to highlight:

- The structure of the organisation providing these services in terms of roles, responsibilities, and accountabilities;
- The dependency of the organisation on third parties and suppliers to achieve its mission;
- The interactions of the organisation with external stakeholders that are required as part of the mission.

Services defined as part of the mission of an ANSP can be ATS, Surveillance Service, Communication Service & Navigation Service. These services and the confidentiality, availability, and integrity of the information the service is dependent on, can be defined as the primary assets of the ANSP. If, for example, the surveillance service is supported by an ATM system, surveillance sensors, tracker, networking etc., those assets are *supporting* assets which may be exposed to vulnerabilities.

Once a clear understanding of the mission, services and assets has been identified, the perimeter of the risk assessment can be defined. The perimeter defines the boundaries of the risk assessment in terms of which services are in scope. All services can be in scope, or a subset of them can be selected.

The selection of the risk assessment perimeter shall take into consideration criteria such as:

- The time at which services were last assessed, recognising that as risks evolve so their existing assessment may become obsolete;
- Occurrences of recent security incidents targeting or impacting specific services;
- Internal or external requirements that may impose a predefined assessment frequency;
- Availability of key stakeholders required as part of the assessment of the perimeter (although unavailability of a single stakeholder should not be considered as a valid criterion to exclude specific business services from the perimeter).

3.2. RISK ASSESSMENT

3.2.1. RISK IDENTIFICATION

The purpose of risk identification is to determine what can happen to cause a potential loss (confidentiality, availability and integrity), and to identify how, where, and why the loss can happen.

3.2.1.1. Identification of the primary assets

Firstly, the relevant primary assets should be determined. Primary assets are “anything that has value to the organisation and which therefore requires protection²”. Within the context

2 ISO 27005:2011 p. 14

of a security risk assessment for aviation service providers, the assets supporting the core functions at the operational level of service should, at least, be identified and placed within the scope of the assessment.

Primary assets or core functions are *intangible*, such as a service or information which is vital to the high-level mission. In an ANSP context, this is typically services or information which the Air Traffic Control Officer (ATCO) uses as primary sources on which to base their operational decisions. Examples of these sources include surveillance tracks, flight data, Controller Pilot DataLink Communication (CPDLC) or communication services. If the confidentiality, integrity or availability of these services is compromised, it may cause an impact on the provision of a safe air traffic service.

Failure to adequately protect primary assets against malicious threats will affect either the organisation directly or its stakeholders. The primary assets are the assets which the organisation needs to safeguard through implementation of cybersecurity controls.

When identifying the primary assets, specific care shall be given to understand their functional relationships. On the one hand, it allows the definition of a logical view of the perimeter of the risk assessment, while on the other it highlights the dependencies (if any) of services on one another. Table 1 provides examples of primary assets for an ANSP:

PRIMARY ASSETS CATEGORIES	PRIMARY INFORMATION ASSETS (DEPENDENCIES)
Surveillance Service	Primary surveillance tracks, secondary surveillance tracks, label information, AIR SUR, GND SUR, Camera picture etc
Communication Service	AIR-GND COM, GND-GND COM, telephony, coordination etc
Flight Data service	Flight plans, SID/STAR, charts etc
Datalink service	DCL, CPDLC
Metrological service	METAR, SNOWTAM, TAF etc
AIS	NOTAM, Airspace management information, AIP etc

Table 1 – Categories of Primary Assets

3.2.1.2. Identification and analysis of impact

When the primary assets are identified and mapped towards the relevant service level ATM-function (i.e. SURveillance, NAVigation, COMmunication), the potential cybersecurity events or scenarios and their impact may be derived.

The identification of the impact aims at systematically characterising the cybersecurity scenarios to which the organisation deems itself vulnerable and wants to prevent within the perimeter of the risk assessment.

