canso
civil air navigation services organisation

CANSO Cyber Security and Risk Assessment Guide

Published June 2014

Contents

Purpose of this document

The purpose of this document is to provide air navigation service providers with an introduction to cyber security in air traffic management, including the cyber threats and risks and motives of threat actors, as well as some considerations to managing cyber risks and implementing a cyber security programme. The appendices include information on standards and a framework for cyber security, and some practical guidance to conducting a cyber risk assessment – a recommended first step to understanding and managing the cyber security risks to systems, assets, data and capabilities in ATM.

1
Introduction

The current trend in air traffic management (ATM), both at the international level as well as within individual air navigation service providers (ANSPs), is toward increased sharing of information and creating a common situational awareness for a wide spectrum of aviation stakeholders. While this enhances the efficiency of operations and raises productivity, it also opens up the potential for cyber attack. And, the vulnerabilities are only growing because current and next generation systems, like NextGen and SESAR, demand more information sharing through increased use of commercially available information technology, shared network and computing infrastructures, and network-centric architectures and operations.

Unlike in the past, information sharing in the future ATM system will not be limited to point-to-point communications, it will also utilise open systems architecture and internet-based flow of information. We are seeing a trend towards increased use of existing technologies, growing interoperability among systems, and use of automation to improve productivity.

This trend is not unique to ATM; most industries are applying information technology to improve the efficiency of existing operations as well as to enable new modes of operation. Benefits are achieved by allowing information to be rapidly shared among humans and systems, wherever and whenever it is needed. Unfortunately, these benefits come with risks. Increased use of information technology means greater exposure to cyber attack. The threat is both very real and very serious. ANSPs must develop and execute security strategies and plans to ensure continued mission operations despite this threat. If we are to transform global ATM performance and achieve safe, efficient, and seamless airspace globally, the global ATM system must meet clear security requirements and expectations. The Global Air Traffic Management Operational Concept (ICAO Doc. 9854) speaks to this and defines the security expectation of an integrated, interoperable and globally harmonised ATM system as:

"…the protection against threats that stem from intentional acts (e.g. terrorism) or unintentional acts (e.g. human error, natural disaster) affecting aircraft, people or installations on the ground. Adequate security is a major expectation of the ATM community and of citizens. The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats. Security risk management should balance the needs of the members of the ATM community that require access to the system, with the need to protect the ATM system. In the event of threats to aircraft or threats using aircraft, ATM shall provide the authorities responsible with appropriate assistance and information."

2
Cyber Threats and Risks

The US Department of Homeland Security has defined a cyber threat as *"any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority."*

A cyber threat can be intentional or unintentional, targeted or non-targeted, and can come from a variety of sources, including: foreign nations engaged in espionage and information warfare; criminals; hackers; virus writers; and disgruntled employees and contractors working within an organisation.

Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures and equipment failures that inadvertently disrupt computer systems or corrupt data.

Intentional 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.

Repeatedly identified as the most worrisome threat is the "insider" – someone who has authorised and legitimate access to a system or network. Other malefactors may make use of insiders, such as organised crime or a terrorist group suborning a willing insider (a disgruntled employee, for example), or making use of an unwitting insider (by getting someone with authorised network access to insert a disk containing hidden code, for example). However, insider threats can be guarded against and deterred by organisational (a policy, for example), logical (authentication, for example) and physical (restricted proximity card access, for example) controls.

It is important to note that a threat can be a combination of a cyber and physical attack, for example, a physical intrusion into a ground infrastructure and a modification of the software code hosted in the infrastructure. This would be an intentional cyber and physical attack. Or, when authorised personnel do not follow procedure to check the infrastructure, and the infrastructure generates and transmits misleading data. This is both a cyber and unintentional physical attack.

3
Motives and Methods

The motivation of intentional actions in attacks may emerge from a variety of sources – a foreign State or terrorist, criminal, or social-issue organisations. Threat agents performing such intentional actions may be unauthorised entities or insiders, and their primary objective is to engineer potential hazards and performance losses in the net-centric aviation system.

Potential attackers span a wide range of abilities, resources, and motives. At the bottom of the scale are the traditional hackers who hone their skills and claim "bragging rights" by vandalising easy targets. Attackers in this group have limited expertise and resources. They are not typically focused on any specific target; they will attempt to compromise any vulnerable systems that can be reached via the Internet. The result of attacks at this level may be limited or may have serious effects far beyond those intended by the hackers. Defences at this level are focused on establishing a perimeter around an organisation's information system infrastructure, and defending that perimeter using firewalls and other commercially available tools.

At the next level are cyber thieves who attempt to acquire critical information – anything from credit card numbers to proprietary business plans. Defences at this level include protecting information and systems not just at the perimeter but wherever it resides within the enterprise, using techniques such as hard drive encryption.

The third level is cyber surveillance, in which attackers seek to obtain a foot hold within an organisation and execute subsequent higher-level attacks on their own timetable. Attackers

at this level will have moderate expertise, and may launch multiple attacks targeting particular organisations. The consequences for ANSPs of attacks at this level and above may be quite serious, ranging from loss of proprietary information to partial or total failures of air traffic management services, whether as an intended or unintended consequence of the attack. Defence at this level requires continuous internal monitoring and system hardening throughout the enterprise.

At the fourth level are cyber espionage units – sophisticated adversaries capable of mounting multiple coordinated attacks aimed at establishing a persistent foot hold within an organisation's infrastructure, which may be used to exfiltrate sensitive information or plant capabilities to disable or disrupt systems. Defence at this level requires an enterprise architecture that can impede an attacker's actions within the organisation's information system infrastructure and ensure continuity of critical mission operations.

At the fifth level is cyber warfare. Attackers at this highest level are very sophisticated, and have the resources for continuous, coordinated attacks. Defence at this level requires agility, adaptation, and flexibility to dynamically reshape operations and maintain mission continuity even while under continuous attack.

There has been a general increase in the capability of the information security attacker due to the support from States and criminal organisations in this low risk, high return environment. This capability is rapidly finding its way into the hands of traditionally less capable cyber attackers, 'hacktivists' – those who deliberately interfere with online data and services in order to bring attention to a political or ideological cause.

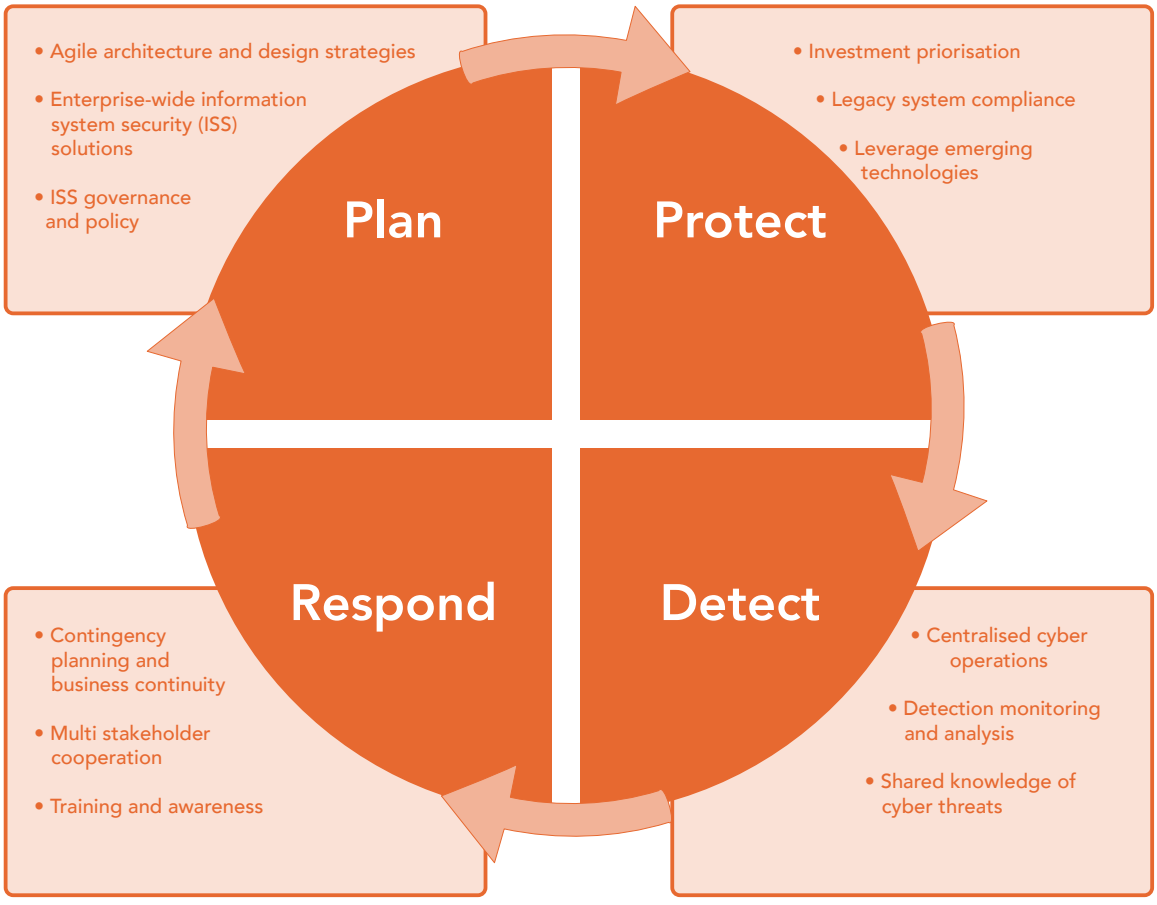
The range of threats is so broad, and the sophistication and resources available to attackers at the top of the scale are so great that this problem cannot be addressed with a single solution, nor can it be addressed only at a single point in time. The tools, tactics, and strategies of attackers at all levels are readily available and will continue to evolve, and the threat will continue to increase. It would be naive to believe that the proliferation of these tools can be controlled through legislation or regulations. Responding effectively to the threat will require a long-term commitment from senior leadership to an ongoing process of building and operating increasing levels of information system security capabilities.

To help organise efforts for responding to the cyber threat, most relevant international standards suggest applying an approach that divides the ongoing security process into four complementary areas: plan, protect, detect, and respond. See the diagram below.

