

CANSO STANDARD OF EXCELLENCE IN CYBERSECURITY

SHAPING
OUR
FUTURE
SKIES

canso.org

Acknowledgements

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

- Aeronautical Radio of Thailand (AEROTHAI)
- Aeronav Inc.
- Avinor Flysikring AS
- Civil Aviation Authority of Singapore (CAAS)
- DFS Deutsche Flugsicherung GmbH
- Empresa Cubana de Navegación Aérea (ECNA S.A.)
- EUROCONTROL
- Federal Aviation Administration (FAA)
- Frequentis AG
- Helios
- Inmarsat Global Limited
- Micro Nav Limited
- NATS
- Park Air
- Polish Air Navigation Services Agency (PANSO)
- NLR

In particular, special appreciation is given for the work the EUROCONTROL Network Manager undertook in developing the underlying ATM Cybersecurity Maturity Model.

Table of Contents

Acknowledgements	2
Executive Summary	4
Introduction.....	5
Enhancing Cybersecurity	8
Excellence in Cybersecurity.....	11
Definition of Maturity Levels	17
Advice and Lessons Learned	22
Conclusions.....	35
Appendix A – Scoring Form	36
Appendix B – Glossary.....	42
Appendix C – Sources	43

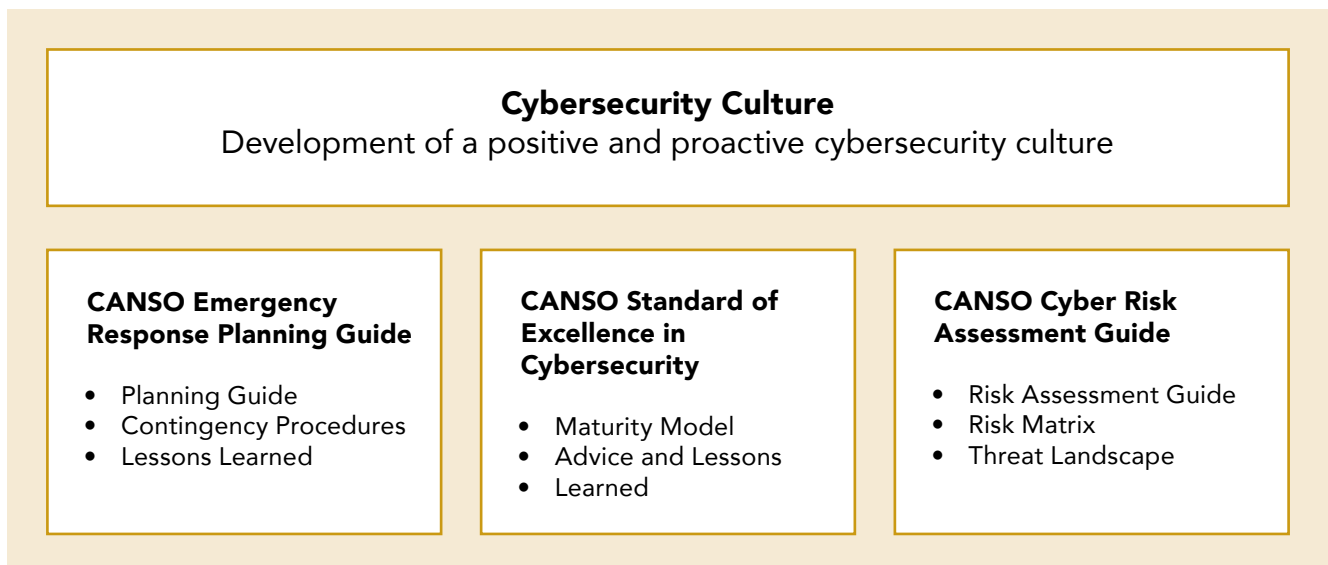
Executive Summary

This Standard of Excellence (SoE) contains the cybersecurity maturity model to enable an Air Navigation Service Provider (ANSP) to assess its own as well as their suppliers' cybersecurity maturity. The maturity model comprises thirteen elements based on six functions that would be expected in an organisation with an effective approach to cybersecurity.

Each element is described in detail in the maturity model, with five different levels of maturity ranging from having informal arrangements in place to an optimised approach. The assessment against each element is conducted using a scoring form containing probing questions, which enables an organisation and its supply chain to identify their current level of maturity. The maturity model is supplemented by advice on getting started and lessons learned from other industry stakeholders, that have already instigated a strong cybersecurity culture.

The model has been designed to be completed by Chief Information Security Officers (CISO) and security managers within a short timescale. The results of the assessment provide a roadmap for improvement to ensure that senior management are aware of an organisation's current exposure to cybersecurity risk and where improvements should be made.

This SoE is part of a collection of documents, which includes a risk assessment guide and an emergency response guide, designed to provide a holistic approach to cybersecurity in an ATM environment. This is shown in the diagram below.



Introduction

“Inspired by the Safety Maturity approach, Cybersecurity Maturity was jointly developed with ANSPs with the aim of having a quick and light assessment of a range of capabilities that you would expect to see in an organisation with an effective approach to cybersecurity. NM has applied it successfully with the top 10 suppliers of NM and it allowed the top management to take the temperature of the situation and draw a roadmap for improvements. The maturity model was found to be extremely useful and appreciated by the suppliers.”

Tony Licu,
EUROCONTROL Network Manager

The *CANSO Standard of Excellence (SoE) in Cybersecurity* helps air navigation service providers (ANSPs) assess, develop and improve their cybersecurity in order to provide safe and resilient air navigation services.

This Standard of Excellence is based on a maturity model developed by EUROCONTROL and CANSO Europe members, and is in line with the CANSO Standards of Excellence in Safety Management Systems and Human Performance Management. In combination, they provide a means to assess, expand and improve ATM safety and security.

This Standard of Excellence complements the CANSO Cyber Risk Assessment Guide that provides ANSPs with an introduction to risk assessment for cybersecurity in Air Traffic Management (ATM), including the cybersecurity threats, risks and motives of threat actors, and an example risk assessment method. Using the CANSO Cyber Risk Assessment guide will enable ANSPs to move towards improved cybersecurity, as measured by this Standard of Excellence.

This Standard of Excellence also complements the CANSO Emergency Response Planning Guide that brings together best practices, knowledge and experience related to contingency plans and procedures from ANSPs around the world. The guide helps ANSPs develop a formal emergency response plan that documents the orderly and efficient

transition from normal to emergency operations and return to normal operations.

Why is cybersecurity necessary?

The trend in ATM, both at an international level as well as within individual ANSPs, is towards increased sharing of information and the creation of a common situational awareness for a wide spectrum of aviation stakeholders. While this enhances the efficiency of operations and raises productivity, it also increases the potential for cyber-attack. Furthermore, the potential vulnerabilities are 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. Also, unlike in the past, information sharing in future of ATM systems will not be limited to point-to-point communications, but will also leverage the benefits of open systems architecture and an internet-based flow of information.

This trend is clearly not unique to ATM; all industries are applying 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: disrupting flows of information, compromising data integrity, losing sensitive information, etc. In ATM, such security compromises can disrupt service provision, undermine safety, and cause reputational damage as well other types of impact, such as financial and regulatory compliance.

The threat is both very real and very serious. ANSPs must develop and execute security strategies and plans to ensure continued operation at the required level of safety despite this threat. If we are to transform global ATM performance and achieve safe, efficient, and seamless use of airspace globally, the global ATM system must meet clear security requirements and expectations.

Furthermore, society demands the highest standards

of aviation safety and security. Any perceived or real shortcomings in the security performance of the aviation industry will negatively impact the reputation of aviation stakeholders with a corresponding impact on customer perception and choice in a highly competitive transport market.

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.

It is essential that ANSPs (individually and collectively) make cybersecurity a top priority, and that they work together to ensure a secure global air transportation system. Cybersecurity is not a choice but a requirement.

What is the regulatory requirement for cybersecurity?

Cybersecurity receives specific consideration in the general legal framework contained in Annex 17 – Security to the Chicago Convention, which states:

- “Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.
- Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, remote access control, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.”

The Aviation Security Manual (Doc 8973 – Restricted) and the Air Traffic Management Security Manual (Doc. 9985 – Restricted) provide some guidance on how to apply the Standards and Recommended Practices (SARPs) contained in Annex 17.

Many States do have additional regulations in place for cybersecurity that cover ATM, though these do vary by region and by State (for example the European NIS directive EU 2016/1148).

What are the cybersecurity threats and risks that ATM faces?

A cybersecurity 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. The CANSO Cyber Risk Assessment Guide gives more details on the potential threat actors and threats addressed in the risk assessment process.

Unintentional threats can be caused by inattentive or poorly trained employees, weaknesses in operating/maintenance procedures, software upgrades, 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.

The most concerning threat that is repeatedly identified is that of 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 influencing 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 cybersecurity and physical attack, for example, a physical intrusion into ground-based infrastructure and a modification of the software code hosted in the infrastructure. This would be an intentional cybersecurity and physical attack. Alternatively, when authorised personnel do not follow procedures to check the infrastructure, and the infrastructure generates and transmits misleading data. This is both a cybersecurity and unintentional physical attack.

What are the top-level security requirements for data and information?