The identification of the impact shall be performed at the level of the primary assets and shall revolve around three generic categories drawn from the Confidentiality, Integrity and Availability (CIA) criteria:

- The unavailability of a primary asset (e.g., total loss, partial loss, late generation or distribution, early generation, or distribution).
- The corruption, inadequacy, or inconsistency of a primary asset (e.g., undetected corruption, detectable corruption).

- The divulgence of a business asset to unauthorised systems or individuals.

Once a list of disruptions has been agreed on, their analysis aims at defining:

- The minimum-security requirement of the associated security criteria (CIA), i.e., the lowest acceptable compromise level which, if exceeded, will result in the cause of disruption;
- The consequence of the disruption modes, supported by illustrative examples of plausible consequences.

To evaluate the *minimum-security requirements* of a primary asset, the analysis shall aim to understand:

- The point at which the business asset does not comply anymore with agreed upon quality levels (if any);
- The point at which key stakeholders are unable to either provide or rely on the operational service(s) associated to the primary asset.

To evaluate the *consequence* of the disruption, the analysis shall aim at expressing the consequences of the compromise of the associated primary assets, and rank these consequences in terms of safety, reputational and business effect (e.g., what is permanently lost or irreversible in case of compromise of the primary asset).

At the ATM functional system level, many ANSPs will already have a lot of internal knowledge about the potential impact on safety, which may be used as inputs when deriving the consequence of a disruption.

3.2.1.3. Identification of the supporting assets

The creation, processing, storage, and transmission of primary assets is reliant on a combination of human, physical, procedural, and technological means, which are referred to as *supporting* assets. Supporting assets are tangible, typically equipment and infrastructure upon which the primary assets rely.

Supporting assets are subject to vulnerabilities which may be exploited by threat actors and, in turn, cause a potential safety impact to the primary assets. Since the supporting assets have vulnerabilities, safeguards must be imposed to control the risk.

Failing to safeguard confidentiality, integrity or availability of a primary asset does not depend on the primary asset itself, but rather on a failure or abuse of those properties by using the supporting assets as a vector to achieve this. Successfully identifying a comprehensive and structured view of the supporting assets requires the adoption of a progressive approach. The inventory of supporting assets shall therefore be built incrementally and iteratively.

Table 2 provides an example of categories to guide the identification of supporting assets.

SUPPORTING ASSETS CATEGORIES	EXAMPLES
IT AND TELEPHONY SYSTEMS	
HARDWARE	
Terminal	Stationary PC, laptop, tablet
Telephony equipment	Mobile or landline phone
Storage device	Hard drive, USB stick, memory card, CD/DVD
Server	Server rack, server blade
Network equipment	Router, switch, wireless access points
Security equipment	Firewall, probe, VPN gateway
Industrial equipment	PLC, SCADA, detector
SOFTWARE	
Infrastructure software	Active Directory, DHCP, DNS, Domain controller, print server, file server
Application software	Web server, application server, mail server, DB server, ERP, operational software
Middleware	Messaging system, object request broker
Hypervisor and Operating systems	Windows, Linux, VMWare
COMMUNICATION NETWORKS / LINKS	
IP network / link	Copper cable, fibre cable, wireless access points
Telephone network / link	Telephone line
ORGANISATION	
Personnel	Staff member, contractor, intern
Paper document	Printed document, hand-written document
Verbal exchange	Meeting discussion, phone conversation
FACILITIES	
Physical enclosure	Site, building, room
Physical security system	Badging system, CCTV systems
Supporting utilities	Heating and cooling systems, electrical systems, fire detection systems

Table 2 – Categories of Supporting Assets

3.2.1.4. Identification and analysis of threat scenarios

Threat scenarios are pragmatic actions, or a succession of actions, that would result in the failure or abuse of a supporting asset, and hence the occurrence of a disruption. Identifying threat scenarios consists of identifying these possible (successions of) actions.

