RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, DC 20036, USA

Report on Information Security Management System (ISMS) for Aviation Organizations

RR-007
September 8, 2025

Prepared by: SC-216
©2025 RTCA, Inc.

Copies of this document may be obtained from:

RTCA, Inc.
1150 18th St. NW, Suite 910
Washington, D.C. 20036, USA

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for price and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) with EUROCAE Working Group 72 (WG-72) and approved by the RTCA Program Management Committee (PMC) on September 8, 2025 and the EUROCAE Secretariat on August 25, 2025.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;

- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders and several advisory circulars.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

DISCLAIMER

This publication is based on material submitted by various participants during the SC approval process. Neither the SC nor RTCA has made any determination whether these materials could be subject to valid claims of patent, copyright or other proprietary rights by third parties, and no representation or warranty, expressed or implied is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

This Page Intentionally Left Blank

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 Purpose 1
1.1.1 Part-IS 1
1.1.2 Supply Chain Security 3
1.1.3 Information Security Risk Assessment for Part-IS 3
1.2 Scope 4
1.3 How to use this Report 5
1.4 Relationship to Other Documents 5
1.5 Term & Concepts 6
1.5.1 Terminology 7
1.5.2 Core Concepts 9

2 ELEMENTS OF AN ISMS FOR AVIATION SAFETY 15

2.1 Guidance for Building an ISMS – Development 16
2.2 ISMS and ISEM Integration 18
2.3 Personnel Requirements to Support ISMS 19
2.4 Information Security Management Manual (ISMM) 20
2.5 Changes and Continuous Improvement 20

3 INTERFACES WITH OTHER MANAGEMENT SYSTEMS 23

3.1 SMS 23
3.2 Levels of Interfacing with SMS 24
3.3 ISMS for Products and Services 25
3.4 ISMS Implementation Maturity 26

4 INFORMATION SECURITY RISK MANAGEMENT 27

4.1 Introduction to ISMS Risk Management 27
4.1.1 Purpose of Risk Management in ISMS 27
4.1.2 Chapter Structure 28
4.1.3 Chapter Scope 29
4.1.4 Relationship to Other Frameworks 30
4.2 Risk Management Approach 32
4.2.1 Recommendations 32
4.2.2 Approach Overview 33
4.2.3 Principles 38
4.3 Scoping & Context 40
4.3.1 Introduction to Scoping 40
4.3.2 Scope Identification 44
4.3.3 Scope Assessment for Safety Significance 49
4.4 Risk Assessment 59
4.4.1 Risk Assessment Activities 60
4.4.2 Risk Identification 64

4.4.3 Risk Analysis 65
4.4.4 Risk Evaluation 68
4.5 Risk Treatment 68
4.5.1 Risk Treatment Activities 69
4.5.2 Risk Treatment Options 71
4.5.3 Standardised Controls 73
4.5.4 Verification and Validation of Declared Controls 74
4.5.5 Supply Chain Risk Treatment 74
4.6 Risk Acceptance 76
4.6.1 Risk Acceptance Activities 77
4.6.2 Risk Acceptability Criteria 78
4.7 Communication, Monitoring & Improvement 79
4.7.1 Risk Communication and Consultation 80
4.7.2 Risk Monitoring and Review 81
4.7.3 Risk Management Improvement 82

5 SUPPLY CHAIN SECURITY 85

5.1 Contracting of ISMS Activities 85
5.2 Supply Chain Security 85
5.3 Risk Assessment 86
5.3.1 Vulnerability Management 86
5.4 Establish Control 87
5.4.1 Addressing Non-Compliant Large Suppliers 87
5.4.2 High Risk, Low Resource 88
5.4.3 Supplier Assurance Questionnaires 88
5.5 Manage Supply Chain 88
5.5.1 Incident Response 88
5.6 Continue to Improve 89