Of paramount importance to cybersecurity in ATM is data integrity and availability, but it is important to fully understand the wider top-level security requirements for data and information:

- **Confidentiality:** the assurance that aviation data is not disclosed to unauthorised persons, processes, or devices. It includes both the protection of operational aviation information and the protection of password and configuration information.
- **Integrity:** assures that aviation data is not modified by unauthorised entities or through unauthorised processes. Integrity supports the assurance that aviation data is not accidentally or maliciously manipulated, altered, or corrupted. Integrity also means that detection occurs with no or minimal false alarms when data has been modified; and that the source of this modification must be identifiable.
- **Availability:** assures timely, reliable, continued access to aviation data 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 confirm it possesses 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. This provides assurance that sender and receiver receive confirmation of the transmission and receipt 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.

How does cybersecurity relate to information security, physical security and personnel security?

Cybersecurity, and information security, a related term, rely upon physical security (e.g. physical access to data centres and machines, deployed systems, etc.) and personnel security (e.g. mitigation of the social engineering and insider threats).

This 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 security, physical security and information security, along with the relevant organisational and procedural aspects.

Enhancing Cybersecurity

“Security is not just a matter of mere compliance, but it relies on an effective capacity for prevention, protection, deterrence, incident detection and response capacity, containment and recovery. The measure of effectiveness of policies, governance, processes and resources defines the effectiveness of the management system and the level of capacity to protect the public value of the provision of air navigation services.”

Francesco di Maio, ENAV
Head, Security Department

The range and sophistication of attacks is so broad, and the resources available to the most potent attackers so great that this problem cannot be addressed with a single solution. Furthermore, the problem cannot be addressed at a single point in time, nor can it be completely eliminated. The tools, tactics, and strategies of attackers at all levels are readily available and will continue to evolve, and the threat will continue to evolve as a result. It would be naive to believe that the proliferation of these tools can be controlled through legislation or regulations. The effective response to this threat will require a long-term commitment from senior leadership to an ongoing process of building and operating increasing levels of cybersecurity capabilities. This includes being more proactive, dynamic, and adaptive to counter constantly changing threats.

Which elements should Cybersecurity improvements address?

Like safety, cybersecurity is a cross-cutting discipline that covers policy, processes, technology and people. It also has a full security incident lifecycle approach: protecting assets from threats, detecting anomalous behaviour, responding to incidents and recovering from compromise. The lifecycle approach 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. An enterprise-wide approach is also needed that enhances security, provides agility to a changing

threat landscape, and reduces overall costs. The effective implementation of this architecture requires organisations to develop policies and fund security solutions throughout the enterprise with total and continuing management commitment.

As a result of reviewing best practice within ATM and other security and safety-related industries, 13 elements of cybersecurity have been identified and addressed by the CANSO Standard of Excellence in Cybersecurity.

Leadership and governance

Goal: Top management demonstrate leadership and commitment to cybersecurity. The policies needed to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Effective leadership and governance help ensure that cybersecurity supports business goals, optimises business investment in cybersecurity, and appropriately manages cybersecurity related risks and opportunities.

To exercise effective cybersecurity governance, ANSP boards and senior management must have a clear understanding of the cybersecurity vulnerabilities and what to expect from their cybersecurity 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 the ISO 27000 series or the National Institute of Standards and Technology's (NIST) Cybersecurity framework, may assist leadership in identifying areas of weakness and enable objectives to be created.

Information Security Management System (ISMS)

Goal: The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives.

An Information Security Management System (ISMS) 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, an ISMS helps the organisation develop proactive, efficient and cost-effective security measures. The cybersecurity programme should fit within this overall framework of an ISMS.

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.

Asset Management

Goal: The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organisation's risk strategy.

It is important to know what assets require protection as assets that are not identified cannot be protected. The process of identifying assets, classifying, and implementing protection measures is therefore an essential component of a cybersecurity programme. An effective asset management programme will help to enhance cybersecurity via the appropriate discovery and analysis of assets. Assets include data, devices/systems, facilities and people. Asset owners should take responsibility throughout the information lifecycle: asset creation/procurement, processing, storage, transmission, and destruction.

Risk Assessment

Goal: The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, including

system-of-system aspects resulting from dependencies.

ANSPs should conduct a risk assessment to determine the greatest risks to the organisation and business, and should consider assessing the adequacy of their cybersecurity 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. 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.

An acceptable risk level is determined by the combination of likelihood and potential impact. For example, a threat that results in a catastrophic impact must be controlled such that it is extremely unlikely to occur.

Information sharing

Goal: The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties

The sharing of information by ANSPs of known or potential cybersecurity threats and vulnerabilities can play a vital part in strengthening the overall response to incidents and their prevention. This requires the establishment of, and full participation in, multi-stakeholder trust partnerships and forums.

Supply Chain Risk Management

Goal: The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.

Supply Chain Risk Management (SCRM) is a discipline that addresses the threats and vulnerabilities of commercially-acquired information and communications technologies used by organisations. Through SCRM, systems engineers can minimise the risk to and from systems and their components obtained from sources that are not trusted or identifiable as well as those that provide inferior material or parts. SCRM is therefore the coordinated efforts of an organisation to help identify, monitor, detect and mitigate threats to supply chain performance. Cybersecurity supply chain risks may

include insertion of counterfeits, unauthorised production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cybersecurity supply chain.

Identity Management and Access Control

Goal: *Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access.*

Such controls should 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.

Human-Centred Security

Goal: *The organisation's personnel and partners are provided with cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Security is part of the organisation's culture.*

The commitment of people to protecting their organisation is an essential component of a strong cybersecurity defence. This means a critical part of the cybersecurity 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.

Protective Technology

Goal: *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Systems and processes are designed to be sensitive to the additional workload created by cybersecurity requirements.*

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 differences in security policies between aviation stakeholders. However, end-to-end security design may reduce the security cost impact on the net-centric aviation system. In order to implement effective cybersecurity strategies, multi-stakeholder trust partnerships need to be established that encourage information sharing and collaboration.

Anomalies and Events

Goal: *Anomalous activity is detected in a timely manner and the potential impact of events is understood.*

Logging allows security monitoring and detection of security events, thereby enabling incident response. Adequate logs also 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, and through regular audit. Updates through reports and management information should be produced and provided to senior management on a regular basis.

Response Planning

Goal: *Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.*

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

With the fundamental understanding that a cybersecurity incident is something that can both be malicious/unlawful or maybe non-malicious but has unintended impacts to operations or safety, organisations must plan for how to deal with these issues.

Mitigation

Goal: Activities are performed to prevent escalation of an event, mitigate its effects, and eradicate the incident.

The incident response and coordination of cybersecurity activities is often complex and challenging for many organisations. It requires an organisation to meet its business and operational needs as well as national regulatory requirements. This includes communicating with external public and private entities to share relevant information.

Recovery Planning

Goal: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

A well-planned and practiced recovery process will build a sound foundation in the event of a recovery being required. A recovery can be as small as from a single malware incident through to a complete disaster recovery scenario.

Planning all procedures, mitigations and resources required are key to building a sound recovery solution regardless of the scale of the incident.

Excellence in Cybersecurity

The adoption of a standard-based maturity model simplifies the Oversight processes, facilitating a loyal, open and trusted relationship with the competent authority. Furthermore, it gives the key to understand how ENAV takes information security seriously, considering it the expression of the “duty of care” connected with the safeguard of relevant public interests, including the protection of the human life on board on the ground, the efficiency and regularity of the transport by air and the protection of an essential service.”

Francesco di Maio, ENAV

The Cybersecurity SoE is essentially a maturity model. Maturity models are a highly simplified (but still useful) view of reality. They are not the same as a detailed audit, gap analysis and/or review, which still serve crucial purposes in cybersecurity.

Who is the Cybersecurity SoE for?

The SoE is for Chief Information Security Officers (CISOs) and/or cybersecurity managers (and similar roles) to use. Given the simplicity of the results, and focus on the most critical elements, the audience of the SoE is most likely to be top management.

How can the Cybersecurity SoE be used?

As a common reference in the ATM industry, four use cases are foreseen:

1. Comparing an ANSP to how it looked in the past, to track improvements over time
2. Comparing an ANSP to how it should look in the future after a roadmap of improvements has been completed to achieve a target level of maturity
3. Comparing ANSPs’ practices to develop and share good practice
4. Assessing suppliers and supply chain maturity

What is a Cybersecurity Standard of Excellence?

The *CANSO Standard of Excellence (SoE) in Cybersecurity* describes a range of functions that would be expected in an organisation with an effective approach to cybersecurity. Each function comprises a number of elements, which have a description of the kinds of activities and processes that would be expected, at different levels of cybersecurity maturity. An ANSP assesses its overall cybersecurity maturity and compares its own practices against those described in the maturity levels of each element, justifying the assessment with evidence to support the result. The Cybersecurity SoE also, where appropriate, defines improvement activities to obtain an increased level of maturity for each of the 13 elements.

Benefits of a Cybersecurity SoE?

The benefits of the Cybersecurity SoE include:

- It highlights the critical elements of effective cybersecurity. A vast number of activities must be done to manage cybersecurity risk; this SoE highlights those considered by industry experts to be the critical aspects. In reality, this is a mixture and tailoring of various wider standards and guidelines. Note that the model does not identify new requirements for ATM stakeholders – instead it is capability and process-based, leaving the determination of detailed requirements to each organisation.
- It allows comparison. The SoE is helpful as it is a common reference for comparison, either internally or externally, as per the use cases above. It specifically acts as a high-level summary for top management as it facilitates a harmonised approach across the ATM industry.
- It provides a summary of what excellence in cybersecurity in aviation looks like and is based on significant inputs from across the aviation industry and other safety-critical industries that may not otherwise exist in a single document.