The Plan quadrant includes the creation of design strategies and an enterprise-wide or overall system-of-systems architecture that enhances security, provides agility, and reduces overall costs. To effectively implement the architecture, organisations must develop policy and fund security solutions throughout the enterprise with total management commitment.

The Protect quadrant includes prioritising information security investments in both new and legacy systems. Protection techniques must be agile; that is, they must be able to quickly change and adapt to an ever-changing threat. This requires the organisation to leverage emerging technologies and implement them at an enterprise-wide level. While some aspects of security must be built into individual systems, enterprise solutions can be shared throughout an organisation and are a key underlying element of an effective architecture. Enterprise security solutions reduce overall costs and, just as importantly, make it possible for new and evolving threats to be addressed centrally rather than having to introduce new measures into every part of the system. The success of any information technology (IT) security programme is, in part, dependent on the ability to detect and respond to a cyber security event.

A model for effective cyber security



The need for the next two quadrants – Detect and Respond – reflects the unfortunate reality that no matter how much planning and protection is put in place, failures will occur and determined attackers will gain access to protected systems. This fact does not minimise the need for good architecture design and investment, both of which reduce the susceptibility to compromise. Adequate intrusion-detection capability is required to monitor and detect potential cyber security incidents at ATC facilities. Detection requires a centralised cyber security operations centre (SOC) staffed by experts with up-to-date knowledge of the evolving cyber threat. The SOC must be supported by analysis tools fed by intrusion monitoring sensors installed throughout the enterprise, which provide the ability to detect when an organisation's information system has been compromised.

The Response quadrant includes contingency planning, procedures, and training and awareness, which allow an organisation to quickly and effectively respond to a compromise and minimise the possible impact on mission operations. Cyber security content is almost non-existent in the curriculum of current training programmes, and what might be needed in regards to cyber security knowledge, skills, and abilities of ATCOs, engineers, technicians, and other staff needs to be identified. The combination of detection and response provide the organisation with an ability to know when cyber compromise is a problem, and assist the organisation in executing cyber procedures to ensure the operational mission is fulfilled (although perhaps degraded) throughout an attack. On the other hand, the "response" action also requires an appropriate evaluation of lessons learned to prevent any re-occurrence and thus promote a cycle of continuous improvement through each of the four quadrants.

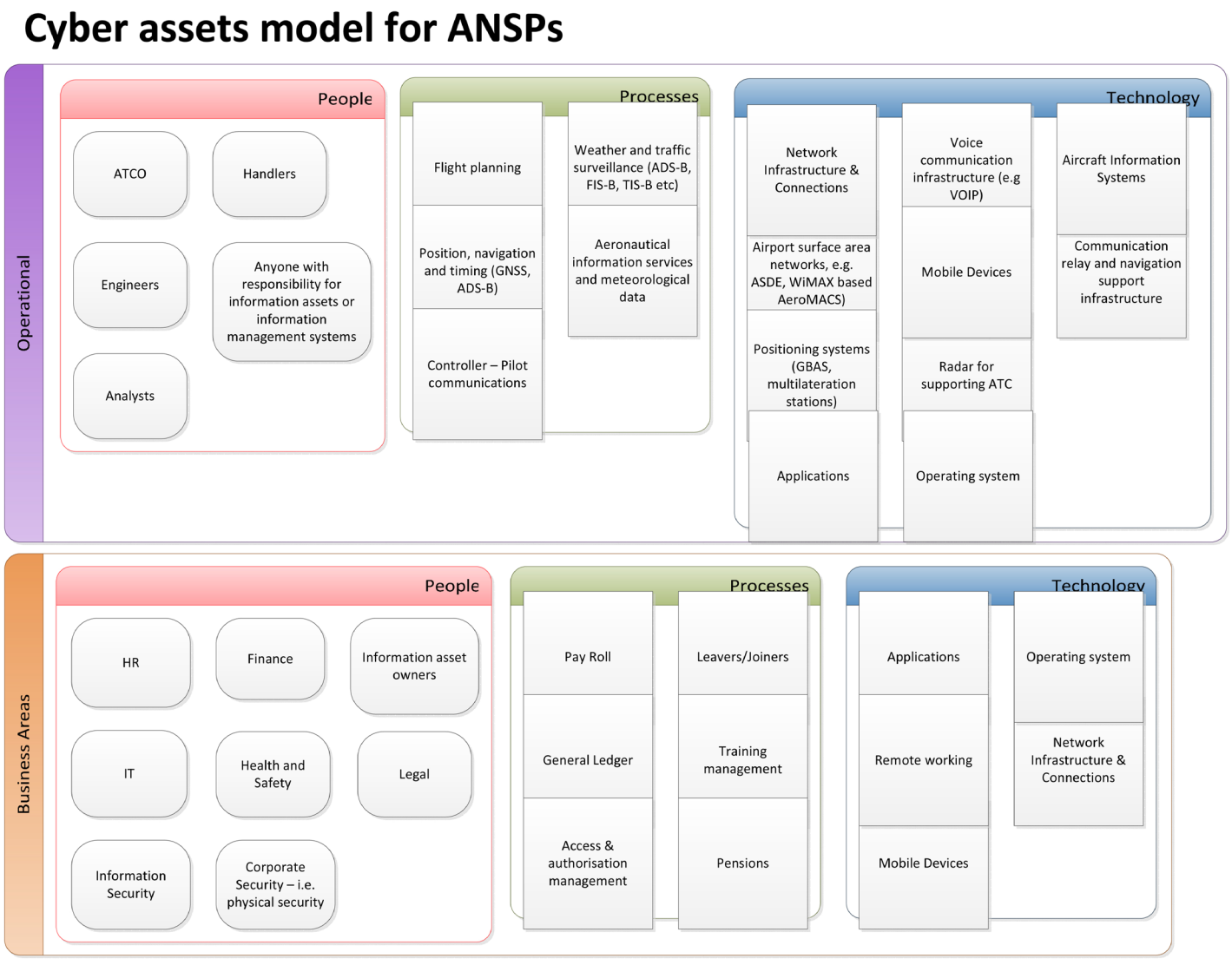
Past experience is not the best predictor of current and future cyber security threats. As new systems like NextGen and SESAR are designed, implemented, and operated, increasing vulnerabilities to the cyber threat must be mitigated. It is essential that ANSPs (individually and collectively) make cyber security a top priority, and that they work together to ensure a secure global air transportation system. Cyber security is not a choice but a requirement.

4
Cyber Assets

There are a number of assets, or components of the aviation system that need to be protected from threats and from becoming a threat.

The cyber assets diagram provides examples of people, processes and technology that you would find within an ANSP, split into operational areas (engineering, operations, air traffic control etc.) and other business areas (legal, finance, HR, etc.). It is important to note that this is not an exhaustive list, but rather an example of some of the key assets involved in the day to day operation of an ANSP.

In the context of applying an information security management system (ISMS) or a cyber security framework, it is often useful to use a profile as a guideline. All organisations face industry-specific risks and issues and it is often not clear from a standard or framework how the controls should be implemented to cover industry specific processes or technology. For example, protective monitoring and physical access control are two controls that are often part of cyber security standards or frameworks. However, while these are beneficial to larger organisations, the cost would be prohibitive for smaller businesses with only marginal benefits. Smaller businesses would be better off if they identified their biggest



risks and invested in a reliable anti-malware platform and email cleaner and ensured that their premises were physically secured, rather than rely on expensive logical controls. This emphasis on prioritisation is one of the key drivers behind using a profile to implement a framework across a wide range of organisations.

The cyber assets diagram would be used as part of an ANSP specific profile for the application of an ISMS. An ANSP specific profile would therefore have two primary benefits to the ATM community: it could be used by any ANSP as a guide on where and how to apply ISMS controls within the context of their organisation; and it would provide a reference document for an auditor on where to look for key ISMS or framework controls within an ANSP and how they should be applied.

Not all of the assets in the diagram would necessarily need to be covered by the scope of an ISMS, but a profile would be able to highlight which areas of the organisation would need to be included in an ISMS and could give an indication of what controls should be considered for securing those assets. A profile could also include an indication of sample maturity levels so organisations could gauge their own progress towards fully implementing an ISMS or framework.

The control domains of an ISMS (ISO 27001) or a security framework (National Institute of Standards and Technology's (NIST) Cybersecurity Framework) are provided as reference within Appendix A and are recommended for use when creating profiles and in the application of controls.

The cyber assets outlined in the diagram on the previous page are described in more detail below. They are split into three key areas – Data and Information; Information Systems; and Physical Assets.

Data and information

In a net-centric environment, data and information are prime assets which need to be protected, as well as the networks and technology handling the data and information. These include:

- Flight operational and planning data: examples include aircraft trajectory, RNP data, and ACARS messages on air-ground communications
- Weather and traffic surveillance data: examples include ADS-B-In, FIS-B, TIS-B, aircraft weather sensor data shared on air-ground and air-air communications
- Position, navigation and timing data: examples include GNSS, ADS-B-Out
- Aeronautical information services and meteorological data: examples include real-time updates on meteorological conditions and airport conditions; emergencies and restrictions that limit airspace use during flight
- Controller-pilot automated messages and voice communications: examples include the two-way communications that replace voice communications with data link of automated messages and receipts
- Aircraft status data: examples include cabin and flight deck video for airspace security
- Airport surface area communications: examples include airport surface area operations data
- Security relevant data: examples include digital certificates, keys, credentials, and passwords

Information systems

The systems that collect, filter, process, create, store and distribute data and information are also prime assets susceptible to the cyber

threat. This includes software, network protocols, computing algorithms, media storage used in the following infrastructures:

- Large-scale information sharing infrastructure: information sharing between multiple users and applications for worldwide collaboration for aviation tasks. Examples include:
  - aeronautical-specific infrastructure such as SWIM, ISDN
  - public infrastructures such as cloud computing and Internet.
- Voice communication infrastructure: transition from analogue to digital voice and an intelligent voice switching system over Internet, i.e. Voice over IP (VOIP)
- Air navigation support infrastructure: deployed extensively for air-ground communications and passive/active monitoring and tracking of aircraft positions.
  - ground-based transponders for air-ground communications
  - positioning systems (e.g., GBAS, multilateration stations) and radars for supporting air traffic control
  - satellites as communication relay and navigation support infrastructure
  - airport surface area network (e.g., ASDE, WiMAX based AeroMACS).
- Aircraft information systems: networked platforms of aircraft, embedded and crew carried.