6 CONSIDERATIONS FOR DIFFERENT AVIATION STAKEHOLDERS 91

6.1 Design & Production 91
6.1.1 Reporting Requirements 91
6.1.2 Asset Management 91
6.1.3 Risk Assessment-Driven Flow-Down Requirements 91
6.2 Airlines / Operators 91
6.3 ATM/ANS 92
6.4 Right Sizing ISMS for Organizations 93
6.4.1 Organizational Size and Complexity 94
6.4.2 Use of Other Guidance 95
6.4.3 Building the Right-Sized ISMS 96
6.4.4 Maintaining the Right-Sized ISMS 100

APPENDIX A ISMS RECOMMENDATIONS 101

APPENDIX B EXAMPLE ISMM STRUCTURE 111

APPENDIX C ACRONYMS & REFERENCES 116

MEMBERSHIP 122

TABLE OF FIGURES

Figure 1-1: Applicability of Part-IS 2
Figure 1-2 Bow-tie representation of management of aviation safety risks posed by information security threats [Source: EASA Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)] 4
Figure 1-3 IS RISK MANAGEMENT CORE CONCEPTS AND RELATIONSHIPS 10
Figure 2-1 EASA Implement/Operate Model 18
Figure 3-1 ISMS Embedded in SMS 24
Figure 3-2 ISMS Partially Overlapping with SMS 25
Figure 3-3 ISMS and SMS are Separate but Interfacing 25
Figure 4-1 ICAO DOC 10204 Manual on Aviation Information Security (MAIS): Risk Assessment Interactions 28
Figure 4-2 Part-IS RISK MANAGEMENT REQUIREMENTS 31
Figure 4-3 SAFETY-ORIENTED ISMS RISK MANAGEMENT APPROACH 36
Figure 4-4 SCOPE ITERATIVE REFINEMENT 41
Figure 4-5 RELATIONSHIP BETWEEN ELEMENTS, ASSETS AND THEIR CLASSIFICATION 42
Figure 4-6 IS ELEMENT AND RISK DOMAIN MODEL 46
Figure 4-7 EXAMPLE OF INTERFACE CHARACTERISTICS 49
Figure 4-8 SCOPE SAFETY ASSESSMENT ACTIVITIES 51
Figure 4-9 EXAMPLE ASSET CLASSIFICATION DECISION TREE 55
Figure 4-10 ANALYSIS AND CLASSIFICATION OF INTERFACES 57
Figure 4-11 EXAMPLE: FUNCTIONAL CHAIN AND INTERFACING ORGANISATIONS 59
Figure 4-12 RISK ASSESSMENT ACTIVITIES ALIGNED WITH ED-201A/DO-391 60
Figure 4-13 RISK TREATMENT OPTIONS 69
Figure 4-14 RISK ACCEPTABILITY MATRIX 79
Figure 6-1: The scope of ATM/ANS Services 93

TABLE OF TABLES

Table 1-1 ISMS RISK MANAGEMENT TERMINOLOGY 7
Table 4-1 SAFETY-ORIENTED IS RISK MANAGEMENT PHASES 34
Table 4-2 COMPARING THREAT-BASED AND ASSET-BASED APPROACHES 38
Table 4-3 SAFETY SIGNIFICANCE CATEGORIES 52
Table 4-4 PROPORTIONATE SUBSTANTIATION APPROACH 53
Table 4-5 Severity of Impact 55
Table 4-6 Adapted Safety Significance for Supporting Assets 56
Table 4-7 EXAMPLE PROPORTIONAL TREATMENT SUBSTANTIATION 62
Table 4-8 EXAMPLE CONTROLS FOR INTERFACES 76
Table 6-1 complexity classification criteria 95

This Page Intentionally Left Blank

1 INTRODUCTION

1.1 Purpose

The purpose of this report is to provide guidance in addressing a management system for Information Security which complements the current Safety Management System. Globally, this is also in response to the desire for consistent information security solutions across the supply chain. This report identifies selected best practices for securing the aviation ecosystem, ensure consistency and minimum information security throughout the supply chain, and establish common understanding for easing audit overhead on all stakeholders. The best practices for securing aviation are expected to be suitable for addressing information security risks in the aviation sector and to be considered by European Union Aviation Safety Agency's (EASA) as a means of compliance for Part-IS.