The identification of threat scenarios is performed at the level of the supporting assets. The level of detail to adopt during this activity therefore depends on the detail of the inventory of supporting assets. A high-level inventory of supporting assets will only allow for the identification of broad and generic categories of (strategic) threat scenarios, while a more detailed inventory of supporting assets will allow a more comprehensive identification of (operational) threat scenarios.

Initially, as the purpose of the risk assessment is to understand the broad risks affecting the primary assets, the focus shall be to derive *strategic threat scenarios*. These scenarios describe the sequence of events that are generated by a malicious threat actor that would lead to a disruption. The overall objective is to understand the entry points, the propagation means and exploitation vectors that are the most relevant within the perimeter of the risk assessment. Specific care shall be given to not get overwhelmed by specific details at this stage of the risk assessment, as this would only result in a dilution of the key highlights of the exercise.

In following iterations of the risk assessment, the focus can evolve to derive more *operational threat scenarios* that provide additional details relating to the achievement of specific strategic threat scenarios. Operational threat scenarios shall consider detailed technological, physical or organisational supporting assets, possible vulnerabilities or weaknesses affecting these assets, as well as relevant, up-to-date and precise compromise mechanisms/actions that can be leveraged by malicious threat actors to achieve disruption.

Once a list of threat scenarios has been agreed, each should be analysed in terms of its perceived likelihood of impact considering, for instance:

- If any existing security control can limit the malicious threat actor task;
- If any remaining weaknesses or vulnerabilities can facilitate the malicious threat actor's task;
- To what extent the entry point of the threat scenario is exposed to the outside world;
- The malicious threat actors' motivation to target an organisation.

When the supporting assets and the threat scenarios affecting them have been identified, the organisation shall draw an inventory of the existing security controls.

Security controls can be technical or organisational, and should belong to one of the following categories:

- Preventative security controls aimed at preventing the occurrence of a threat scenario;
- Protective security controls aimed at detecting, blocking or containing the occurrence of a threat scenario;
- Response and recovery controls aimed at minimising the disruption or disturbance of the business services from a threat scenario.

The identification of existing security controls allows the organisation to analyse threat scenarios in light of existing defence mechanisms, considering previous efforts invested by the organisation.

3.2.2. RISK ANALYSIS

A risk analysis may be qualitative or quantitative. Often organisations lean to a qualitative approach due to the lack of accurate and reliable data to support a quantitative approach. The output of the risk analysis is a defined risk level for each identified risk which is derived from the defined impact and threat level.

Traditional risk assessment methods encompass a consideration of both probability and severity of impact to achieve an overall risk calculation. The probability calculation can be based on either a measurement of environmental factors (e.g. occurrences of floods) or historic data (e.g. number/prevalence of component failures). With Security Risk Assessments, the way in which probability is considered tends to be different from traditional risk assessments as an additional element, the threat actor, needs to be considered.

For non-targeted cyber threats (e.g. generic malicious code such as traditional computer viruses), the probability element is driven by viruses circulating at the point at which the assessment takes place, and specifics around vulnerabilities that exist within the operating environment. The historic data used to provide a probability assessment is highly dynamic and can change on a week-by-week basis.

Serious cyber threat actors (APTs) who display a clear intention to target a particular organisation or area of business (e.g., aviation), are mostly considered to be capable of successfully causing an impact irrespective of the organisation's defences.

When the likelihood of the threat scenario and its corresponding impact is determined, this information may be fed into a risk matrix (Figure 2) which will assign a risk level (unacceptable, tolerable, acceptable) that may be benchmarked against the risk *acceptance criteria*.

		PROBABILITY OF IMPACT				
Category		Very Unlikely	Unlikely	Likely	Very likely	Extremely likely
SEVERITY OF IMPACT	Catastrophic					
	Severe					
	Major					
	Minor					
	Insignificant					

Figure 2 – Example Risk Classification Matrix

3.2.3. RISK EVALUATION

When the risk level is determined and benchmarked against the risk acceptance criteria, it will provide guidance as to the scope of mitigating efforts that need to be developed to control the risk.