Physical assets

A number of physical assets also pose a threat to the aviation system. These include:

- manned and unmanned aircraft, and their payload (i.e., passengers, baggage and cargo)
- devices brought onboard aircraft, including passenger-owned devices and crew-operated mobile devices
- networking and information technology infrastructure (e.g., radar, ground stations, satellites)
- airport information infrastructure
- organisations responsible for information assets and information management systems
- individual persons, employed by organisations, who are authorised and responsible to carry out operations and procedures that involve information assets and information management systems

5
Cyber Security in ATM

Within the context of the Convention on International Civil Aviation (ICAO Doc. 7300, or the "Chicago Convention"), air navigation services are provided as part of a State obligation and States must safeguard essential national security or defence policy interests and in many cases must meet certain legal requirements, obligations and specific procedures regarding critical infrastructure protection. Of paramount importance to cyber security in ATM is data integrity and information assurance. Thus, it is important to understand the requirements for data and information assurance as well as the measures and strategies that can be taken in this regard.

Information assurance requirements

- 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: assures that aviation information is not modified by unauthorised entities or through unauthorised processes. Integrity supports the assurance that aviation information is not accidentally or maliciously manipulated, altered, or corrupted. Integrity also means that detection occurs with no or minimal false alarms when information has been altered; the alteration source must be identifiable.
- Availability: assures timely, reliable, 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 possess appropriate permission and privilege.
- Non-repudiation: assurance that the data sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, assuring that sender and receiver processing of the data.
- Traceability: all actions performed on each asset must be logged in a format and for a time period that can satisfy both regulatory and consumer needs.

Enterprise systems, wireless, and 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 detection of spoofing, and regulations and criminal statutes need to be in place to deter spoofing and other such threats. Spoofing is where a person or programme successfully masquerades as another by falsifying data and thereby gaining illegitimate access,

usually due to lack of authentication mechanisms for identity verification.

Mitigating physical attacks on cyber assets

Methods to prevent or detect adverse human actions, physical destruction or sabotage of networking and information technology infrastructure of cyber, radio frequency (RF) jamming, etc. The physical methods used to defeat physical attacks targeted at cyber assets can include physical access control to systems; physical checks and processes; detection of abnormal and unauthorised sources of RF energy; and aircraft security, which is dependent on the security of the connections to the ground and airborne and satellite systems.

This also means that 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.

Cross-correlations between physical and information security allow one to understand events that, individually considered, are meaningless, but could be of significance if related and properly analysed.

Cyber security 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.

Aircraft operators are assumed to operate correctly, reliably managing software configuration and other digital content important for the secure operation of their fleet in the net-centric ecosystem. Air traffic controllers and pilots are trusted with various air traffic control tasks, including protecting their credentials against misuse.

Cyber security solution strategies

The security architecture must be developed to identify points of unauthorised entry, vulnerabilities, and mitigations. An end-to-end security architecture is required as multiple stakeholders are involved in information sharing. 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, due to 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. In order to implement effective cyber security 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. And, 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 the right information 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. Risk from cyber threats will evolve over time. Hence, the security model to measure and assess the evolving threat impact and risks will need to be adaptive. Security planners will be required to adjust the security models to minimise risk, yet enable air commerce. Again, threat information sharing between stakeholders will be critical, which requires the establishment of multi-stakeholder trust partnerships and forums.

Threat mitigation strategy

Mitigations for every conceivable cyber and physical threat that will have a significant impact on the net-centric aviation system need to be established. The mitigating measures must be sufficient to make the threat somewhat unlikely or implausible with minimal risk. 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 must be promulgated to the entities responsible for implementing them, for example by way of guidance or as instructions.

Threat response strategy

Mechanisms are needed for responding to detected threats and unanticipated security failures that create unacceptable risks in the net-centric aviation system. And, the rules, procedures, processes that respond to unanticipated or detected security events in the 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.

Through this, a common framework for marking information assets is outlined below to enable stakeholders to understand their responsibilities when handling information. The originator should assign an appropriate level of classification for information, having a common glossary and a common term of reference to understand the relevance of information managed. One of the possible ways to classify information is to give one of four Information Handling Levels 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.

6
Managing Cyber Risks

ANSP management needs to be able to assess the impact of security and the lack of security on the net-centric aviation system performance. This includes performing cost-benefit analysis due to the introduction or the absence of security functions. Suitable policies, procedures and processes need to be determined. Detection mechanisms need to be put in place to identify the presence of a threat and decision support tools are needed for threat evaluation and mitigation. An approach is needed that uses standardised mitigations and scopes each threat to a minimum risk manageable, based on established policies, rules, processes and procedures.

Assessing the risks to ATM systems

A robust risk assessment methodology is required to ensure all vulnerabilities are identified for each ATM system and the required properties of the data it processes in terms of the three most important data assurance requirements: confidentiality; integrity; and availability.

Risk assessment involves defining the scope and identifying the assets that are potentially at risk. A thorough analysis and evaluation of risks is then conducted, and the necessary controls put in place to reduce the risk to manageable or acceptable levels. A generic risk assessment methodology is explained in greater detail in Appendix B.

The risks to ATM can be managed by first identifying the overall systems in a functional unit and the associated risks, e.g. LAN, computers, HVAC, WAN connection, radio systems, etc. For generic ATM systems, threats will exploit the vulnerabilities to create a risk, and the level of this risk will be unique to each ANSP and business unit, e.g. an IT system for business support would not be provisioned unless required for the business function, but the integrity and availability of data for operational systems will be higher than other business areas. It is therefore important to understand the threats and vulnerabilities, and examples are provided in Appendix B.

7
Conclusions and Recommendations

Cyber security as a part of ATM Security and, more generally, of overall aviation security

Cyber security receives specific consideration in the general legal framework contained in Annex 17 – Security to the Chicago Convention, which recommends that "each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation." The Aviation Security Manual (Doc 8973 – Restricted) and the Air Traffic Management Security Manual (Doc. 9985 - Restricted) provide guidance on how to apply the Standards and Recommended Practices (SARPs) contained in Annex 17. The importance of air traffic management to the aviation security process is evidenced by recent amendments to Annex 17 that include measures relating to cyber threats and oblige States to ensure protection to infrastructures and facilities and to harmonise security programmes into the national legal framework.

Society expects a high standard of aviation safety and security and the level of security performance will determine society's confidence in air transport. The lack of a high level of security performance would impact the reputation of aviation stakeholders and thus, influence customer perception and choice.

The performance of the future ATM system must therefore contribute to ensuring a high level of security to be achieved by the aviation industry as a whole. Expectations are that this can be achieved not only by ensuring that the infrastructure which makes up the ATM system is itself resilient to attack, but also that the system will provide information that can be used by other organisations to act and protect air transport and the aviation system as a whole.

Risk assessment

ANSPs should conduct a risk assessment to determine the greatest risks to the organisation and business, and should consider assessing the adequacy of their cyber security controls against a recognised standard or framework. This assessment can be scoped against a subset of controls or against a profile that matches an ANSP's business environment and needs.

The NIST Cybersecurity Framework is one of the standards available and provides a common taxonomy and mechanism, primarily focussed towards organisations that provide critical national infrastructure, to:

1. Describe their current cyber security posture
2. Describe their target state for cyber security
3. Identify and prioritise opportunities for improvement within the context of a continuous and repeatable process
4. Assess progress toward the target state
5. Communicate among internal and external stakeholders about cyber security risk

As part of the process, threats and vulnerabilities to the organisation will be documented and control gaps will be identified for areas that have insufficient or ineffective controls to mitigate assessed risks. Guidance on how to conduct a risk assessment is provided in Appendix B.

Cyber security as part of an enterprise-wide approach

As cyber attacks grow in intensity and become increasingly sophisticated, changing constantly in response to the defensive systems they encounter, it will become necessary to adopt an approach to cybersecurity that is proactive, dynamic, and adaptive, evolving beyond the

realm of traditional IT management. It will need to be of concern to the ANSP board and senior management where cyber issues can be addressed from the perspective of enterprise risk management, thereby enabling the organisation to adopt an approach that incorporates a wide range of integrated cyber security activities to understand and mitigate enterprise risks.

Security management system

A security management system (SeMS) sets out the organisation's security policies as an integral part of its business processes, and is based on the same concepts used for a safety management system (SMS). It provides an organisation-wide approach to security through the development of a security culture as well as a system-wide security model that encourages close cooperation between all relevant stakeholders, both within and outside the organisation. Developed in conjunction with an efficient threat assessment mechanism and risk management programme, SeMS helps the organisation develop proactive, efficient and cost-effective security measures. The cyber security programme should fit within this overall framework of a SeMS.

Leadership and governance

Effective leadership and governance helps ensure that cyber security supports business goals, optimises business investment in cyber security, and appropriately manages cyber security related risks and opportunities.

To exercise effective cyber security governance, ANSP boards and senior management must have a clear understanding of the cyber security vulnerabilities and what to expect from their cyber security programme. They need to know how to direct the implementation of an information security programme, how to evaluate their own status with regard to an existing security programme, and how to decide the strategy and objectives of an effective security programme. Use of a framework, such as NIST's, may assist leadership in identifying areas of weakness and enable objectives to be created.

Duties and responsibilities

Information security is not only a matter for information technology staff but it is an organisational concern as well. Security controls need to be in place to safeguard an information system from attacks against the confidentiality, integrity, and availability of computer systems, networks and the data they use. And the security controls that are selected and applied must be based on a risk assessment of the information system. As such controls can restrict the power or influence held by any one individual, a proper separation of duties must be designed to ensure that individuals do not have conflicting responsibilities. Separation of duties in IT security is now considered a best practice to prevent potential conflicts of interest in the organisation. Conflicts of interest might include a situation in which the IT department decides and applies, on its own, policy and procedures without third-party assessment and evaluation.

The security department can be requested to act as an independent party to provide advice, audit systems and processes without having a direct role in operation. Security managers should, on the other hand, be skilled, prepared and provided with the appropriate resources, authority and power to act in a decisive manner, by either imposing security requirements for a new project or existing technologies, or by enforcing procedures and policies that have been adopted at the executive level of the organisation.

Security culture

The commitment of people to protecting their organisation is an essential component of a strong cyber defence. This means a critical part of the cyber security programme must be to focus on the human aspects of the organisation – on

developing a positive security culture that is grounded in employees' attitudes, evident in the behaviours people exhibit and which is reinforced by the actions of leaders.