Aviation organizations may want to apply the best practices in this report to other regulations and business processes that are relevant to the aviation sector. While business risk management is not included in the scope, these organizations are welcome to extend these processes.

1.1.1 Part-IS

The European Union (EU) introduced Part-IS through several regulatory vehicles (EU 2022/1645, EU 2023/203, EU 2023/1769, and EU 2024/1109). Part-IS applies to aviation organizations approved either by EASA or EASA Member State Civil Aviation Authorities only. In other jurisdictions, including the United States, regulatory authorities have not issued requirements for an ISMS. References to Part-IS in this document only apply to Part-IS within the European regulatory framework. The regulations define the requirement for an Information Security Management System (ISMS) for aviation safety both for the aviation industry and for the authorities assigned for the oversight authorities of Part-IS in the industry.

Part-IS is applied to competent authorities and approved organisations via either an Implementing Rule or a Delegated Rule. The vehicle is dependent on the type of organisation, but the rule itself is equal to all organisations. See Figure 1-1 for which rule applies to each organisation.

 ©2025, RTCA, Inc.

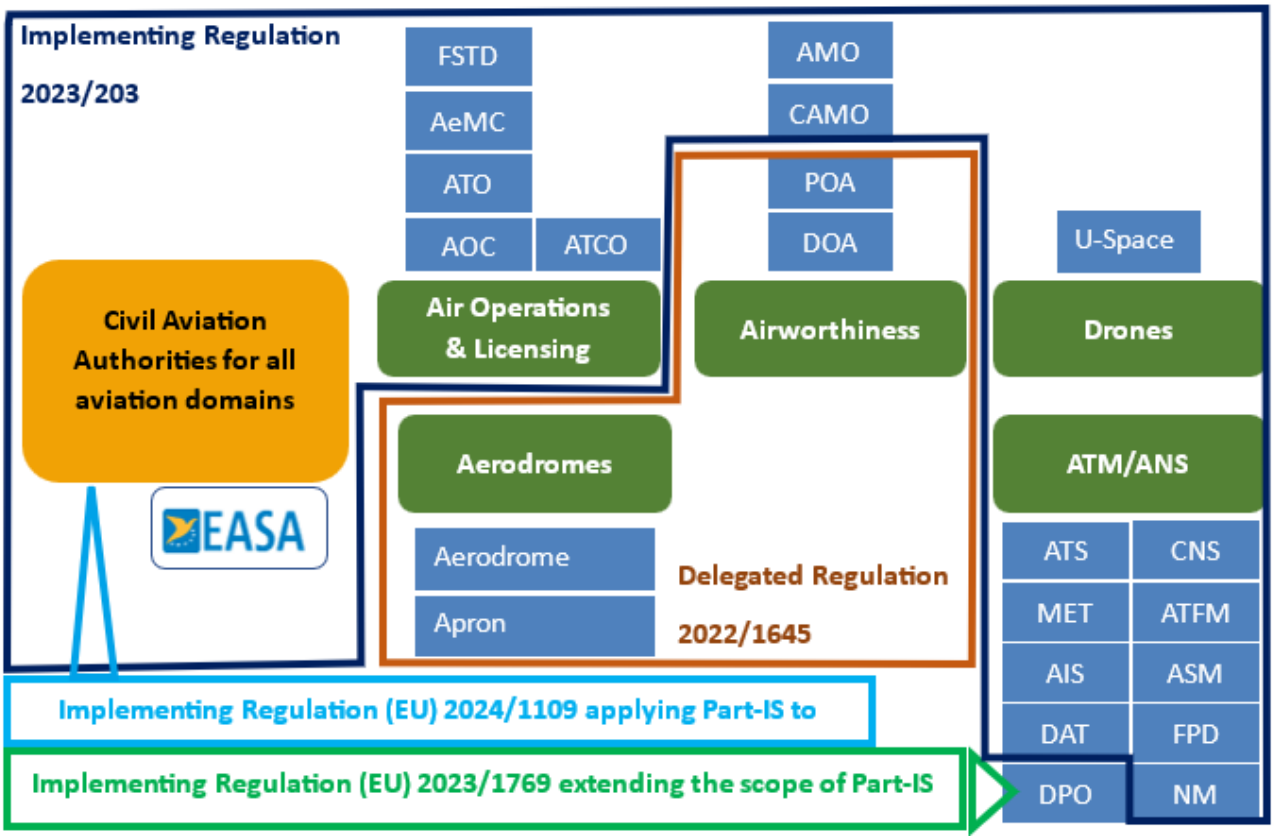


FIGURE 1-1: APPLICABILITY OF PART-IS

According to the European rulemaking process for aviation, regulations need to be accompanied by material to assist the implementation of the regulations and ensure consistent and fair finding of compliance. This material is categorised into groups:

Acceptable Means of Compliance (AMC) are non-binding. The AMC serves as a means by which the requirements contained in the regulations can be met. However, applicants may decide to show compliance with the requirements using other means. Both Civil Aviation Authorities (CAAs) and organisations may propose alternative means of compliance. 'Alternative Means of Compliance' are those that propose an alternative to an existing AMC. Those Alternative Means of Compliance proposals need to be accompanied by evidence of their ability to meet the intent of the Implementing Rule (IR). Use of an existing AMC gives the user the benefit of compliance with the IR.

Guidance Material (GM) is non-binding explanatory and interpretation material on how to achieve the requirements contained in the Regulations, and the AMCs. It contains information, including examples, to assist the user in the interpretation and application of the Regulations and the AMCs.

EASA and the European Commission have introduced sector specific information security requirements ensuring that aviation safety is not impacted by information security.