The risk evaluation will give risk owners and practitioners a basis on which to prioritise between the risks and determine the need for further risk mitigation and monitoring.

The framework for risk evaluation may be defined as presented in Table 3:



ACCEPTANCE THRESHOLD	ACCEPTANCE CRITERIA
 UNACCEPTABLE	Derived risk cannot be accepted, mitigating action is mandatory
 TOLERABLE	Risk can be accepted if the cost/effort of implementing mitigating control can be shown to be disproportionate to the effectiveness of the control.
 ACCEPTABLE	Risk is acceptable, no mitigating effort is deemed necessary

Table 3 – Risk Acceptance Thresholds

3.3. RISK MITIGATION AND MONITORING

For ANSP management to fully assess the cybersecurity risks on the net-centric aviation system performance, several activities need to be undertaken. These include the performance of a cost benefit analysis relating to the introduction of relevant cybersecurity functions and the determination of suitable policies, procedures, and processes to support a holistic cybersecurity posture. A key aspect is the presence of detection mechanisms which need to be established to identify the presence of a threat, and decision support tools for threat evaluation and mitigation. Once a threat has been detected it is the ANSP management's responsibility to consider ways in which their organisation can address that threat, including the mitigation and monitoring mechanisms.

Risk mitigation and monitoring represents a strategy to allow an organisation to prepare for, and mitigate, the effects of threats they may face (recognising that some threats may not be avoided entirely) using identified steps to reduce the negative effects of threats on service provision. The way in which risks may be mitigated is likely to vary from organisation to organisation and, therefore, it is up to each one to identify the most appropriate methodologies and priorities (recognising the impact of each risk and prioritising accordingly).

Key steps in risk mitigation are identification of risk mitigations, prioritising risk mitigation and monitoring the established risk mitigation plan. Further details and examples of these steps are provided below:

- Identification of appropriate risk mitigation strategies that will effectively mitigate the identified risk (e.g. emergency contingency systems, segmentation of network domains, access control, detection means etc.);
- Prioritisation of risk mitigation strategies based on an assessment of cost and effectiveness against the identified risks (The organisation's risk appetite will inform the definition of cost-effectiveness for the identified mitigation strategies);
- Implementation and monitoring of progress. This step sees the re-evaluation of the plan's effectiveness in mitigation as needed.

Risk monitoring allows a tracking of risks as they change in significance. This step requires the existence of effective metrics for tracking risk as it evolves. Risks can change if the environment (threat picture) changes or if the organisational technical infrastructure changes.

3.4. RISK ACCEPTANCE

Risk acceptance indicates that an organisation is willing to accept the level of risk associated with a given activity or process. There may be times when the risk level resulting from a risk assessment process is not defined as acceptable, but an organisation may choose to accept the risk because all other alternatives are unacceptable.

Acceptance of residual risks must occur at the executive management level of the organisation and, therefore, much of the risk acceptance process concerns the effective communication of residual risks to decision makers. Once accepted, residual risks are considered as ones that the management of the organisation knowingly takes. The level and extent of accepted risks comprise one of the major parameters of the risk management process.

As mentioned in “3.2.3. Risk Evaluation” on page 16, the criteria for the acceptance, or otherwise, of a residual risk will vary from industry to industry and organisation to organisation, and may include parameters such as fatalities which may occur, legal repercussions and financial impact.

It is likely that, over time, the nature of risks will change and evolve, for example through changing technical conditions. In such instances, further iterations of the risk management process are required which will result in a re-evaluation of residual risks and, therefore, risks that had previously been accepted may require a different treatment.

It is important that, for consistency of assessing and presenting risks including their acceptability, the same risk matrix used in the original risk assessment should be applied again to verify that the risk is mitigated to an acceptable level (“3.2.2. Risk Analysis” on page 15).