It is therefore important that management take their information security responsibilities seriously, support the information security policies and act as a role model for the employees they manage. Management responsibilities should include information security tasks to reflect this.

Training and awareness

Similarly, training is a critical element of security as employees need to understand the value of sensitive information and their role in keeping it safe. Employees need to know the policies and practices they are expected to follow in the workplace regarding cyber security.

ANSPs should implement an annual training programme that enables users to understand their security responsibilities and the procedures they need to follow while working within the organisation, handling sensitive information. The training programme should be reviewed annually to ensure it is current and incorporates the latest cyber security intelligence.

As a minimum, the security training programme should include guidance on:

- their legislative and regulatory responsibilities for the information they process e.g. data protection
- how to handle protectively marked information assets and their personal responsibility to ensure secure processing of information e.g. storing and transferring
- mechanisms they can use to report an incident in the event of an actual or suspected security breach

Monitoring and reporting

Adequate logs enable post-incident investigations and support disciplinary action and/or prosecution in the event of a security breach. ANSPs should take measures to ensure that logging is enabled for key operational and business systems and monitored using technology, e.g. a security information and event management (SIEM) tool such as HP ArcSight, IBM Q1 Labs, Splunk, or LogRhythm, and through regular audit.

Updates through reports and management information should be produced and provided to senior management on a regular basis.

Industry collaboration and information sharing

The sharing of information between ANSPs of known or potential cyber security threats and vulnerabilities can play a vital part in strengthening our overall response to incidents and their prevention.

Generation of an information sharing protocol provides a means by which information sharing and handling, confidentiality, liability and appropriate behaviour are established and managed by the stakeholders involved.

Appendix A

International Standards

This appendix gives further details about the ISO 27000 series of standards and other security frameworks as follows:

- A.1. Description of each of the standards ISO 27001 to ISO 27006
- A.2. ISO 27005 standard that provides guidelines for information security risk management (ISRM)
- A.3. Cybersecurity Framework of the US Commerce Department's National Institute of Standards and Technology (NIST).

A.1. ISO 27000 series of standards

The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.

The ISO 27001 standard, originally published in October 2005, provides the specification for an information security management system (ISMS). The objective of the standard is to "provide requirements for establishing, implementing, maintaining and continuously improving an ISMS". Regarding its adoption, this should be a strategic decision and is influenced by an organisation's needs and objectives, security requirements, the organisational processes used and the size and structure of the organisation. While the 2005 version of the standard heavily employed the Plan-Do-Check-Act (PDCA) model to structure the processes, the latest 2013 version places more emphasis on measuring and evaluating how well an organisation's ISMS is performing.

The ISO 27002 standard, also published in 2005, provides a code of practice for information security and outlines the potential controls and control mechanisms, which may be implemented, subject to the guidance provided within ISO 27001. The two documents are intended to be used together, with one complementing the other. The ISO 27002 standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation". The actual controls listed in the standard are intended to address the specific requirements identified through a formal risk assessment. The standard is also intended to provide a guide for the development of "organisational security standards and effective security management practices and to help build confidence in inter-organisational activities". A new version published in 2013 contains 114 controls, as opposed to the 133 documented within the 2005 version.

ISO 27001 - *Information technology — Security techniques — Information security management systems — Requirements*	**ISO 27002** - *Information technology — Security techniques — Code of practice for information security management*
ISO 27003 - *Information Technology — Security techniques — Information security management system implementation guidance*	**ISO 27004** - *Information technology — Security techniques — Information security management — Measurement*
ISO 27005 - *Information technology — Security techniques — Information security risk management.*	**ISO 27006** - *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

A.2. ISO 27005 – Information security risk management (ISRM)

The ISO 27005 standard provides guidelines for information security risk management (ISRM) in an organisation, specifically supporting the requirements of an information security management system defined by ISO 27001. The ISO 27005 standard does not provide or recommend a specific methodology, but provides an overview of the ISRM process including risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

The *SESAR ATM Security Risk Assessment Method* – Draft Edition 00.02 dated 20 December 2012, provides a sample threat list of deliberate actions that is based on ISO 27005:

Loss of essential services	Failure of air-conditioning
	Loss of power supply
	Failure of telecommunication equipment
Disturbance due to radiation	Electromagnetic radiation
	Thermal radiation
	Electromagnetic pulses
Compromise of information	Interception of compromising interference signals
	Remote spying
	Eavesdropping
	Theft of media or documents
	Theft of equipment
	Retrieval of recycled or discarded media
	Disclosure
	Data from untrustworthy sources
	Tampering with hardware
	Tampering with software
	Position detection
Technical failure	Saturation of the information system
	Breach of information system maintainability
Unauthorised action	Unauthorised use of equipment
	Fraudulent copying of software
	Use of counterfeit or copied software
	Corruption of data
	Illegal processing of data
Compromise of functions	Abuse of rights
	Forging of rights
	Denial of actions
	Breach of personnel availability

A.3. NIST Cybersecurity Framework

The *Framework for Improving Critical Infrastructure Cybersecurity* was drafted by the US Commerce Department's National Institute of Standards and Technology (NIST), and was released in February 2014. It does not introduce any new standards or concepts but rather it leverages existing cyber security practices that have been developed and refined by other organisations, not limited to but including the International Organization for Standardization (ISO).

The framework itself comprises a risk-based compilation of guidelines that can help organisations identify, implement, and improve cyber security practices, and creates a common taxonomy for internal and external communication of cyber security issues, as well as an assessment mechanism which enables organisations to determine their current cyber security capabilities, a target 'state', and a plan for improving and maintaining their cyber security capabilities. The framework is also an iterative model that is designed to evolve and adapt with changes in the cyber security threat landscape, including new processes and technologies – it is therefore well suited to the ATM industry.

The framework assessment mechanism contains three key elements: Core; Implementation Tiers; and Profile. The Framework Core defines standardised cyber security activities, desired outcomes, and applicable references, and comprises five Functions that can be performed concurrently and continuously: Identify, Protect, Detect, Respond, and Recover. The Framework Core, in effect, describes the continuous cycle of business processes that constitute effective cyber security.

Function	Description	Category
Identify	An understanding of how to manage cyber security risks to systems, assets, data and capabilities	Asset management
		Business environment
		Governance
		Risk assessment
		Risk management strategy
Protect	The controls and safeguards necessary to protect or deter cyber security threats	Access control
		Awareness and training
		Data security
		Information protection processes and protocols
		Maintenance
Detect	The controls and safeguards necessary to protect or deter cyber security threats	Anomalies and events
		Security continuous monitoring
		Detection processes
Respond	Incident response activities	Response planning
		Communications
		Analysis
		Mitigation
		Improvements
Recover	Business continuity plans to maintain resilience and recover capabilities after a cyber breach.	Recovery planning
		Improvements
		Communications

Each category breaks down into a number of controls, for example:

Protect controls		
Access Control (PR.AC)	PR.AC-1	Identities and credentials are managed for authorised devices and users
	PR.AC-2	Physical access to assets is managed and protected
	PR.AC-3	Remote access is managed
	PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties
	PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate.

Note: In the table above PR.AC is the coding that NIST uses in the format '[Function].[Category]-[Sub-category]'. PR stands for 'Protect'; AC stands for 'Access Control'

Implementation tiers are used to create a context within which organisations can better understand how their current cyber security capabilities stand against the characteristics described by the NIST Framework. The tiers can be seen in the table below – NIST recommends that any organisation planning to develop effective cyber security capabilities should be aiming to progress to Tier 3 or 4.

Tiers of cyber security maturity		
Tier 1	Partial	Risk management is ad hoc, with limited awareness of risks and no collaboration with others.
Tier 2	Risk informed	Risk-management processes and programmes are in place but are not integrated enterprise-wide; collaboration is understood but organisation lacks formal capabilities.
Tier 3	Repeatable	Formal policies for risk management processes and programmes are in place enterprise-wide, with partial external collaboration.
Tier 4	Adaptive	Risk management processes and programmes are based on lessons learnt and embedded in culture, with proactive collaboration.

The profile aspect of the framework recognises that different industries and organisations have different business needs, operating models, risk appetites and available resources for developing a robust cyber security programme. The profile enables organisations to align and improve their cyber security practices based on their individual circumstances. A current and target profile can be defined and a comparison of these states can be used to identify the gaps that should be closed in order to enhance cyber security and provide the basis for a prioritised roadmap to help achieve these improvements.