The current CANSO Standard of Excellence in Safety Management Systems (SMS) does not address security vulnerabilities, yet an insecure system cannot be assumed to be safe since security vulnerabilities may add new causes to the existing safety hazards, or may add new hazards. Therefore, the Cybersecurity SoE complements the SMS SoE by focusing on cybersecurity. Safety and cybersecurity are different disciplines, but safety and security teams need to coordinate, and so the Cybersecurity SoE and other CANSO cybersecurity guidance help by highlighting best practices.

How has the Cybersecurity SoE been created?

In 2018 the EUROCONTROL Network Manager developed an ATM Cybersecurity Maturity Model in collaboration with several European ANSPs, in order to undertake a review of its own cybersecurity and that of its critical suppliers. A maturity model approach was taken to be able to compare suppliers. Sharing this model with the wider ATM community was a further objective and this has led to the creation of SoE by EUROCONTROL Network Manager in collaboration with CANSO's CSTF.

Is the Cybersecurity SoE based on a standard?

The SoE is based on NIST's Framework for Improving Critical Infrastructure Cybersecurity (CSF), together with some elements of the ISO27001 Information Security Management System (ISMS) standard. The NIST CSF was chosen as a pragmatic and widely-used standard. The 'Tiers' within the CSF were a helpful starting point, and linked (crucially) to a wider target-setting process that encompasses an organisation's business objectives, threat/risk environment, and requirements and controls.

The CSF was extended to emphasise leadership and governance, drawing on ISO27001. The role of human factors in security has also been emphasised. The purpose of the model is to highlight the most critical elements in the ATM context – it should not be seen as a replacement for applying the whole standard. Traceability with the NIST CSF can be found through the EUROCONTROL publication of the maturity model.

What do the maturity levels represent?

The levels of maturity in the Cybersecurity Standard of Excellence are the same levels used in both the CANSO Standard of Excellence in Human Performance Management (SoE in HPM) and the CANSO Standard of Excellence in Safety Management System (SoE in SMS). There are five maturity levels defined, increasing from Level A to Level E where each level is described as follows:

- A Level A – Informal Arrangements**
Cybersecurity processes and / or requirements have not been agreed at the organisation level – they are either not routinely undertaken or depend on the individual assigned to the task.
- B Level B – Defined**
Cybersecurity processes and/or requirements are defined but not yet fully implemented, documented or consistently applied.

- C Level C – Managed**
Cybersecurity processes and/or requirements are formally documented and consistently applied.
- D Level D – Assured**
Evidence is available to provide confidence that cybersecurity processes and/or requirements are being applied appropriately and are delivering positive, measured results.
- E Level E – Optimised**
Cybersecurity processes and/or requirements set international best practice, focusing on innovation and improvement. Feedback and improvement are embedded in the organisation. The effectiveness of the cybersecurity improvement actions is measured and evaluated against defined improvement criteria.

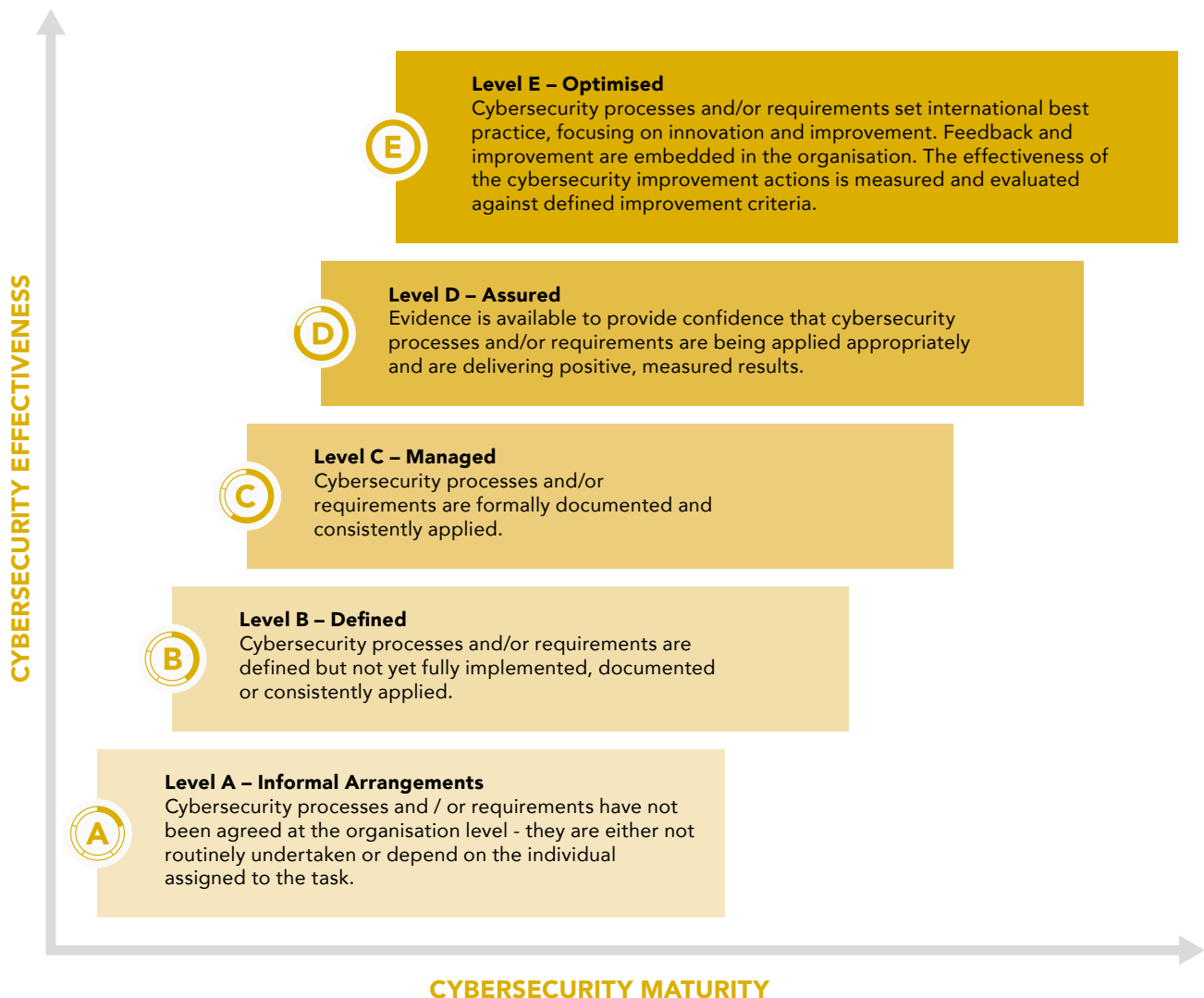


Figure 1: Cybersecurity Maturity and Effectiveness

What is the target level of cybersecurity maturity?

The model allows a broad assessment of strengths and weaknesses. Crucially it should facilitate discussions over improvement areas and the practices required to improve maturity. Achieving 'Level C – Managed' should provide an acceptable level of cybersecurity assurance for many ANSPs and is seen as the minimum target level.

However, the target maturity level for each element should be based on a variety of factors, including an ANSP's business objectives, threat environment and cybersecurity risks, regulatory and other requirements.

How do I use the Cybersecurity SoE?

The high-level model is a maturity assessment with thirteen elements and five maturity levels. For each level of maturity, there is a series of statements which describe what will be in place once an organisation reaches a particular level of maturity. All organisations start at 'Level A: Informal Arrangements' and, as they become more mature, progress to 'Level B: Defined' and then on to higher levels of maturity. An organisation must fulfil all elements of one level before it is possible to move to the next level; i.e. it may be possible to fulfil some elements at a higher level but the assessed level relates to that level at which all elements are fulfilled.

Note that the selected elements are the ones that are seen as most important and relevant. Appendix A contains a scoring form to complete which includes columns to populate with rationale and evidence. Each element also has a set of 'probing questions' that can be used to challenge the organisation through more open questioning.

The selected elements, and the definitions of the levels, are independent of specific cybersecurity threats and risks faced by an ANSP or supplier. Threat and risk assessments will always be required, for a proper, tailored approach to cybersecurity, and the CANSO Cyber Risk Assessment Guide is an introductory guide to doing this.

What inputs are needed for the assessment?

A wide variety of expertise and documentation is necessary to complete and evidence the assessment. This includes, but is not limited to, policies, procedures, records and system-level documentation.

Of critical importance is for every ANSP to already know what their top-level cybersecurity requirements are. These requirements come from ICAO Annex 17, internal policy and business objectives, regional or national regulations, national threat assessments, etc. These top-level requirements should then be decomposed into more detailed requirements for controls.

Who needs to be involved and how long does it take?

The maturity model enables quick assessment by someone who has a suitably broad overview of the organisation. Allocating a minimum of half a day, just for a CISO and their team, is advised.

However, given the broad and holistic nature of the maturity model, assessments from a wider range of perspectives, including from technical and operational personnel, will often be needed and will inevitably take longer, particularly on first use. Recurring assessments should take less time.

Discussion and insight arising from any differences in perspective are a key benefit of the assessment. It is therefore recommended to invite all parts of the organisation to contribute and review the assessment.