3.5. RISK COMMUNICATION AND CONSULTATION

The purpose of risk communication and consultation is to help relevant stakeholders affected by the risk to understand the risk and gain support for the necessary mitigating actions. Communication will promote awareness and understanding of the risk whereas consultation will be in the form of feedback and information to support decision-making.

Risk communication and consultation takes place within all steps of the risk management process. It helps to bring different areas of expertise together as a whole.

3.5.1. SHARING RISK METHODOLOGY WITH STAKEHOLDERS

It is crucial to consider different views at the start of the risk evaluation process so that stakeholders are consulted and aligned with the risk criteria and risk evaluation. Subsequent communication should then be easier with focus on the risk findings and risk mitigation options rather than challenging the methodology itself. It will be helpful to explain that likelihood of cybersecurity risk does not depend on historical occurrence of cybersecurity incidents in aviation industry.

3.5.2. SHARING RISK FINDING AND RECOMMENDATIONS WITH STAKEHOLDERS

Stakeholders’ awareness and understanding of the risk is vital so that they can provide feedback and assess the feasibility of the risk mitigating options.

3.5.3. RISK TREATMENT

Organisations vary in culture, values, and cybersecurity maturity level. Hence, organisations may not be able to adopt every industry best practice recommendation. It is important for stakeholders to reach a consensus on how to mitigate the risk if there are no feasible recommendations. Also, it helps to build a sense of ownership for those who are affected by risk or delegated to treat the risk.

3.5.4. BUDGET APPROVAL AND APPRAISAL OF RISK ASSESSMENT OUTCOME

Management will decide whether to approve the business case and associated budget to support the investment of efforts and solutions to mitigate risk. Briefing management is a vital step in agreeing their support for the investment and enables management to demonstrate oversight of the risk. It may also be helpful to associate the cybersecurity risk with the potential impact on service delivery which may facilitate management's understanding of the nature of the risk.

4. CONCLUSIONS AND RECOMMENDED PRACTICES

As malefactor activity increases globally, ANSPs must be proactive in their assessment of cybersecurity risk. Understanding their organisation's mission, role in public safety, and impacts to the global economy is a critical first step. The information provided in this document supports ATM organisations in developing or improving their cybersecurity assessment processes and policies. The application of a comprehensive and effective process of cybersecurity risk identification, analysis, evaluation, mitigation and monitoring will help maintain aviation safety and security through the delivery of safe and secure air navigation services.

ANSPs wishing to incorporate cybersecurity management into their integrated risk management system can use this risk assessment guide as a basis for that objective.

It is also fundamental that the risk assessment process is dynamic and subject to continuous improvement and regular review to ensure that changes in the external threat landscape, ATM system architecture, system configuration and/or system operation are accounted for.

This guidance used in conjunction with the CANSO Standard of Excellence in Cybersecurity and CANSO Emergency Response Planning Guide should enable ANSPs to improve their approach to management of cybersecurity risk and promote a more resilient global air navigation system.

APPENDIX A – CYBERSECURITY IN ATM

Within the context of the Convention on International Civil Aviation (ICAO Doc. 7300/The Chicago Convention), Air Navigation Services are provided as part of a State obligation which includes the requirement to safeguard essential national security or defence policy interests. In many cases, States must meet certain legal requirements, obligations and specific procedures regarding critical infrastructure protection. Of paramount importance to cybersecurity in ATM is data integrity and information assurance and therefore it is important to understand the requirements for these as well as the measures and strategies that can be taken to secure them.