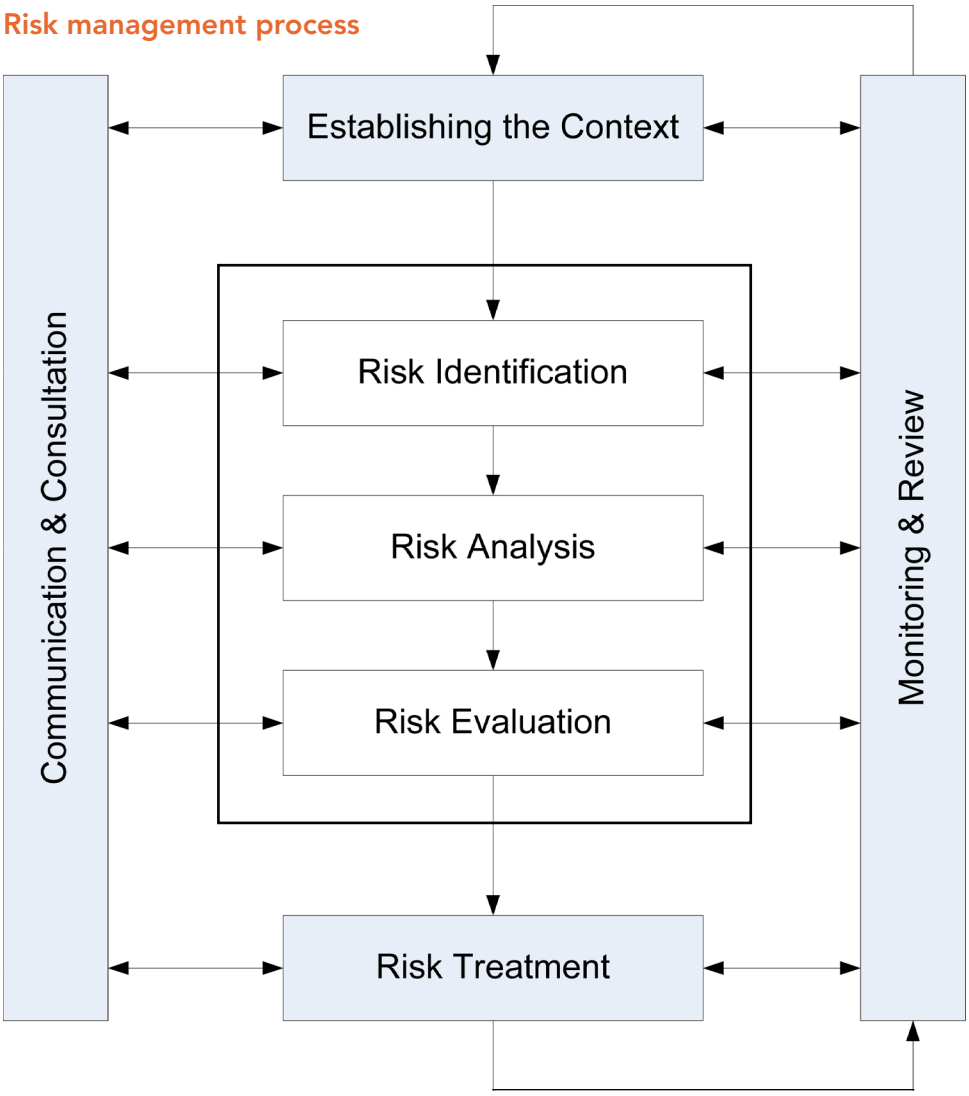
Appendix B

Risk Assessment Methodology

B.1 Overview

The risk assessment methodology forms part of a standard risk management process depicted below, which enables an organisation to effectively identify, assess, and treat risk.The term "risk" refers to the likelihood of being targeted by a given attack. A risk assessment is therefore performed to determine the most important potential security breaches to be addressed and evaluates these in terms of cost impact (consequence) and probability of occurrence (likelihood). Analysing risk in this way can help determine appropriate security budgeting and policy. As part of this process, it is important to first establish the context for the risk assessment. This involves defining the scope and identifying the assets that are potentially at risk. The identification, analysis and evaluation of risks together comprise the Risk Assessment component of the risk management process. The Communicate & Consult part of the process recognises that engagement of stakeholders, both internal and external to the organisation, is key to identifying, analysing and monitoring risk. The Monitor & Review component of the process comprises the controls put in place to ensure that the risk assessment process continues to operate effectively.

Figure 1: Risk management process



B.2 Threats and vulnerabilities

A "threat" refers to the source and means of a particular type of attack. A threat assessment should be performed to determine the best approaches to securing a system against a particular threat. Penetration testing exercises should be conducted to assess threat profiles and help develop effective countermeasures. While a risk assessment focuses more on analysing the potential and tendency of the organisation's resources to fall prey to various attacks, a threat assessment focuses more on analysing the attacker's resources and can help develop specific security policies that need to be implemented. The term "vulnerability" refers to the security flaws in a system that will allow an attack to be successful. Vulnerability testing should be performed on an ongoing basis in order to resolve such vulnerabilities and for maintaining ongoing security vigilance.

The potential threats and vulnerabilities within ATM systems could include:

Weaknesses in business critical applications

A possible application weakness is if there is poor quality software and/or if it has not been developed and tested with sufficient rigour. Issues of information and system availability and integrity can often be addressed through ensuring proper safety requirements for ATM systems. The weakness in application security is not just an issue in terms of the application itself, but also in terms of the security of under or overlying systems. Application vulnerabilities can often be exploited not just to deny access to a specific application but also to gain access to the wider system or network.

Weaknesses in operating and business critical systems

Due to the expense of creating an operating system (OS), there is a limited choice of practical OS to use. Modern operating systems come in a limited number of forms, e.g. Linux, Windows, Unix, OSX and Android. Operating systems fulfill a number of key roles, which requires that they have multiple capabilities. This complexity results in not only capability specific vulnerabilities that can be exploited but also unintentional design flaws or conflicts with other systems or applications. The latter can easily be seen by the number and regularity of patches issued.

Unsupported or unmaintained software

Commercially available software is constantly being assessed for weaknesses and vulnerabilities by software vendors, users and those with malicious intent. Failure to ensure that Commercial Off The Shelf (COTS) software is covered by support agreements and/or rigorous patching procedures can lead to known vulnerabilities being exploited. This is particularly the case for legacy systems connected to the Internet.

Poor access control

A lack of proper access controls can increase the likelihood of unauthorised individuals gaining access to areas that should be forbidden to them. If an organisation fails to limit who can access their information and physical assets, then they increase their exposure to both insider and outsider threats. Theft and unauthorised disclosure of confidential or business critical information as a result of poor access controls can damage a firm's reputation as well as incur a financial impact. Access controls can be both physical and logical, i.e. barriers that require a proximity card to gain access to the building are physical controls whereas digital access rights linked to a user account managed through Active Directory are logical controls. Having rigorous access controls must also be combined with proper authorisation management – it is no use having access controls if a user can request access to a system and be granted access without proper approval, or if access is given before the approval is confirmed.

Poor change management

If there is no organisational process for change management, then uncontrolled changes can introduce instability and openly expose an organisation to systems vulnerabilities.

Weak network controls

Most network devices are designed by default to allow access to data by any user or system that wants to access it. Effective controls must be applied to ensure only those systems/people that legitimately need access to the network are allowed. Weak network controls can be either internal or external – in all cases, an organisation needs to ensure that boundary network controls are effective and do not allow unauthorised access to the network from outsiders.

Poor cloud and virtual machine implementation and management

Cloud computing and virtual machines are relatively new technology platforms in the ATM environment. Use of these new technologies can increase an organisation's exposure to emergent risks and threats. Cloud computing, in particular, can increase a firm's exposure due to the reliance on a third party service. An organisation can leave itself vulnerable if their cloud service provider is affected by a denial of service (DOS) attack, for example.

Poor asset management

Business assets can be both tangible (physical assets such as laptops, servers, etc.) and intangible (information stored digitally). If an inventory of assets is not kept, then it will be difficult for an organisation to keep track of its assets and could result in a delay in an organisation realising that it has lost assets, be they physical assets or information assets. Further, if the value of an asset to the organisation is not properly assessed and recorded, then proportionate controls to secure the asset and its immediate environment cannot be implemented.

Obsolescence

Upgrading existing hardware and software can often be deemed too expensive in terms of immediate benefit to the business. However, reliance on legacy or obsolete systems can expose an organisation to a number of risks and leaves it vulnerable to exploitation. Obsolete systems do not have the same level of service support as current systems and thus vulnerabilities due to conflicts with other software or hardware are unlikely to be found and patched.

Poor software control

Operational system performance can be heavily impacted if the incorrect software has been installed. If there are no policies in place to restrict the installation of software on operational systems then any user could install anything on their system. This could result in the introduction of malware to the network or just degrade operational system performance. While the focus for this should be on key operational systems, it is also important to ensure that corporate (finance, HR, etc.) systems are not left vulnerable, as these can often be an inroad to the rest of the organisation if network controls are not tight enough e.g. if network domains are not separated from each other i.e. segregated.

In a contingency situation, the operational software and the last backup are required to restore operational services back to business as usual. Backup copies of software required for normal operational service should not be kept at a different site in case of a fire or other unforeseen incident that could result in their damage or loss.

Lack of effective monitoring

If there is no intrusion detection or threat monitoring system in place for the network, then it is unlikely that an organisation will know that it has been attacked until long after it has happened; whether this is an external threat trying to breach the network from outside or an insider trying to

gain access to systems they are not authorised to use. An organisation cannot just rely on network monitoring as not all activities or actions, particularly from a motivated external threat, will be identified. Other protective monitoring controls should be applied which could include an effective intrusion detection system.

Lack of effective logging

If an organisation does not log all system activity then it will limit its capability to track actions and activities back to system users in the event of an incident. Effective logging capability gives an organisation forensic capabilities that are critical for determining who did what and when they did it, in a timely manner, facilitating an effective response. Without these capabilities, it could be some time before a security incident is discovered.

Lack of response capability

If an organisation does not have some form of response capability, then regardless of the logging or monitoring controls in place, it will be unable to act with the required speed and efficacy.

Lack of alternate capability (back up and contingency)

System availability all of the time cannot be guaranteed - no organisation is immune from disaster. If an organisation does not have alternative capability or contingency plans in place, be it for operational systems, people, or power for its facilities, then it exposes itself to a high level of risk. An organisation that cannot operate effectively during a disaster or incident due to lack of alternate capability could suffer significant financial and reputational damage (loss of business/trust etc.).

Lack of cyber security training and awareness

If an organisation does not invest in cyber security training for staff then it is likely to suffer from a number of security related issues. Some of the vulnerabilities that can occur as a result of poor cyber security awareness include:

- Lack of personal security online (social networking for example), including leaving details that could compromise the security of the organisation in the public domain
- Improper use of sensitive information
- Leaving key cards unattended
- Not locking laptops/computers when they are unattended
- Allowing tailgating, i.e. the act of following someone into a building without proper authorisation
- Installing malicious software onto the organisations systems

The lack of proper awareness training may lead to exploitation of staff by social engineering, which is a technique that is often used to glean information about people and their work through a number of mediums. If employees use the same password at home as they do at work, and they do not take measures to protect their personal password then they have immediately left the organisation vulnerable to a breach.

Security controls in supplier relationships

A supplier is unlikely to consider an ANSP's security as a high priority unless it is required to, for example by a contractual agreement. In many cases, unless an organisation is explicit in its security requirements, it may find that its suppliers will dictate or heavily influence the technical security implementation used. It is often the case that an organisation will also have relationships with several suppliers or third parties. The result is that there can be a wide range of information exchange point solutions in use, with broad diversity in approach, transfer mechanisms, protocols and encryption standards used. It is the responsibility of the organisation to ensure that its suppliers are secure; that consistent security controls are used; and, ultimately, that it is not vulnerable to a security breach via a third party.