The Cyber Maturity scheme was a good opportunity for DSNA to confront different internal perspectives on our efforts to integrate cybersecurity. Indeed DSNA has been working from the start in the implementation of the NIS Directive in France with other aviation stakeholders. We are running a major technical and organisational programme to improve and better integrate all relevant security controls into our Integrated Management System. The maturity scheme was answered by several people, manager, ATM infrastructure expert and IT-cyber expert, and the outcome was relatively homogeneous. This provided a good check on our progress, together with a comforting view regarding applicability of the chosen standards in relation to others in this field. Additionally, the maturity scheme was deemed to be of good quality and aligned with the views of our National Cyber Security Agency, ANSSI.”

Stéphane Deharvengt, DSNA, Deputy head Safety, Quality and Security Management

Can I assess a single system or department?

If a more in-depth application is desired, then assessments can be undertaken on a scope smaller than the entire organisation: for example, an assessment could be undertaken on each organisational department or each critical system (or even sub-system). Depending on organisation and architecture, some questions will still be answered for the whole organisation, whilst others will be anchored on the specified scope.

If doing an in-depth assessment and a single, top-level result is required then it is possible to combine each corresponding score. Whilst averaging might be the most obvious way of combining the scores for each element, it is recommended to report the minimum score of each element, as in cybersecurity the principle of being only as strong as the weakest link applies.

As already stated, the SoE is not a replacement for detailed audits, gap analyses, system reviews, vulnerability scanning, penetration testing, etc.

The capability maturity model enables the trusted relationship with suppliers – especially for those defined “critical” – defining the terms of reference and the expected level of services, aligned with the institutional mission of any ANSP.

Francesco di Maio, ENAV

How is a supplier assessed?

Assessment of a supplier can be done by the supplier itself, or by the customer or a third party. For suppliers it is important to note that there is often one score for their IT infrastructure and another for their product, so it is important to specify which is of interest. Given the SoE is not a replacement for detailed audits, gap analyses and/or reviews, assessment of a supplier using the SoE is not a replacement for contractual reviews and audits, nor should it be used as the sole basis of the assessment of cybersecurity elements of a contract.

How could the results of the SoE be presented?

The following is an example of how the results can be presented to senior management. Figure 2 shows an example assessment of an ANSP and five of its suppliers. The suppliers have been ordered by overall maturity.

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Ident ity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

Figure 2: Example Assessment

What to do with the results of the SoE?

The model should give a broad assessment of strengths and weaknesses, and specifically where there are gaps between current and target maturity. Improvements can be identified and placed into a

roadmap to increase maturity. As well as the advice earlier and later in this SoE, the NIST CSF guidance on establishing and improving a security programme can be used and adapted (as in the Figure 3) if required. Specific metrics may be needed to track improvements in particular elements.

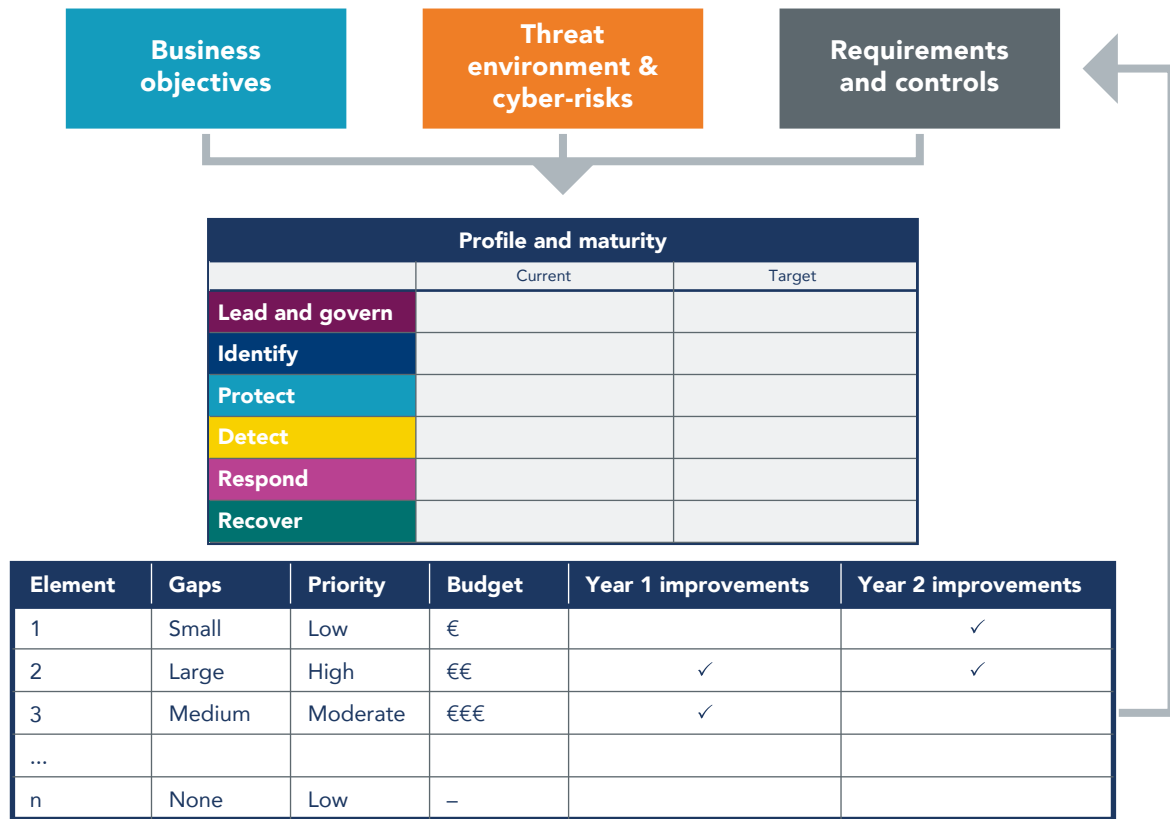


Figure 3: Gap Analysis and Roadmap

What is the added value of the Cybersecurity SoE compared to ISO 27001?

The Cybersecurity SoE adds value even if your organisation's Information System Management System (ISMS) is fully compliant with ISO 27001 requirements. The Cybersecurity SoE has been specifically designed to meet the needs of an ANSP, whereas ISO 27001 is industry agnostic. In addition, the SoE provides a structure for continuous improvement of an organisation's cybersecurity maturity based on the concept of a maturity model approach.






We have applied this maturity model successfully to our IT systems: it has certainly provided a global view of our situation and challenges, as well as a high-level perspective, understandable to the management team.






We believe that it is a useful and effective tool, easy to apply, and one which we can gradually approach the complexity of cybersecurity of critical processes, systems and technologies involved in the provision of Air Navigation services.






We are convinced that, as the model evolves, it will become increasingly useful, practical and it will be widely used by multiple aviation stakeholders.






Gerardo Sarmiento Fernández, ENAIRE,
Responsable de la Oficina de Ciberseguridad /
CISO División de Seguridad






Definition of Maturity Levels

		Maturity levels					
Element	Description	 A Informal Arrangements	 B Defined	 C Managed	 D Assured	 E Optimised	
LEAD AND GOVERN	Leadership and Governance	Senior management demonstrate leadership and commitment to cybersecurity. The policies needed to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	No overarching policy, strategy or plan	Policy established, together with parts of a strategy or plan; roles & responsibilities are established but no or weak link with top management	Policy supported by a strategy and plan approved by top management; key risks are accepted by top management	Plan is funded and, with visible top management commitment, delivering intended improvements across the organisation	Updated regularly to reflect progress, threats and risks
	Information Security Management System (ISMS)	The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives.	No documented ISMS	Parts of an ISMS documented, resourced and applied, but independently of other depts/systems	Fully operational ISMS, that is externally audited and with links to other parts of the security management system and the QMS and SMS	Certified ISMS, with KPIs defined and tracked, and ISMS/ QMS/SMS processes are coordinated	Regular review against new good practices; KPIs show continual improvement; Certified Integrated Management System (IMS)

		Maturity levels					
Element	Description	 A Informal Arrangements	 B Defined	 C Managed	 D Assured	 E Optimised	
IDENTIFY	Asset Management	The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organisation's risk strategy.	No formal inventory of systems, their interdependencies and interfaces	Ad hoc, not formalised	All critical systems and interfaces are identified and described in a consistent way with clear owners	Interdependencies are well-understood and there is regular review and updates	Automated updates as the environment changes
	Risk Assessment	The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, including system-of-system aspects resulting from dependencies.	No documented risk assessment processes or assessments	Ad hoc; no formalised assessment process	Management-approved processes that lead to cybersecurity requirements being identified	Consistent, organisation-wide application with identified risk and requirement owners; external validation of risk levels by authorities; Security risk assessment is taken into account in safety risk assessment, and vice versa	Continual review and linking of risks to latest vulnerabilities and threats; assurance that system-of-systems aspects are addressed
	Information sharing	The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties	No, or very limited, cybersecurity information sharing	Using some threat intelligence and vulnerability information; Informal information sharing internally and externally where appropriate	Trends are identified; Internal and external sharing based on formal processes linked to risk assessment, vulnerability management, response and recovery processes; Relevant risk information is shared between safety and security functions	Threat intelligence and vulnerability information for all critical systems; Consistent, widespread and effective sharing between all relevant parties.	Information sharing is habitual and proactive; demonstrable leadership in improving industry-wide information sharing