DATA INTEGRITY AND INFORMATION ASSURANCE REQUIREMENTS

The requirements around data integrity and information assurance when considered within an aviation context may be broken down into the following elements:

- **Confidentiality:** the assurance that aviation information is not disclosed to unauthorised persons, processes, or devices. It includes both the protection of operational aviation information and the information assurance of password or configuration files;
- **Integrity:** the assurance that aviation information is not modified by unauthorised entities or through unauthorised processes. Integrity supports the assurance that information is not accidentally or maliciously manipulated, altered, or corrupted, and also means that detection of alterations occurs with no or minimal false alarms; the alteration source must be identifiable;
- **Availability:** assures timely, reliable and continued access to aviation data and information systems by authorised users. Availability controls protect against degraded capabilities and denial of service conditions;
- **Authentication:** assurance of the identity of message senders and receivers. Authentication supports the validation of messages and information system requests;
- **Authorisation:** the verifiable identity of each entity handling any asset must be checked to ensure that the entity possesses appropriate permissions and privilege levels;
- **Non-repudiation:** assuring both the sender and receiver involved in the processing of the data. This is achieved through ensuring that the data sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity;
- **Traceability:** ensures that all actions performed on each asset are logged in a format and for a time period that can satisfy both regulatory and consumer needs.

ENTERPRISE SYSTEMS, WIRELESS, ANZD CLOUD COMPUTING SECURITY

Information exchanges on the ground network benefit from the use of enterprise security and cloud computing security considerations for addressing information assurance, mixed criticality of assets, and multiple business domains. Wireless security solutions at all layers, including physical-layer security of wireless networks, can help secure the aviation system.

AERONAUTICAL SYSTEMS SECURITY

Pre-shared symmetric key-based solutions can provide data link security and aeronautical information exchange security (e.g. ACARS, satellite links). Position verification mechanisms are needed for the detection of spoofing³, while regulations and legal statutes need to be in place to deter spoofing and other such threats.

³ Spoofing is where a person or programme successfully masquerades as another by falsifying data, thereby gaining illegitimate access, usually due to lack of authentication mechanisms for identity verification.

MITIGATING PHYSICAL ATTACKS ON CYBER ASSETS

Mitigation represents methods used to prevent or detect adverse human actions, physical destruction or sabotage of networking and information technology infrastructure, including aspects such as cyber, radio frequency (RF) jamming, etc. The physical methods used to defeat physical attacks targeted at cyber assets can include:

- System Access Controls;
- Physical checks and processes;
- Detection of abnormal and unauthorised sources of RF energy.

An Information Security Management System (ISMS) is part of a more complex security framework called a Security Management System (SeMS) in which strong and robust relationships exist among the main pillars of personnel, infrastructures, information, organisation, and procedures; thereby enabling an entity to enhance security performance by proactively managing risks, threats, and areas where there are gaps and vulnerabilities which may have a negative impact on that performance.

Cross-correlations between physical and information security allows an understanding of events that, individually considered, are meaningless, but could be of significance if related and properly analysed.

CYBERSECURITY DEVELOPMENT AND MANAGEMENT

Security of the net-centric aviation system must be designed, implemented and administered appropriately, e.g. proper assignment and management of suitable access privileges at each entity, proper management and protection of strong passwords, cryptographic and security quantities.

Within this net-centric aviation system, aircraft operators are assumed to operate in an appropriate manner, reliably managing software configurations and other digital content important for the secure operation of their fleets.

CYBERSECURITY SOLUTION STRATEGIES

The security architecture must be developed to be able to identify points of unauthorised entry and vulnerabilities, and to include suitable mitigations. An end-to-end security architecture is required as multiple stakeholders are involved in the process of information sharing within the aviation domain while a security and trust relationship must exist between information suppliers and information consumers. The global scale of the aviation system makes achieving end-to-end security challenging, especially considering needs such as system interoperability and security policies. However, end-to-end security design may reduce the security cost impact on the net-centric aviation system. To implement effective cybersecurity strategies, multi-stakeholder trust partnerships need to be established that encourage information sharing and collaboration.

It will also be necessary to determine how to evaluate the security strength of the aviation system. A high assurance level for an end-to-end security architecture is challenging due to the need for cost-effective and timely analytical methods that can assure security integrity. High-level security standards for solutions that cover airborne, space, and ground-based systems in the net-centric aviation system are needed. These standards should be defined such that they do not add unnecessary cost nor open additional exploitable vulnerabilities.