Lack of screening of business-critical data

Data is vulnerable to corruption and it is important that an organisation ensures the integrity of its data and information. An organisation's data should be checked for corruption as it enters and leaves one of its systems. Corrupt data can impact an organisation in several ways. It can damage the organisation's reputation and impact trust amongst its customer base and service users; or it can damage an organisation's systems or hamper/limit its operations in some way. In the context of ATM, a corrupted flight plan can "hang" a flight data processing (FDP) system if it is not screened to ensure integrity before being processed. This is known as a "buffer overflow", an anomaly whereby a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory thereby resulting in erratic program behavior or even a system crash. As such, buffer overflows are the basis of many software vulnerabilities and can be maliciously exploited.

Systems are not synchronised to a single clock

Many ATM systems operate in a real-time environment, relying on an accurate time. Lack of synchronisation between facilities or systems can cause: disruption to services; corrupted information; and data being dropped.

Environmental and physical

Systems and facilities must be designed to work effectively in the environment in which they are deployed. Site construction/location must consider the perennial environmental risks like wind and rain, but also take into account less likely events such as flood, extreme high temperatures and how this might impact support services that are critical to service operation like power and site access.

Loss of information-related assets

Loss or theft of information-related assets is linked to both poor access control and cyber security awareness. It includes assets that could be stolen that contain valuable data, for example an unattended laptop. Items can also be stolen that might affect operational performance, e.g. theft of cabling. It is not the physical loss, but rather the loss of the information asset linked to the physical media, or the impact on operational performance and service provision.

Equipment disposal

Redundant information assets such as old hard drives, printers, routers, can contain valuable intellectual property and other sensitive information if not securely sanitised. Such items need to be securely destroyed to ensure confidentiality of any residual data.

Radio-based technology

Interference can degrade the performance of radio-based technologies such as a Wi-Fi network, radar, radio or navaid. Information transferred over this technology may also be susceptible to interception if not adequately secured e.g. encrypted Wi-Fi.

HVAC (heating, ventilation, and air conditioning

IT hardware has power, humidity and temperature limits and a breach in these limits will affect its operational performance. Poor maintenance of HVAC systems or a deliberate attack could disable hardware and therefore disrupt or halt any interconnected software systems e.g. turning off air conditioning within a server room leading to the overheating of racks and disruption of an operational ATM system.

B.3 Dealing with the Human Threat

Human actions can constitute a security risk, and these can be broken down into two types of actions:

— Intentional: people carry out negative actions for different reasons, often based on their motivations. Motivations can be influenced though communications, education, money,

beliefs, etc. However, "negative" beliefs are hard to change and can only be identified through screening and monitoring. Third parties can influence the motivations of people through direct contact and persuasive communication, money, etc.
- Unintentional: how people behave is also influenced by motivations and personality. This can be due to lack of care, lack of pride, lack of training, time pressures, a belief they know better

As a general rule:
- Personality plus motivation influences behaviour
- Negative behaviour plus capability can equate to a cyber security risk

It is important to identify those 'threat actor groups' that could pose a risk, and this needs to be done through a thorough threat assessment. A 'threat actor group' is a group of people who can reasonably be considered to have the same characteristics in terms of capability, motivation and opportunity to perform an attack. For example, an organisation's set of cleaners may be grouped together as one threat actor group, rather than conducting a threat assessment for each individual cleaner. Security personnel normally do not have the necessary "soft skills" to do this job without assistance. The internal Human Resources department should have a specialist in this area. It must also be understood that different cultures exist in different areas of a business and, therefore, different approaches might need to be taken when working with these groups.

Part 7 of the ISO 27002 standard provides for controls relating to Human Resources security and ensures that the employee understands, is aware of and fulfils his security responsibilities. This also ensures that only those employees with the right personality and motivations are identified for certain roles. This is done through proper screening, testing, awareness education and training, as well as having in place the disciplinary processes to deal with an employee who commits an information security breach. The ISO standard provides for the basic controls; any residual risk can be minimised by a number of other controls, such as restricting access to certain employees and thereby limiting their capability to be a risk.

Below are listed the different types of 'threat actor groups' which have access to information systems:
- Normal users: these are users of ANSP information systems that have routine access to a broad amount of information with no special access rights or permissions
- Privileged users: users of ANSP information systems, e.g. system administrators, specialist engineers, technicians, that are able to change configuration, edit/create access rights, manage system hardware including security controls
- Indirectly connected: these are individuals, not necessarily authorised, that may be able to access ANSP information systems via a connected system
- Service consumers: these are users that benefit from the output of the information system and do not themselves access it or manipulate the data
- Rest of the world (Internet): these are 'group threat actors' that are unauthorised and outside the control of an ANSP or its business partners. They will typically be outside the physical and logical ANSP borders or those of their business partners
- Handlers: this is the group of people required to handle, transport, supply or deliver ANSP information assets
- Service providers: this 'threat actor group' includes those non-ANSP but authorised entities that support the ANSP business and therefore have an interaction with ANSP information assets. This is usually through a service level agreement and contractual processes
- Bystanders: these are users that may have been granted physical access to ANSP information assets or areas but with no access rights to the actual systems or information. Cleaners, visitors or maintenance personnel would typically fit this group

B.4 Consequence of risk occurring

Category	OPERATIONAL		FINANCE	SERVICE DELIVERY	REPUTATION
	Effect on Aircrew & Passengers	Overall ATM System effect			
Catastrophic 1	Multiple fatalities due to collision with other aircraft, obstacles or terrain.	Sustained inability to provide any service.	Financial loss greater than $200M or insolvency such that government support is required.	Sustained inability to provide a service.	Irreparable damage to relationships with a majority of key stakeholders (owner, customers, employees, public, suppliers) resulting in the organisation not continuing in its current form.
Major 2	Large reduction in safety margin; serious or fatal injury to small number; serious physical distress to air crew.	Inability to provide any degree of service (including contingency measures) within one or more airspace sectors for a significant time.	A financial loss such that board approval of response is required.	Inability to provide any degree of service.	Sustained 'outrage' from majority of key stakeholders on capability to provide functions/services.
Moderate 3	Significant reduction in safety margin.	The ability to provide a service is severely compromised within one or more airspace sectors without warning for a significant time.	A financial loss such that CEO approval is required.	The ability to provide a service is severely compromised.	Expressions of 'outrage' by a key stakeholder on organisations services/ activities.
Minor 4	Slight reduction in safety margin.	The ability to provide a service is impaired within one or more airspace sectors without warning for a significant time.	A financial loss such that delegate approval is required.	The ability to provide a service is impaired	Occasional complaints from key stakeholders requiring additional management attention to reach a satisfactory outcome.
Insignificant 5	Potential for some inconvenience.	No effect on the ability to provide a service in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency measures if the condition prevails.	A financial loss that can be managed within a business unit/ branch/ section budget.	Negligible effect on the ability to provide a service.	Isolated complaint by individual stakeholder which can be managed to a satisfactory outcome as part of day-to-day business.

B.5 Likelihood of risk occurring

We have adopted the definitions in the table to the right for estimating the likelihood of an identified risk occurring.

	Event is expected to occur
1	More frequently than hourly
2	Between hourly and daily
3	Between daily and yearly
4	Between yearly and 5 yearly
5	Between 5 and 50 years
6	Less frequently than once every 50 years

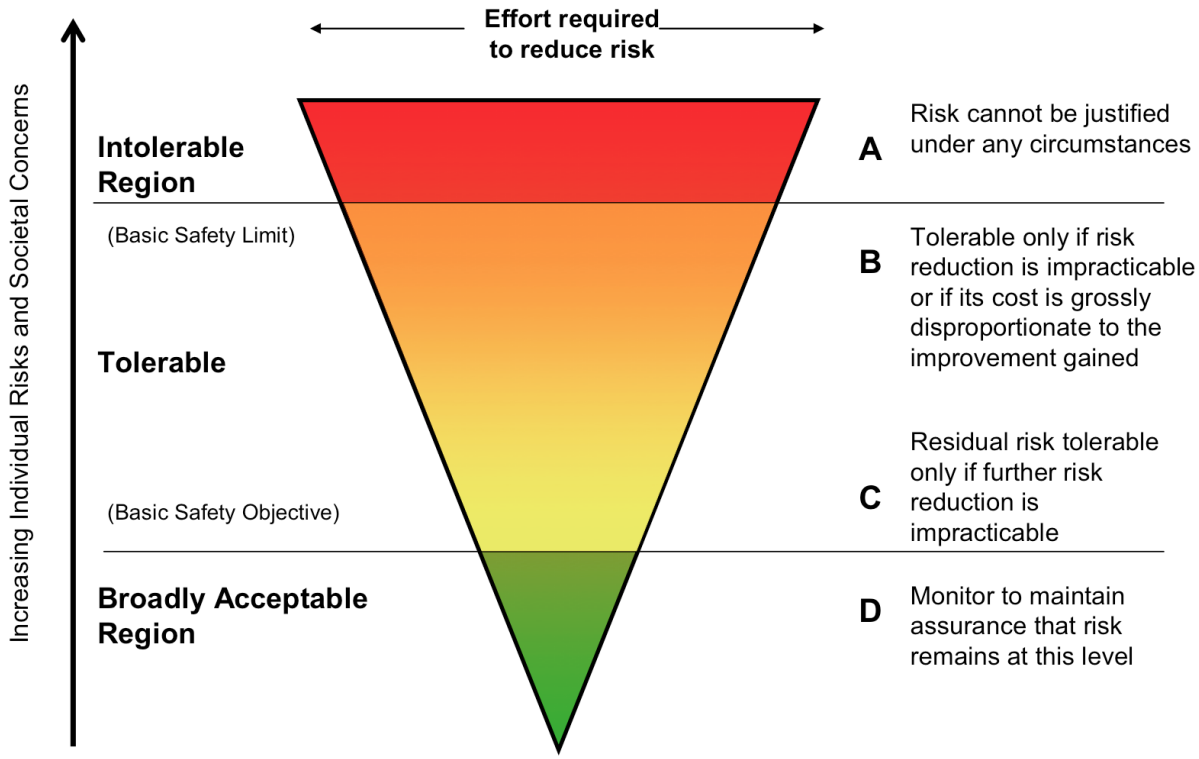
B.6 Assessment of the level of risk and risk tolerance

We have reviewed all identified risks and provided for each an overall risk ranking which is a combination of the two characteristics of consequence and likelihood. For example, a risk with a major consequence but a "5" likelihood would be described as having a "B" or "tolerable" risk rating.