		Maturity levels					
	Element	Description	 A Informal Arrangements	 B Defined	 C Managed	 D Assured	 E Optimised
IDENTIFY	Supply Chain Risk Management	The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.	No complete overview of all suppliers / partners	Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cybersecurity maturity	Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance	Requirements placed on suppliers with proportionate compliance checks and processes / penalties / measures for non-compliance	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices
	Identity Management and Access Control	Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access.	No access controls on critical systems or areas	Access controls on some critical systems and areas	Access controls on all systems and areas and linked to logs	Consistent controls within organisation-wide approach, including supply chain	Regular updates against new good practices
PROTECT	Human-Centred Security	The organisation's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Security is part of the organisation's culture.	No awareness/training programme	Ad hoc activities to inform and educate	Coherent programme in place that addresses whole organisation, including addressing human factors and organisational culture	Sustained activities with follow-ups, differentiated for different roles, leading to increasing compliance and performance	State of the art syllabus, with systematic testing, leading to routine and proactive cybersecurity risk reporting from staff

Maturity levels							
	Element	Description	 A Informal Arrangements	 B Defined	 C Managed	 D Assured	 E Optimised
PROTECT DETECT RESPOND	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Systems and processes are designed to be sensitive to the additional workload created by cybersecurity requirements.	Primary reliance on network boundary protection	Some requirements for technical controls are defined upfront, supporting the ‘security-by-design’ principle; some non-essential services are disabled	Requirements for technical controls are defined and implemented; the principle of least functionality is also implemented (e.g. non-essential services are turned off) on all critical systems	Technical controls are demonstrated to be effective; Security architecture with virtual separation implemented and effective; Full control over technical infrastructure; Implementation designed with the human in mind, making it ‘easy to do the right thing’ and ‘hard to do the wrong thing’	Security architecture can adapt dynamically to changing threat and risk landscape
	Anomalies and Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	No documented procedures or controls	Ad hoc and typically manually	Suitably resourced controls are in place to detect anomalies and events; some detection is automatic; penetration testing flags missed positives	Procedures to reduce false positives; resourcing includes safeguards and/or emergency cover	State of the art detection capabilities are combined with additional mitigations when new threats are known not to be detectable
	Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	No plans exist to respond to security anomalies	Plans exist with high-level responsibilities	Well-defined responsibilities at all levels, 24/7/365 reaction times based on logic and agreements with suppliers / partners; violations of plans are addressed	Exercises and audits drive improvements in plans; resourcing includes safeguards and/or emergency cover; information sharing includes voluntary sharing with other parties	Response planning is widely coordinated, frequently exercised and updated, drawing on new good practices and knowledge

		Maturity levels					
	Element	Description	 A Informal Arrangements	 B Defined	 C Managed	 D Assured	 E Optimised
RESPOND	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Incidents cannot be contained or mitigated; there is no graceful degradation of services	Some incidents can be contained or mitigated without full loss of services; in some cases full loss of services cannot be avoided	Incidents can be contained and/or mitigated with minimal service loss; Sites have appropriate manual disaster recovery services	Sites have automated disaster recovery services with limited (or no) human intervention; data breaches and loss of data integrity have well-rehearsed mitigations	Mitigations are monitored, regularly tested and adapted to ensure alignment with the operational environment; Automation exists to address incidents before they are apparent to humans; Self-healing exists
	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	No recovery procedures established for cybersecurity incidents	Procedures exist for some systems	Procedures exist for all critical systems, together with backups for systems and data to recover from outages	Regular testing of procedures, including communication with internal and external stakeholders	Lessons identified from exercises and incidents (both internal and external) drive updates in policy and procedures
RECOVER							

Advice and Lessons Learned

For each of the capabilities in the maturity model, advice on getting started and lessons learned to improve maturity are given. References to standards and other documents are also given – these provide a foundational understanding. They include ICAO guidelines for the aviation community and standards/frameworks that have been widely accepted by both governments and industry that should be tailored to meet the unique needs of the organisation. In combination, the advice and lessons learned should support the progress towards greater levels of cybersecurity maturity.

Leadership and Governance

References

References to cybersecurity standards do not generally help with leadership and governance issues. Obtaining senior management commitment to cybersecurity activities requires understanding of your organisation, both in terms of policies but also the softer aspects of influence and change.

Getting Started

- **Raise awareness:** Activities and campaigns should be run to raise senior management's awareness of cybersecurity threats and potential consequences to safety, continuity of operations and finance.
- **Identify top-level responsibilities:** Current roles and responsibilities of executives should be reviewed. Furthermore, it should be considered how their roles could be extended to include cybersecurity responsibilities. Organisational structures may need to be changed in order to accommodate cybersecurity responsibilities.
- **Encourage management peer learning:** Management should be encouraged to discuss with managers from other organisations, that have started their cybersecurity journey, to learn about how they set up an ISMS and overcame early challenges.

Lessons Learned

- **Provide management with a 'big picture' of cybersecurity plans:** An overview of what the ANSP wants to achieve should be provided as well as steps that should be taken to achieve these goals. This includes actions and milestones across the security incident lifecycle: plan, protect, detect, respond and recover.
- **Combine cybersecurity with safety:** An effective way to raise awareness is to combine cybersecurity with safety – highlighting how security vulnerabilities can undermine the safety of operations.
- **Use metrics to raise awareness:** Regular management reports on a range of cybersecurity threats to your organisation should be provided, for example, the number of firewall breach attempts, the number of unpatched systems, the number of security incidents, etc.
- **Show the return on investment:** As implementing an information security management programme will require resources, it is important to demonstrate benefits. This can be hard as good security prevents incidents that would otherwise have happened, so the benefits are not always visible or tangible. Showing how the above metrics improve, and how the programme reduces risks, are ways of showing the return on investment.

Information Security Management System (ISMS)

References

- ISO 27000 gives a general description, including describing an ISMS (sub-section 4.2) and critical success factors for an ISMS (sub-section 4.6)
- ISO 27001 gives auditable requirements for an ISMS
- NIST CSF is a framework but effectively equivalent to an ISMS

Getting Started

- **Decide which standard to use and commit to it:** Many standards and frameworks are available (ISO, NIST, etc.) and some people have a strong preference. However, they are broadly equivalent and mappings between them are available to help determine which is best for your organisation (e.g. the NIST CSF maps to ISO controls, and vice versa). Committing to implement a standard is much more important than which standard is chosen.
- **Obtain commitment from senior management:** Implementing an ISMS is not easy or quick, and so strong and continuing management commitment is needed. A case will need to be made to senior management, usually addressing both the financial and resource needs, and a senior management sponsor should be appointed.
- **Develop a security policy and identify key stakeholders:** A security policy states the intentions and directions of senior management. It provides a foundation on which to build the ISMS. The policy will identify the responsible roles for the ISMS, for example the accountable manager, process owners, etc. Knowing the key stakeholders is essential to building the ISMS, and starting the conversation about the policy will help to identify the key stakeholders.

Lessons Learned

- **Take your time:** Most ANSPs will already have parts of an ISMS, but it still takes time and effort to build a complete, functioning and effective ISMS. For most ANSPs, expect it to take around two years.
- **Have a clear and enduring reason for developing an ISMS:** The initial decision is not enough. Security benefits are hard to quantify, and security is like safety – if done right, nothing will happen and operations will continue normally. An ISMS needs strategic endorsement from budget holders, and ideally also regulators.
- **Ensure that the scope of your ISMS is clear:** An ANSP's ISMS should cover the whole operational environment and dependencies. However, an ISMS can start on a smaller scale. Irrespective of whether starting with the operational environment and/or the business/administrative environment, make sure the scope of your ISMS is clear to everyone.
- **Pilot procedures and processes before rolling out further:** Identify a candidate system/unit to trial procedures and policies. Initial procedures and processes are unlikely to be final so evolve them to meet organisational needs. At each step, refine the procedure/process. With this approach, the earlier an issue is corrected, the less significant its impact is likely to be.
- **Define the ISMS' relationship to, and interfaces with, your Safety Management System (SMS):** An ISMS and SMS cannot be independent, and indeed share many similarities. However, due to differences in the expertise and methods needed, an SMS and ISMS should not be combined into one management system, even if there are benefits in having safety and security managed within the same department.
- **Apply pressure on implementing policies to make the change:** Efforts may falter without a strong driving personality behind the ISMS. Referencing back to agreed policies gives authority to the change.

Asset Management

References

- NIST CSF (Asset Management (ID.AM))
- NIST Special Publication 800.53 CM-8
- ISO 27002 – Section 7 Asset Management
- CANSO Cybersecurity and Risk Assessment Guide has an example asset structure

Getting Started

- **Define what 'assets' means in the organisation:** Assets refer to the people, processes and technology within an organisation that are involved in day-to-day operations. There are several groups that should be considered: data, devices and services, facilities and people. These can be further split up into operational and administrative assets.
- **Establish a master asset list:** This captures all the asset information. Keep in mind that your assets may be IT systems, IT networks, buildings, people, meeting rooms, printers and scanners, processes, cloud services, etc. Asset management is continuous work and should always undergo regular review to ensure the asset listing reflects the latest information. A list of authorised hardware provides insight into the components that comprise an organisation's infrastructure, whilst a software inventory provides insight into the applications that are approved for use in the environment (and also supports white-listing).
- **Establish an Information Security Classification:** As well as developing an inventory of assets, the people who are responsible for each asset should also be identified. An example with three levels of classification could include "confidential – information for senior management only", "restricted – information for employees" and "public – information available to the public"

Lessons Learned

- **Spend enough time on asset management:** It is essential to distinguish between primary assets and supporting assets. Primary assets are the critical processes and information, required for continued operation. Supporting assets are the hardware, software, network and site as well as their operators. Even where there is good configuration management already in place, much coordination and explanation will be required to get all parties to contribute actively to build the asset lists.
- **Conduct periodic review:** Periodic review of inventories should be undertaken to ensure changes are updated. This facilitates vulnerability tracking and assessing the impact of newly discovered vulnerabilities.