ADAPTIVE THREAT MONITORING AND EVALUATION

The ability to match the need for the right information at the right time with an appropriate level of assurance controls will be a key challenge. The dynamic operational environment of the net-centric aviation system may require the tightening or loosening of these controls based on the type of events and threats. The risks posed by cyber threats will evolve over time

and therefore the security model to measure and assess the evolving threat impact and risks will need to be adaptive. Security planners will be needed to adjust the security models to minimise risk and simultaneously support and enable an active and prosperous air commerce industry. As highlighted earlier, threat information sharing between stakeholders will be critical and this requires the establishment of multi-stakeholder trust partnerships and forums.

THREAT MITIGATION STRATEGY

Mitigations should be established for every conceivable cyber and physical threat that will have a significant impact on the net-centric aviation system. The measures will need to be sufficient to reduce the risk associated with the threat and allow the risk to be rated as minimal. An acceptable risk level is determined by the potential impact; for example, a threat that results in a catastrophic impact must be an extremely improbable security risk.

Cyber threat mitigations may be specified as a requirement to be implemented and they may also be stated as a dependency in the net-centric aviation system. Such dependencies must be clearly identified and communicated clearly to the entities responsible for implementing them.

THREAT RESPONSE STRATEGY

Mechanisms consisting of rules, procedures and processes are needed for guiding responses to detected threats and unanticipated security failures that create unacceptable risks in the net-centric aviation system.

INFORMATION SHARING AND HANDLING

Within a ‘system of systems’ environment, such as ATM, that involves a number of actors, it is important to establish an appropriate information sharing protocol, which will allow stakeholders to commit to sharing information and intelligence openly, yet securely, to increase overall situational awareness of the cyber threat within ATM.

A framework (commonly known as the Traffic Light Protocol/TLP) for marking information assets is presented in Table 4⁴, the use of which will enable stakeholders to understand their responsibilities when handling information; the originator is responsible for assigning an appropriate level of classification to the information. It is recommended that one of the four Information Handling Levels is assigned to every piece of information shared within a community of stakeholders:





INFORMATION HANDLING LEVEL	DESCRIPTION
 RED	Personal for named recipients only: in the context of a meeting, for example, red information is limited to those present at the meeting. In most circumstances, red information will be passed verbally or in person.
 AMBER	Limited distribution: the recipient may share amber information with others within their organisation, but only on a ‘need-to-know’ basis. The originator may be expected to specify the intended limits of that sharing.
 GREEN	Community wide: information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside the community.
 WHITE	Unlimited: subject to standard copyright rules. White information may be distributed freely outside the community without restriction.

Table 4 – Traffic Light Protocol Framework

4 TLP as defined by the UK Centre for Protection of National Infrastructure (CPNI) – <https://www.cpni.gov.uk/terms-conditions>

APPENDIX B – LISTS OF POTENTIAL THREATS AND IMPACTS

THREAT – Any circumstance or event with the potential to adversely impact organisational operations, assets or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