The conversion of the combination of consequence and likelihood into a risk rating has been achieved by use of the following matrix.

Likelihood Criteria		Consequence Criteria				
Event expected to occur:		Catastrophic 1	Major 2	Moderate 3	Minor 4	Insignificant 5
1	More frequently than hourly	A	A	A	A	C
2	Between hourly and daily	A	A	A	B	D
3	Between daily and yearly	A	A	B	C	D
4	Between yearly and 5 yearly	A	B	C	C	D
5	Between 5 and 50 years	A	B	C	D	D
6	Less frequently than once every 50 years	B	C	D	D	D

The previous matrix provides a guide to determine which risks are the highest priorities from the perspective of the timeliness of the corrective action required. The following diagram outlines the position in more definitive terms.



B.7

Sample risk assessment tables

L = Likelihood
C = Consequence
R = Risk

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
ID.AM-1	**IDENTIFY**	Asset Management	Risk of loss, theft and/or misuse of organisational assets or information assets.	Inventory of physical assets is made; protective marking scheme is in place.	3	3	**B**	Reduce	Ensure that an inventory of assets is completed, including who owns individual assets; the acceptable use of assets and information associated with information and information processing facilities; and a procedure for the return of assets owned by the organisation by external third parties, employees or contractors on termination of their employment, contract or agreement. Policies for the use of disposable or removable media should be put in place, particularly where these devices are used for the transport of protectively marked information. A protective marking scheme for information assets should be in place to ensure compliance with legal requirements and to aid staff in determining how assets should be dealt with. This should also aid with preventing unauthorised disclosure.			**D**

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
ID.BE-1	**IDENTIFY**	Business Environment	Operational activities are disrupted due to dependencies not being fully understood and risk managed.	Operational and business dependencies are identified and mapped. Frameworks/ guidelines are established for dependency relationships (e.g. receive flight plans by a certain time, if not received by deadline then can chase). Alternative capabilities/ redundancies for dependencies are identified and established.	4	5	**D**	Accept				
ID.GV-1		Governance	Incurring penalties for failing to meet regulatory requirements	Business activities are audited for compliance and business maintains links with regulators to ensure that business objectives and strategy meet with regulatory requirements.	4	5	**D**	Accept				
ID.RA		Risk Assessment	Inconsistency in risk assessments and/or approach to risk assessments.	Use a risk assessment framework to guide those conducting risk assessments and increase consistency between deliverables.	4	5	**D**	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
ID.RM	**IDENTIFY**	Risk Management Strategy	Motivated and capable outsider threat attempting to hack the overall system through exploitation of vulnerability due to insufficient supply chain risk management.		3	3	**B**	Reduce	Emphasise the need to implement supply chain risk management, as well as an associated policy, to minimise exploitation vulnerabilities in hardware, software and firmware. Emphasise the need and associated policy (FAA) to use secure software development practices to minimise exploitation vulnerabilities.	5	4	**D**
PR.AC-1	**PROTECT**	Access Control	Risk of unauthorised access to confidential or business critical information.	Access rights assigned to roles; approval system in place for access rights requests.	3	4	**C**	Reduce	Ensure an access management policy is in place; adopt an access authorisation procedure that manages access rights requests; ensure appropriate levels of approval are in place for different levels of access rights and that access rights are not granted until proper approvals are in place.	5	4	**D**
PR.AC-2			Organisation is vulnerable to physical attacks, which could take business critical and operational systems offline.	Physical access to buildings and facilities is restricted to authorised personnel only. Business critical facilities should have further restrictions on who has access. Logical controls are backed up by physical controls. Access rights need to be authorised and approved before access is granted.	5	4	**D**	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
PR.AT-1	**PROTECT**	Awareness and Training	No cyber or information security awareness training for staff or contractors, particularly covering accidental disclosure of confidential or business critical information.	Line manager training events that outline roles and responsibilities for managers to ensure that their staff have read online courses.	3	3	**B**	Reduce	Implement broad cyber and information security awareness training to enhance the ability of staff to recognise the diverse range of cyber threats and their capability to critically impact upon ATM infrastructure and business as usual procedures. Ensure that contractual obligations and requirements are included for all staff with respect to continual education and awareness training, so that everyone is aware of their responsibilities. Staff should be made aware that management will expect them to apply information security In line with the policies and procedures of the organisation. A culture of information security should be encouraged within the organisation whereby information security is integrated into standard business practices.	6	3	**D**

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
PR.DS-1			Data from primary radar could be corrupted or otherwise compromised or lost due to an attack by a motivated and capable intruder via the internet.	Secondary radar is available as a backup to the primary radar in the event that the data from the primary radar is compromised, corrupted or lost.	4	5	D	Accept				
PS.DS-2	**PROTECT**	Data Security	Saturation of data processing resources due to obsolete or legacy systems.		3	3	B	Reduce	Ensure access to data processing resources is managed to prevent saturation; prioritise systems so that business critical systems can have access to data processing resources when they need them; and ensure resource requirements are reviewed regularly.			
PS.DS-5			Systems rely on synchronised time and are vulnerable to corrupted times in the system	All business-critical systems synchronised to a single reference clock. Validation takes place (both logical and physical) to check this.	5	4	D	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
PS.DS-6	PROTECT		Confidential or business critical information could be leaked unintentionally through incorrect disposal of equipment and/ or media.		4	4	C	Reduce	Procedure for the safe disposal of media should be disseminated to the organisation and enforced. All portable media should be disposed of in the proper and approved way.	5	5	D
PR.IP-1		Information Protection Processes & Procedures	Change management controls and processes are not suitable to the environment they are intended to operate in and are not integrated with information security policies.	Change management process is in place and has information security embedded in it.	4	3	C	Reduce	A change management process should be in place that governs effective change management within the organisation. Effective use of the change management process should mitigate the impacts of changes to the business and control the impacts of changes to the organisation, business processes, information processing facilities and systems on information security.	4	6	D

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
PR.MA-1	PROTECT	Maintenance	Poor engineering procedures could leave organisation at risk to information or cyber based attacks.	Regular checks carried out by line management.	4	3	C	Reduce	An audit which looks at engineering procedures including line manager's checks.	5	3	C
PR.PT-1		Protective Technology	GPS infrastructure could be victim of cyber disruption or attack due to vulnerability in the infrastructure to spoofing/ exploitation.	Secure development policy which covers GPS program.	4	2	B	Reduce	Further emphasise the need to employ highly secure development and implementation practices such as those being used for the GPS Operational Control System (OCX) Program. Employ redundant systems – operators and ATCOs should be able to operate from an alternative means to GPS.	5	3	C
PR.PT-2			Compromise of ATM systems due to weakness in business-critical applications or applications that give access to wider system.	Secure development policy in place; business critical applications are tested and reviewed when there are system or platform changes; information regarding technical vulnerabilities of business critical applications are obtained and highlighted as soon as possible; and development, testing and operational environments are kept separate.	5	4	D	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
PR.PT-3	**PROTECT**	Protective Technology	Business critical systems disrupted by attack from internal/external threats due to vulnerabilities in operating systems, for example where exploits have not been fixed due to irregular rolling out of patches.	Ensure information regarding technical vulnerabilities of business critical operating systems are obtained and highlighted as soon as possible; ensure there is a secure development policy in place; ensure business critical operating systems are tested and reviewed when there are system or platform changes; and ensure that the development, testing and operational environment are kept separate.	5	4	**D**	Accept				
PR.PT-5			Unable to track or audit historical activities of users in the event of a security event or incident.	All user activities, including from administrator and operator accounts, are recorded and time/date stamped (systems are synchronised to same clock on regular basis to ensure accurate time/ date stamping). The logs are secured and can only be accessed by authorised users, and access is only available once proper approvals are in place. Access to the logs themselves should also be logged (separately).	4	5	**D**	Accept				
DE.AE	**DETECT**	Anomalies & Events	Intruders are able to breach network without being detected or the incident is not flagged up appropriately or in time for a response to be mobilised.	A baseline level of network operations and activity, as well as expected data flows, has been established for users and systems. Incident alert thresholds have been established and anything that does not conform to the thresholds is flagged up as an incident. Detected events are analysed via data aggregated from a number of sources in order to understand targets and methods and the impact of the event.	3	5	**D**	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
DE.CM	DETECT	Security Continuous Monitoring	Threats to the organisation would not be caught due to insufficient monitoring procedures.	Monitoring system in place to monitor traffic on network.	3	2	A	Reduce	Monitoring systems should be put in place to pick up information security events and incidents, unusual user activities, exceptions and faults. This monitoring should include administrator and system operator activities. The facilities supporting the monitoring systems should be protected from tampering/unauthorised access. There should be a reporting system in place that assesses information security events, classifies them, and escalates the events to be dealt with as necessary.	5	4	D
DE.DP		Detection Processes	Failure of critical system such as flight data processing (FDP) due to malware infection.	Anti-virus software installed on all systems. Staff are aware of the threat that malware poses to vulnerable systems through awareness training. It is necessary to ensure that appropriate malware detection capability is in place so that malware can be caught before it propagates throughout a network and infects critical systems – however, due to business critical nature of certain systems, it may not be possible to ensure most up to date definitions and patches are applied in a timely manner. Best judgement should be used as to when patches should be applied.	3	4	C	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
RS.RP	RESPOND	Response Planning	Response has not been prepared for information security incidents or crises that would affect the organisation in such a way that systems and activities that are business critical are disrupted.	Response plan is in place for the organisation, which integrates information security and cyber security into the wider organisational strategy. Strategy is owned by a senior manager who has responsibility for ensuring that the plan is implemented appropriately. Incident response plans and procedures are in place.	5	4	D	Accept				
RS.CO		Communications	In the event of a security incident, response plan cannot be implemented because key staff had not been made aware of it.	Response plan is available to staff as a soft copy document on the employee portal.	4	3	C	Reduce	Include contractual obligations for key staff to be familiar with all organisational policies, including the response plan. Ensure staff are made aware of the plan through both formal and informal training. Ensure staff buy-in by having key staff input into the plan when it is reviewed and updated.	4	5	D
RS.AN		Analysis	In the event that a security incident is reported, no further investigation is carried out into the nature of the breach and resulting collateral damage, i.e. the cost.	Analysis and reporting framework in place to provide step guidance on how to proceed an investigation when a breach is identified.	4	3	C	Reduce	Breaches are logged and mandatory investigation timeframes are enforced, i.e. a SIEM tool.	4	5	D