Risk Assessment

References

- ISO 27005
- NIST CSF (Risk Assessment (ID.RA))
- NIST Special Publication 800-30
- NIST Special Publication 800-39
- ED-201
- EN 16495
- CANSO Cyber Risk Assessment Guide

Getting Started

- **Decide which risk assessment method or risk model to use:** The risk assessment method chosen needs to be in-line with the ISMS that will be implemented. This will ensure that the ISMS is cohesive.
- **Start simple:** Instead of a full security risk assessment for each asset, it is possible to start with a higher-level assessment covering operational assets, as long as this is eventually developed into a more detailed assessment. Similarly, a full review of an assessment may not be needed when making a change, it may be preferable to have a process that first decides if there are security-relevant changes and only then undertake the review.
- **Begin by defining the risk assessment process:** Definition of a security risk assessment process for an ANSP will take time, but it is a prerequisite for all other steps.
- **Scope each security risk assessment carefully:** Asset management is one of the main inputs to the risk assessment as it identifies assets that need to be risk assessed. The effort for each security risk assessment may vary depending on the complexity of the asset and the knowledge of the attendees. Once the asset list is known (covered in Asset Management, above) it may be possible to group things together to minimise the effort for each assessment.

Lessons Learned

- **Security risk assessment must to be integrated into many other processes:** It takes time to establish assessments as many ANSP stakeholders need to implement their part of the process. Interfaces from security risk assessment to safety, change management, legal, enterprise risk management, data protection, national authorities, suppliers, etc. will need to be defined. For change management, one possibility is to open a change request for the security risks identified for an asset; this way it is possible to make sure that the results of the security risk assessment do not only exist on a piece of paper.
- **It takes time to internalise the process:** Everyone needs approximately one year to internalise and adopt the process. Remember, that it also took several years to implement and embed safety into the organisation.
- **Be aware of the level of effort required:** If the right technical and operational experts are available, then it will take between 2 hours and 1 day for an initial assessment on each system. The risk assessment for a single application may be simpler. The risk assessment for a CNS-system installed at more than one site may be more complicated and may require deeper knowledge of the system.
- **Use software tools to help:** Tools can collect and organise information in the risk assessment process. It may be possible to initially execute security risk assessments using spreadsheets. As soon as security requirements are updated or risk assessments repeated because of changes to the ATM system it will be harder to track both the changes in your process and the changes to the security requirements and the corresponding risks for an asset.

Information Sharing

References

- NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations
- ISO 27005, Annex 9 and 11
- ICAO doc. 8973 section 18.1.6 (RESTRICTED)
- ICAO doc. 9985 Appendix A section 3.2, 3.3, 3.4 and Appendix B section 4.15 (RESTRICTED)
- Aviation schemes such as the EATM-CERT, ECCSA and A-ISAC

Getting Started

- **Identify internal and external stakeholders within the cybersecurity domain:**
Identifying internal stakeholders will ensure that all relevant subject matter experts (SMEs) are updated and involved in the cybersecurity work. Knowing the external stakeholders (regulator, key suppliers and partners, etc.) ensures that information flows between essential functions inside and outside of the company. National regulations may specify requirements for information sharing which should be complied with.
- **Use online resources:** A cost-effective way to get information from the cybersecurity domain is to make use of online resources. These online resources will provide the SMEs within the organisation with better insights into current methods of attack. This again will make it possible to guide senior management to a risk-based approach to decision making.
- **Establish an information sharing protocol:**
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. This allows stakeholders to commit to sharing information and intelligence openly, yet securely, to increase overall situational awareness of cybersecurity threats within ATM. A common example for information security classification is provided in the element "Asset Management".

Lessons Learned

- **Establish a good reporting culture and incident management:** Centralised incident management is essential to have a structured, standardised approach to mitigate cybersecurity attacks and to keep senior management informed. This requires dedicated resources in the organisation and a competence scheme for the individuals involved.
- **Recognise that maturity will come with time and resources:** The safety domain has developed over a long period and therefore many mature processes and a robust culture have developed. Existing safety reporting processes should be used to build a strong security reporting culture. This ensures that issues are followed up within the organisation and that relevant information is shared with relevant parties.

Supply Chain Risk Management

References

- NIST CSF (Supply Chain Risk Management (ID. SC))
- ISO 27002 Section 15 – Supplier Relationship

Getting Started

- **Educate your procurement/purchasing department:** They need a basic understanding of cybersecurity and to understand all relevant and applicable legal requirements (e.g. export rules). They also need to know that the cybersecurity chain is only as strong as its weakest link and that the subcontractor is one of the links in the chain.
- **Identify the security requirements that you expect your suppliers to meet:** Appropriate security requirements should be identified and flowed down to the suppliers. It is recommended to collaborate with suppliers to ensure requirements are interpreted correctly and agreed. A means will need to be established to share protected information, such as an NDA.
- **Evaluate your suppliers' cybersecurity maturity:** This Standard of Excellence can be used as a starting point. Even if suppliers do not formally possess the certification that is expected, they can still be mature. Equally, just possessing a certificate does not necessarily make them mature.

Lessons Learned

- **Be aware of the cost:** There are costs associated with improving cybersecurity and suppliers may seek to recover these costs. However, in the long term it is more cost effective to implement cybersecurity measures correctly from the beginning. The cost of not addressing cybersecurity threats will become prohibitive when an incident occurs.
- **Include cybersecurity in the contract:** Without provisions for addressing cybersecurity in contracts, suppliers may not prioritise cybersecurity requirements over other requirements.
- **Be precise:** Requirements that apply to ANSPs are often too generic for subcontractors, so requirements should not be blindly flowed down, but adapted as necessary. This is equally true for complete guidance documents and standards, if only a section of those is actually applicable. Only the sections that are relevant should be referred to. More specific requirements are more likely to be understood and implemented correctly. This saves all parties time, effort and money.
- **Let the cybersecurity professionals communicate directly:** Identify the people responsible for cybersecurity across all stakeholders and encourage them to communicate directly.
- **Adopt a collaborative approach:** Suppliers are on the same learning curve and increasing their cybersecurity maturity. Agree on a roadmap for improvements to the product/ system/service security controls and underlying architecture.

Identity Management and Access Control

References

- NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations
- ISO 27005, Annex 9 and 11
- ICAO doc. 8973 section 18.1.6 (RESTRICTED)
- ICAO doc. 9985 Appendix B section 3.2 (RESTRICTED)

Getting Started

- **Review access privileges to assets on a regular basis:** Reviews should be on a role-based approach with emphasis on privileged users. Primary assets are identified as the organisations' most valued assets, and therefore senior management should ensure that asset owners are focused on keeping access privileges updated and that strict procedures for gaining access are implemented and followed.

Lessons Learned

- **Implement centralised access control and monitoring:** This ensures standardisation and that management of access privileges is the responsibility of the asset owners. Centralised services are recognised as a more cost-effective management approach than local administration. The centralised service also facilitates exchange of lessons learned between SMEs. Access control policies are more easily implemented in the organisation and standardisation of systems is maintained by the same centralised service.
- **Recognise that maturity will come with time and resources:** Designing and implementing centralised access control and monitoring are time consuming tasks. The rewards from the time invested include less administrative burden, more control of user accounts/permissions and better visibility of activities on your assets. It takes many years to build a layered solution and it should be in continuous evolution.

Human-Centred Security

References

- ISO 27001 / ISO 27002: Annex 7.2.2
- NIST Special Publication 800-53: AT-1, AT-2, AT-3, AT-4
- ICAO 8973 section 18.1.6 (RESTRICTED)
- CANSO Standard of Excellence in Human Performance Management

Getting Started

- **Promote the policies and procedures that employees should follow:** Check that appropriate policies and procedures are in place and that they are followed consistently. Any shortfall provides the basis for an awareness raising campaign for employees.
- **Relate awareness campaigns to the current cybersecurity environment:** This can be the global environment and within the ANSP sector. Monitor the information sharing channels to identify current threats and events and use this information to publish timely additional training.
- **Perform background checks of employees with privileged access:** Additional checks carried out on employees that have physical or logical access to assets will help to identify if a person's history may present a future insider threat.

Lessons Learned

- **Establish a robust training programme:** The training programme should consist of documentation, training sessions and videos. Employees need to understand the value of sensitive information and their role in keeping it safe. Employees need to know the policies and procedures they are expected to follow in the workplace regarding cybersecurity. Training should be tailored to each user's environment, tools, roles and risks that relate to their area of work. Core topics include legal responsibilities, phishing, viruses and malware, insider threats, social engineering, handling sensitive information assets and how to report and respond to an actual or suspected cybersecurity incident.

- **Draw lessons from a more mature organisational group:** Implement the training programme with the use of lessons learned from a more mature group within the organisation such as Safety. If Safety or other groups already carry out training programmes or campaigns, consider joining these efforts together for a more consistent employee training experience. Develop the training materials using the methods and materials that are known to work in other organisational groups.
- **Add cybersecurity training to your onboarding process for new employees:** New employees are potentially unaware of the cybersecurity threats and impacts faced by ANSPs. Ensure a training module for every new employee is dedicated to cybersecurity awareness, best practice and common threats. New employees should also be aware of their responsibilities to cybersecurity and how to react and report in the event of experiencing a cybersecurity incident in their role.
- **Cybersecurity training should be refreshed and provided on a regular basis:** Refresher training should be at least annually. Security awareness is only effective if it is regularly practiced, due to the evolving cybersecurity landscape.
- **Provide a proportionate level of controls:** Excessive controls on systems and services may lead employees to circumvent the controls. Policies and technological controls that still allow employees to effectively collaborate and do their work will help prevent accidental data loss. A prime example of this would be blocking all file sharing versus allowing file sharing with controls such as monitoring and encryption.