THREAT	DEFINITION
Botnet	A network of hijacked computer devices used to carry out scams and cyberattacks.
Brute Force	An attack using excessive forceful attempts to guess login information, encryption keys, or find a hidden web page.
Cross-site Scripting (XSS)	The use of third-party web resources to run scripts on a victim's system. The attacker injects a payload onto a vulnerable webserver, which then harvests user data or steals their session to take over their account.
Data Exfiltration	A technique used by malicious actors to target, copy, and transfer sensitive data. Data exfiltration can be done remotely or manually. See data leakage.
Data leakage	The unauthorised transmission of data from within an organisation to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. See Data Exfiltration.
Denial of Service	An attack which floods the target with traffic or sending it information that triggers a crash; the intention being to shut down a machine or network, making it inaccessible to its intended users.
Espionage (or cyber spying)	A form of cyber-attack carried out against a competitive company or government entity with the goal of providing the attacker with information that gives them advantages over competing companies or governments.
Hacking	The act of compromising digital devices and networks through unauthorised access to an account or computer system.
Insider Threat	Threats posed by individuals from within an organisation, such as current or former employees, contractors and partners.
Malware	Any type of malicious software designed to harm or exploit any programmable device, service or network.
Man-in-the-middle	An attack where the malicious actor is positioned in a conversation between a user and an application, either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.
Malicious Payload	An attack component responsible for executing an activity to harm the target. Examples include worms and ransomware.
Nation State actors	Actors that may be part of a state apparatus or receive direction, funding, or technical assistance from a nation-state.
Phishing	A type of social engineering attack often used to steal user data such as login credentials or credit card numbers.
Ransomware	A form of malware that attempts to encrypt data and then extort a ransom to release an unlock code.
SQL Injection	A web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database, generally allowing the attacker to view data that they are not normally able to retrieve.
Virus	A type of malicious software, or malware, that spreads between computers and causes damage to data and software.
Worm	A type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction and does not need to attach itself to a software program to cause damage.

IMPACT – The undesired outcome of a defined threat should it be allowed to propagate to its ultimate extent.

IMPACT	DEFINITION
ATC Systems	Systems used operationally in the provision of Air Traffic Control (ATC) services are impacted in one or more of Confidentiality, Integrity and Availability. The consequence is a total or partial loss of a system, or the loss of trust in the system or supporting data upon which the Air Traffic Controller is basing their decisions. This will result in limits placed upon the provision of ATC services, delays to aircraft and financial loss for the company. A worst-case scenario could see damage to or loss of aircraft though this would likely require other safeguards, both human and technical to have also been breached.
Corporate systems	Systems used by the company to support its activities including those dealing with emails, personal and financial data are impacted in one or more of CIA. The consequence is the loss of data related to company employees, third party employees or customers which in turn puts the company at risk of legal and regulatory action depending upon the legal framework within which the company operates.
Physical infrastructure systems	Physical infrastructure used by the company to house and support its activities is impacted by an attack. Such infrastructure includes physical access control systems and Heating, Ventilation, and Air Conditioning (HVAC), many of which have some degree of internet and electronic connectivity. The impact is that parts of the business are unable to operate, for example due to an inability for staff to access the buildings or through excessive heat due to inoperative air-conditioning systems.
Reputation	A publicised cyber-security incident or a disclosure of a vulnerability within the company systems results in the reputation of the company as a reliable and trustworthy entity being damaged, or the travelling public having reduced confidence in it as a provider of ATC services.
Third party	Risk of disruption caused by a compromise of systems and services delivered by or connected to third parties such as contractors or other ATC companies. In such a situation there is the possibility of legal and regulatory action depending upon the legal framework within which the company operates, or a loss of external business contracts.

Table 5 – Lists of Potential Threats and Impacts

APPENDIX D – GLOSSARY

ABBREVIATIONS

ACARS	Aircraft Communications Addressing and Reporting System
ANSP	Air Navigation Service Provider
APT	Advanced Persistent Threat
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
CANSO	Civil Air Navigation Services Organisation
CCTV	Closed Circuit Television
CD	Compact Disc
CIA	Confidentiality, Integrity, Availability
CNI	Critical National Infrastructure
COM	Communication
CPDLC	Controller Pilot Data Link Communication
CSTF	Cyber Safety Task Force
CVSS	Common Vulnerability Scoring System
DB	Database
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of Service
DVD	Digital Versatile Disc
ERP	Emergency Response Plan
GND	Ground
HVAC	Heating Ventilation & Air Conditioning
IP	Internet Protocol
ISMS	Information Security Management System
SeMS	Security Management System
TLP	Traffic Light Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
XXS	Cross Site Scripting

Table 6 – Abbreviations



CANSO



canso.org