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
RS.MI	RESPOND	Mitigation	In the event of a virus breach, limited action is taken to halt it's propagation throughout the system.	Anti-malware packages installed on systems.	3	3	B	Reduce	Shut down infected networks and consider shutting down adjacent networks to prevent propagation.	3	4	C
RS.IM		Improvements	Lessons learnt from previous security incidents/ crises are not implemented.	Lessons learnt from implementation of response plan are recorded in a log and acted upon.	4	5	D	Accept				
RC.RP	RECOVER	Recovery Planning	Lack of resilience and recovery capability within the organisation resulting in increased time between an incident and returning to business as usual.	Disaster recovery plan is in place for the organisation, which integrates information security and cyber security into the wider organisational strategy. Plan is owned by a senior manager who has responsibility for ensuring that the plan is understood, disseminated throughout the organisation and implemented appropriately. Recovery plan has redundancies and alternative capabilities built in in the event of unavailability of key staff.	5	4	D	Accept				
RC.IM		Improvements	Lessons learnt from previous security incidents/ crises are not implemented.	Lessons learnt from implementation of business continuity strategy or plan are recorded in a log and acted upon.	4	5	D	Accept				

Ref	Function	Category	Risk	Existing controls	Current risk			Accept/ reduce	Recommended controls	Residual risk		
					L	C	R			L	C	R
RC.CO	**RECOVER**	Communications	Reputation suffers as the result of a breach in a way that impacts the operation of the business, either financially or operationally.	Communications and public relations team are well briefed in the event of an incident on the potential impacts to the organisation. Good communication within the organisation from the Communications and PR team on lines to take with the media.	4	3	**C**	Accept				

B.8

Treatment recommendations

Ref #	Recommendation	Risk Rating	Commentary	Status
S1.1				

10
Sources

ICAO Doc 9985 ATM Security Manual, 1st Ed. (Restricted)

ICAO Doc. 8973 Aviation Security Manual, 8th Ed. (Restricted)

"Cyber Security of a Net-Centric Aviation Ecosystem", Network Centric Operations Industry Consortium (NCOIC), version 1.0, December 2011

"Information Security in a Net-Centric Environment – Enforcing Secure Data Sharing in a Distributed Network", Network Centric Operations Industry Consortium (NCOIC), version 3.0, January 2012

"Analysis of Cybersecurity Content in the Air Traffic Collegiate Training Initiative (AT-CTI) Program", Juan Lopez Jr. and Deanne W. Otto, Two Cultures: International Journal of Technology, Humanities, and Human Security. ISSN 2324-738X Vol. 1, no. 1

"A Taxonomy of Operational Cyber Security Risks", James J. Cebula and Lisa R. Young, Software Engineering Institute. Technical Note CMU/SEI-2010-TN-028, December 2010

"The Connectivity Challenge: Protecting Critical Assets in a Networked World – A Framework for Aviation Cybersecurity", The American Institute of Aeronautics and Astronautics (AIAA). August 2013

Glossary of Key Information Security Terms (NISTIR 7298, Revision 2.) Richard Kissel, Editor. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), May 2013

Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. National Institute of Standards and Technology (NIST). February 12, 2014

"Getting ahead of the threat: Aviation and cyber security", Emilio Iasiello, iSIGHT Partners. Aerospace America. The American Institute of Aeronautics and Astronautics (AIAA). July-August 2013

Article "Under Attack? Cyber security and air traffic management" Airspace Magazine Issue 14 Quarter 3 2011

CANSO Members

CANSO – the Civil Air Navigation Services Organisation – is the global voice of air traffic management worldwide. CANSO Members support over 85% of world air traffic. Members share information and develop new policies, with the ultimate aim of improving air navigation services (ANS) on the ground and in the air.

CANSO represents its Members' views in major regulatory and industry forums, including at ICAO, where it has official Observer status. CANSO has an extensive network of Associate Members drawn from across the aviation industry. For more information on joining CANSO, visit www.canso.org/joiningcanso.

canso
civil air navigation services organisation

Full Members - 84

- Aeronautical Radio of Thailand (AEROTHAI)
- Aeroportos de Moçambique
- Air Navigation and Weather Services, CAA (ANWS)
- Air Navigation Services of the Czech Republic (ANS Czech Republic)
- AirNav Indonesia
- Air Traffic & Navigation Services (ATNS)
- Airports and Aviation Services Limited (AASL)
- Airports Authority of India (AAI)
- Airports Fiji Limited
- Airservices Australia
- Airways New Zealand
- Albcontrol
- Austro Control
- Avinor AS
- AZANS Azerbaijan
- Belgocontrol
- Bulgarian Air Traffic Services Authority (BULATSA)
- CAA Uganda
- Civil Aviation Authority of Bangladesh (CAAB)
- Civil Aviation Authority of Botswana
- Civil Aviation Authority of Mongolia
- Civil Aviation Authority of Singapore (CAAS)
- Civil Aviation Authority of Swaziland
- Civil Aviation Regulatory Commission (CARC)
- Comisión Ejecutiva Portuaria Autonoma (CEPA)
- Croatia Control Ltd
- Department of Airspace Control (DECEA)
- Department of Civil Aviation, Republic of Cyprus
- DFS Deutsche Flugsicherung GmbH (DFS)
- Dirección General de Control de Tránsito Aéreo (DGCTA)
- DSNA France
- Dutch Caribbean Air Navigation Service Provider (DC-ANSP)
- ENANA-EP ANGOLA
- ENAV S.p.A: Società Nazionale per l'Assistenza al Volo
- Entidad Pública Aeropuertos Españoles y Navegación Aérea (Aena)
- Estonian Air Navigation Services (EANS)
- Federal Aviation Administration (FAA)
- Finavia Corporation
- General Authority of Civil Aviation (GACA)
- Ghana Civil Aviation Authority (GCAA)
- Hellenic Civil Aviation Authority (HCAA)
- HungaroControl Pte. Ltd. Co.
- Instituto Dominicano de Aviacion Civil (IDAC)
- Israel Airports Authority (IAA)
- Iran Airports Co
- Irish Aviation Authority (IAA)
- ISAVIA Ltd
- Japan Civil Aviation Bureau (JCAB)
- Kazaeronavigatsia
- Kenya Civil Aviation Authority (KCAA)
- Latvijas Gaisa Satiksme (LGS)
- Letové prevádzkové Služby Slovenskej Republiky, Štátny Podnik
- Luchtverkeersleiding Nederland (LVNL)
- Luxembourg ANA
- Maldives Airports Company Limited (MACL)
- Malta Air Traffic Services (MATS)
- National Airports Corporation Ltd.
- National Air Navigation Services Company (NANSC)
- NATS UK
- NAV CANADA
- NAV Portugal
- Naviair
- Nigerian Airspace Management Agency (NAMA)
- Office de l'Aviation Civile et des Aeroports (OACA)
- ORO NAVIGACIJA, Lithuania
- PNG Air Services Limited (PNGASL)
- Polish Air Navigation Services Agency (PANSA)
- PIA "Adem Jashari" - Air Control J.S.C.
- ROMATSA
- Sakaeronavigatsia Ltd
- S.E. MoldATSA
- SENEAM
- Serbia and Montenegro Air Traffic Services Agency (SMATSA)
- Serco
- skyguide
- Slovenia Control
- State Airports Authority & ANSP (DHMI)
- State ATM Corporation
- Sudan Air Navigation Services Department
- Tanzania Civil Aviation Authority
- Trinidad and Tobago CAA
- The LFV Group
- Ukrainian Air Traffic Service Enterprise (UkSATSE)
- U.S. DoD Policy Board on Federal Aviation

Gold Associate Members - 11

- Airbus ProSky
- Boeing
- FREQUENTIS AG
- GE Air Traffic Optimization Services
- GroupEAD Europe S.L.
- ITT Exelis
- Lockheed Martin
- Metron Aviation
- Raytheon
- Selex ES
- Thales

Silver Associate Members - 70

- Adacel Inc.
- Aeronav Inc.
- Aireon
- Air Traffic Control Association (ATCA)
- 'Association Group of Industrial Companies "TIRA" Corporation
- ATAC
- ATCA – Japan
- ATECH Negócios em Tecnologia S/A
- Aviation Advocacy Sarl
- Aviation Data Communication Corp (ADCC)
- Avibit Data Processing GmbH
- Avitech GmbH
- AZIMUT JSC
- Barco Orthogon GmbH
- Brüel & Kjaer EMS
- BT Plc
- Comsoft GmbH
- CGH Technologies, Inc
- CSSI, Inc.
- EADS Cassidian
- EIZO Technologies GmbH
- European Satellite Services Provider (ESSP SAS)
- Emirates
- ENAC
- Entry Point North
- Era Corporation
- Etihad Airways
- Guntermann & Drunck GmbH
- Harris Corporation
- Helios
- Honeywell International Inc. / Aerospace
- IDS – Ingegneria Dei Sistemi S.p.A.
- Indra Navia AS
- Indra Sistemas
- INECO
- Inmarsat Global Limited
- Integra A/S
- Intelcan Technosystems Inc.
- International Aero Navigation Systems Concern, JSC
- Jeppesen
- JMA Solutions
- Jotron AS
- LAIC Aktiengesellschaft
- LEMZ R&P Corporation
- LFV Aviation Consulting AB
- Micro Nav Ltd
- The MITRE Corporation – CAASD
- MLS International College
- MovingDot
- NLR
- Northrop Grumman
- NTT Data Corporation
- Núcleo de Comunicaciones y Control, S.L.U.
- Quintiq
- Rockwell Collins, Inc.
- Rohde & Schwarz GmbH & Co. KG
- RTCA, Inc.
- Saab AB
- Saab Sensis Corporation
- Saudi Arabian Airlines
- Schmid Telecom AG
- SENASA
- SITA
- SITTI
- Snowflake Software Ltd
- STR-SpeechTech Ltd.
- TASC, Inc.
- Tetra Tech AMT
- Washington Consulting Group
- WIDE

Membership list correct as of 12 June 2014. For the most up-to-date list and organisation profiles go to www.canso.org/cansomembers