Protective Technology

References

- ICAO 9985, Appendix B, Chapter 3 and 4
- ISO 27033-1-2015, Network Security Part 1
- Overview and Concepts
- Center for Internet Security (CIS), CIS Benchmark
- NIST National Vulnerability Database

Getting Started

- **Make use of free online resources:** These can help with the understanding of the cybersecurity landscape: For example, MITRE publishes the current vulnerabilities and exposures for many products which help to understand what should be patched or updated to mitigate risk. The Cybersecurity and Infrastructure Security Agency (CISA) publishes alerts on new vulnerabilities that have been announced, some may be critical and require early attention.
- **Use existing measures:** Some mitigating defences are critical to business continuity in an ATM environment and also affect safety. Redundant systems should enable continued safe operation despite a cybersecurity incident. These redundant systems should ensure continued availability of mission-critical services such as voice communications. Networks used for critical systems involved in ATC should be segregated from networks that allow public access. Backups are critical as a final line of defence in the event of a system compromise. If compromised, a system may require reconstruction from backup and configuration information.
- **Perform a physical risk assessment:** Cybersecurity cannot be achieved if physical security is compromised. Secure assets by restricting access based on a need to access basis. The system cannot function if electricity supplies or network connectivity are disrupted. If assets are switched off incorrectly or network cables are unplugged from the operational network, then this will also undermine the system's functionality.
- **Update anti-malware definition regularly:** Every anti-malware engine has to be updated to detect new malicious software.

- **Focus on the systems with the highest risk:** Retrofitting security to every legacy system is expensive and time-consuming, though necessary in the long-term (unless migrated to new technology). Start with high-risk systems, especially those that are externally facing.

Lessons Learned

- **Perform regular vulnerability scanning:** Vulnerabilities are weaknesses in the system which could be exploited by threat actors who have access to the asset. Frequently, new software and device vulnerabilities are publicly disclosed. ANSPs need to resolve these vulnerabilities faster than potential hackers can exploit them. End of Life (EoL) software is most vulnerable as there are no security bug fixes available to resolve any new publicly disclosed vulnerability. The vulnerability scanner definitions also have to be updated to detect new vulnerabilities. A test/development environment should be used to simulate the operational environment for deployment of system updates.
- **Harden systems:** System hardening is a technique implemented to reduce the attack surface and vulnerabilities in application, server, operating system, database and network components. Unnecessary services should be disabled. Users should be given the minimum privileges necessary to perform their tasks. The Center of Internet Security (CIS) benchmarks, or similar, should be referenced to harden the system. System hardening should also be applied to systems provided by suppliers before being deployed.
- **Design and build a layered 'defence in depth' strategy:** An initial assessment of the system's defences should be performed and further layers of defence added as necessary. Having multiple layers of protection means any potential attacker has more barriers to overcome.
- **Perform system architecture review and network segregation:** Review the data flows in the system and apply the principle of least privilege for system access. Assets with different functionality should be segregated by different networks while those with similar functionality should be grouped in the same

network. Firewalls should be placed between different networks and configured to allow authorised traffic only to pass through. This can be difficult when there are legacy systems, but it is necessary to provide a more robust layer of defence.

- **Aim for agility:** Protection techniques should be agile; that is, they should be able to quickly change and adapt to an ever-changing threat. This requires the organisation to use emerging technologies.
- **Implement at an enterprise-wide level:** While some aspects of security must be built into individual systems, enterprise solutions can be implemented 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.

Anomalies and events

References

- ISO 27001 / ISO 27002: Annex 12.4
- NIST Special Publication 800-92
- ICAO 9985 Appendix C table C-9 (RESTRICTED)

Getting Started

- **Aim for a centralised location for gathering log data:** This should be a single, non-repudiable location. Log data will only provide useful information when combined and triaged against other data.
- **Regularly review the captured data:** Events captured by your system will provide no value in preventing an attack if they are not regularly reviewed and correlated. Thresholds for event types will help identify unwanted events.
- **Generate regular reports from the captured data:** Weekly or monthly reports will help to identify any common patterns in the systems and infrastructure. Regular reports can also provide senior management with further data and visibility of the operations cybersecurity landscape.

Lessons Learned

- **Make use of existing safety procedures as far as practicable:** Have a process in place that details the steps for cybersecurity event analysis. Existing safety processes will be able to assist in creating processes for handling cybersecurity events. A close relationship between the two processes keeps procedures consistent and effective.
- **Choose a centralised monitoring tool or Security Information and Event Management (SIEM) solution:** This can analyse live data and automatically produce alerts upon detecting anomalies and works across multiple (compatible) systems. When choosing a SIEM, consider the data formats that operational systems provide and how these can be interpreted. For systems that are air-gapped, a process for collecting and storing the log data from these will avoid any gaps in event triage. Wherever possible, the collection of log data should be automatic to prevent any delays in threat detection. The sources of log data should not be limited to computers and servers, they should also include infrastructure and application layers where appropriate. The wider the scope of data collection, the greater the visibility of operational activity as well as security.

Response Planning

References

- ICAO 8973 Chapter 4 and 18.4 (RESTRICTED)
- ICAO 9985 Chapter 1 & 2 (RESTRICTED)
- ISO 27001/27002: Annex 16 & 17
- NIST Special Publication 800-61
- NIST Special Publication 800-37
- Internet Security Forum – “Standards of Good Practice” modules TM 1 & 2, BC 2, SI 1 & 2
- CANSO Emergency Response Guide

Getting Started

- **Identify roles and responsibilities:** Roles and responsibilities should be identified and assigned for each part of the organisation. The scope of the responsibilities should be clearly defined and documented, including a role with ultimate responsibility, should the event fall outside any documented processes. Event response should include roles and responsibilities for individuals involved, a procedure that should be followed that states which actions should be performed and when.
- **Ensure effective communications:** Communication paths, both internally and externally, should be defined and documented, and include any regulatory compliance reporting requirements. The communication paths should be continually evaluated, validated and updated as required. If an event should occur, communication to key stakeholders, such as airspace users, regulators and the media should be managed.
- **Have a long-term plan for improvement:** Response planning and implementation should be continually developed, adapted and evolved to meet the organisation’s needs. Changes in the operational environment or regulatory changes require updates to the plan.

Lessons Learned

- **Use all communication channels:** Communication should include widely used channels, such as social media, to provide status updates of any incidents that may have occurred, as well as the resulting impacts on service delivery.
- **Establish continual validation and training:** This should consist of documented policies, processes and procedures, human resources, effectiveness of technical tools and solutions and awareness of the legal framework. One of the commonly performed means of validation is tabletop exercises, which should be performed by the organisation at least annually, with all stakeholders involved. The plan should be adapted as the operational environment changes throughout the year as these changes may not be reflected in tabletop exercises.

Mitigation

References

- NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations
- ISO 27005
- ICAO doc. 9985 Appendix A section 2.25 and appendix B section 2.8 (RESTRICTED)

Getting Started

- **Identify roles and responsibilities:** Making decisions is difficult during an incident scenario, so there should be a role defined with ultimate responsibility for incident management. Event response should include the roles and responsibilities for individuals involved, a procedure that should be followed which states which actions should be performed and when.
- **Plan responses:** Having good documentation of each ATM system component and its means of connectivity throughout the system will pay dividends. This document should include mitigating mechanisms, procedures to be followed and incident response plans in the event of system loss.
- **Make all employees aware of how to report an incident:** All employees in the organisation should know how to report an incident so that detailed records of activity can be gathered. This could be as simple as a phishing attempt but may show a larger scale activity taking place.

Lessons Learned

- **Perform testing:** Test your incident response mitigations, these are better tested in a non-operational environment and refined before being tested in operational environments. Individuals involved should know their roles, what is expected of them and the actions they should perform in the event of an incident.
- **Perform user awareness training:** Confirm that users understand how to identify incidents, raise incidents and that they follow the appropriate procedures.
- **Conduct analysis of your incident response:** Confirm that your response plans worked as intended and if not, update to address any shortfalls. Confirm that your incident response team acted as intended and if not, update the training programme to address any shortfalls. Plans and training programmes should be updated and retested periodically, to reflect the current threat landscape.

Recovery Planning

References

- NIST Special Publication 800-61: Computer Security Incident Handling Guide
- NIST Special Publication: 800-34: Contingency Planning Guide
- ISO 27035: Information Security Incident Management

responsibilities, obtain input from all areas of the organisation, ensuring that senior management are involved in the process. Include plausible scenarios to cover as many eventualities as possible. Expand the scope of the recovery plan to address each critical system ensuring that supporting assets are included.

Getting Started

- **Focus preparation on your primary assets:** The primary assets allow the organisation to operate and therefore are of utmost importance in terms of recovery. Create backups of configuration data and other critical information to bring the asset back online or restore to a working state. Document procedures for recovery and configuration of assets.
- **Create a recovery plan, starting with a single system:** Include key employees in the planning process. Document roles and

Lessons Learned

- **Perform testing:** Test your recovery plan in a non-operational environment. Check that backups function and configuration data is correct. Time the process and ensure it matches the documentation. Individuals involved should know their roles, what is expected of them and the actions they should perform during the recovery process.
- **Align plans with safety plans:** The recovery plans should work in conjunction with the safety plans and should include input from the safety manager.

Conclusions

Cybersecurity is a fundamental part of ATM security and, more generally, of overall aviation security. Cybersecurity receives specific consideration in the general legal framework contained in Annex 17 (Security) to the Chicago Convention. Furthermore, 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 will 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 that a high level of security is achieved by the aviation industry as a whole. This can be achieved not only by ensuring that the infrastructure which comprises the ATM system is resilient to attack, but also that the ATM system will provide information that can be used by other organisations to protect air transport and the aviation system as a whole.

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
LEAD AND GOVERN	Leadership and Governance				<ul style="list-style-type: none"> Do you have an approved policy, strategy, plan and budget? How is the whole organisation aligned with them? Who is responsible for what? How do you ensure that security is integrated into all operational processes? 	<ul style="list-style-type: none"> Do you have an approved policy, strategy, plan and budget for securing the product/service? How is the whole organisation aligned with them? Who is responsible for what? How do you ensure that security is integrated into all processes that deliver the product/service?
	Information Security Management System (ISMS)				<ul style="list-style-type: none"> What standards(s) do you use? How is the ISMS coordinated/integrated with the QMS/SMS? How do you measure the effectiveness of the ISMS? 	<ul style="list-style-type: none"> What standards(s) do you use? If there is a supporting ISMS, how is it coordinated/integrated with the QMS/SMS? How do you measure the effectiveness of the ISMS?

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
IDENTIFY	Asset Management				<ul style="list-style-type: none"> • How many critical systems / assets do you have? • How do you label physical and data assets? • What are their dependencies? • What is your patching policy? • How do you identify and trace vulnerabilities? 	<ul style="list-style-type: none"> • How many critical systems / assets do you have for delivering the product/service? • How do you label physical and data assets? • What are their dependencies? • What is your patching policy? • How do you identify and trace vulnerabilities?
	Risk Assessment				<ul style="list-style-type: none"> • How do you identify and assess threats? • Is there a process that identifies, assigns and tracks cybersecurity requirements? • How do you ensure that the process works? • What is your organisation's risk tolerance? 	<ul style="list-style-type: none"> • How do you identify and assess threats? • Is there a process that identifies, assigns and tracks cybersecurity requirements? • How do you ensure that the process works? • What is your risk tolerance your own organisation and your customers?

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
IDENTIFY	Information sharing				<ul style="list-style-type: none"> Who do you share risk information with? 	<ul style="list-style-type: none"> Who do you share risk information with?
	Supply Chain Risk Management				<ul style="list-style-type: none"> How do you determine the level of trust you have with different suppliers / partners? How do you ensure the right requirements are placed on suppliers? How do you ensure the right supplier/partner behaviours? 	<ul style="list-style-type: none"> How do you determine the level of trust you have with different sub-contractors / partners in delivering the product/service? How do you ensure the right requirements are placed on sub-contractors? How do you ensure the right sub-contractors/partner behaviours?

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
PROTECT	Identity Management and Access Control				<ul style="list-style-type: none"> How do you assign access rights? 	<ul style="list-style-type: none"> How do you assign access rights?
	Human-Centred Security				<ul style="list-style-type: none"> How do you ensure that awareness leads to the right behaviours? What indicators do you use to predict who will later be detected violating security policy? 	<ul style="list-style-type: none"> How do you ensure that awareness leads to the right behaviours? What indicators do you use to predict who will later be detected violating security policy?
	Protective Technology				<ul style="list-style-type: none"> Do you have a defined security architecture (for now or future)? How does it support security by design? How does it support data exchange and protection, and resilience? How have you addressed the human factors in ensuring security controls are effective? 	<ul style="list-style-type: none"> Do you have a defined security architecture (for now or future)? How does it support data exchange and protection, and resilience?
DETECT	Anomalies and Events				<ul style="list-style-type: none"> How do you ensure that all cybersecurity events / incidents can be detected? 	<ul style="list-style-type: none"> How do you ensure that all cybersecurity events / incidents can be detected?

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
RESPOND	Response Planning				<ul style="list-style-type: none"> How do you determine the required reaction times for services? Do you consider cyber-attacks with subtle and believable data manipulation? Do you have a Service Level Agreement (SLA), or similar requirements, between Ops and supporting departments (inc IT)? How you ensure that enough resourcing is in place to respond to events/incidents? 	<ul style="list-style-type: none"> How do you determine the required reaction times for services? Do you consider cyber-attacks with subtle and believable data manipulation? Do you have a Service Level Agreement (SLA), or similar requirements, between the departments that deliver the product/service? How you ensure that enough resourcing is in place to respond to events/incidents?
	Mitigation				<ul style="list-style-type: none"> How do you respond to security events? Who do you communicate with during an incident (internally and externally)? How often are the lines of communication tested? Are contacts named or are they roles and numbers that automatically change as people move roles in an organisation? Are the means of contact (phones, email, etc) themselves resilient to an attack? What forensics capabilities do you have (internally and from third parties)? 	<ul style="list-style-type: none"> How do you respond to security events? Who do you communicate with during an incident (internally and externally)? How often are the lines of communication tested? Are contacts named or are they roles and numbers that automatically change as people move roles in an organisation? Are the means of contact (phones, email, etc) themselves resilient to an attack? What forensics capabilities do you have (internally and from third parties)?

Appendix A – Scoring Form

	Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
RECOVER	Recovery Planning				<ul style="list-style-type: none"> • Do your operational contingency procedures include cybersecurity incidents? • How do you return to normal operations? • In returning to normal operation, how do you demonstrate that there are no residual/persistent cybersecurity vulnerabilities? 	<ul style="list-style-type: none"> • For services, do your contingency procedures include cybersecurity incidents? • For services, how do you return to normal operations? • In returning to normal operation, how do you demonstrate that there are no residual/persistent cybersecurity vulnerabilities?

Appendix B – Glossary

This SoE draws heavily on the NIST Cybersecurity Framework (CSF) and ISO 27001 standard. These documents define the terms used within and should be consulted as necessary. The following glossary explains some key terms used within the SoE:

ISMS – Information Security Management System.

As per ISO 27001, an ISMS comprises the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives.

KPI (Key Performance Indicator).

A Key Performance Indicator is a measurable value that demonstrates how effectively a company is achieving key business objectives. Organisations use KPIs at multiple levels to evaluate their success at reaching targets.

SMS (Safety Management System).

A Safety Management System is a systematic approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures.

QMS (Quality Management System).

A Quality Management System is a set of policies, processes and procedures required for planning and execution in the core business area of an organisation.

SIEM (Security Incident and Event Management).

A Security Incident and Event Management system is an approach to security management that combines security information management and security event management functions into one security management system.

NDA (Non Disclosure Agreement).

A non-disclosure agreement is a legally binding contract that establishes a confidential relationship. The party or parties signing the agreement agree that sensitive information they may obtain will not be made available to other parties.

SME (Subject Matter Expert).

A subject matter expert in business is an individual with a deep understanding of a particular process, function, technology, machine, material or type of equipment.

Administrative network.

A network that supports enterprise business functions, such as office applications, finance, human resources, etc.

Operational network.

A network that supports the operational functions of an ATM service, such as communication, navigation and surveillance systems, meteorological systems, etc.

Primary asset.

The primary assets are the core processes and information required for the delivery of the ATM service.

Supporting asset.

The supporting assets are the assets upon which the function of the primary assets rely.

Appendix C – Sources

- CANSO Cyber Risk Assessment Guide
- CANSO Emergency Response Planning Guide, December 2019
- CANSO Standard of Excellence in Human Performance Management, 2019
- Center for Internet Security Benchmarks (<https://www.cisecurity.org/cis-benchmarks/>)
- ED-201, Aeronautical Information System Security (AISS) Framework Guidance. Issued in December 2015.
- EN-16495:2019 – Air Traffic Management – Information Security
- ICAO Doc. 8973 Aviation Security Manual, 10th Edition, 2017 (Restricted)
- ICAO Doc. 9985 ATM Security Manual, 1st Edition, 2013 (Restricted)
- Internet Security Forum “Standards of Good Practice” Modules TM 1&2, BC 2, SI 1&2
- ISO 27000:2018 – Information Technology – Security Techniques – Information Security Management Systems
- ISO 27001:2013 – Information Technology – Information Security Management
- ISO 27002:2013 – Information Technology – Security Techniques
- ISO 27005:2018 – Information Technology – Information Security Risk Management
- ISO 27033:2015 – Information Technology – Security Techniques – Network Security
- ISO 27035-1:2016 – Information Technology – Security Techniques – Information Security Incident Management
- Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology (NIST). April 2018
- NIST National Vulnerability Database (NVD)
- NIST Special Publication 800-30 – Information Security – Guide for Conducting Risk Assessments, Revision 1
- NIST Special Publication 800-34 – Contingency Planning Guide for Federal Information Systems, Revision 1
- NIST Special Publication 800-37 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2
- NIST Special Publication 800-39 – Information Security – Managing Information Security Risk, March 2011
- NIST Special Publication 800-53 – Security Controls, Revision 4
- NIST Special Publication 800-61 – Computer Security Incident Handling Guide, Revision 2
- NIST Special Publication 800-92 – Guide to Computer Security Log Management, September 2006



CANSO

canso.org