This report is intended to be developed into a full standard that will be proposed as providing an Acceptable Means of Compliance and Guidance Material. Until such material is fully developed and accepted, the AMC and GM published by EASA may be used in combination with this report.

The terms information security and cyber security are sometimes used interchangeably but cyber security may also be limited to embedded systems. Information security is the term for the discipline and is more encompassing for all domains securing electronic systems – including enterprise information technology, operational technology and embedded systems. Information security is the established term for aviation as used by EASA AMC 20-42 and Opinion 03/2021. For this reason, only the term information security will be used except where cybersecurity is part of a document title.

1.1.2 Supply Chain Security

Civil aviation has both an enormously complex and globally connected supply chain. As such, civil aviation's supply chain continuously poses a great risk to the security of the aviation industry as it allows multiple points for malicious actors, including both externally motivated and insider threats, to subvert the activities of an organization for its products and services.

For Part-IS, it is important to consider that civil aviation industry attacks can impact nearly everything in the supply chain. This includes the electronic components – the software and firmware of Complex Electronic Hardware (CEH) running in products or powering servers providing services in addition to the electronic hardware itself. This also includes the data used to build physical structures as well as the data and production systems used to manufacture non-electronic components such as structural items.

For purposes of this report, the supply chain ecosystem encompasses acquisition or delivery of data and information, including software and Information Technology (IT) related services, and non-physical goods and services such as software, firmware, data and cloud applications from external companies to an organization.

The provider of ISMS activities needs to demonstrate that their services ensure the organisation complies with Part-IS or any other applicable regulation and agree to audits by the Competent Authority. Contracting Part-IS activities (as detailed in IS.OR.235, Contracting of information security management activities) involves outsourcing specific information security tasks, such as risk assessments, incident response planning, or the management of secure systems, to third-party providers. The focus is on ensuring these providers align with organisational ISMS (Information Security Management Systems) and regulatory frameworks like Part-IS. Such contracts specify the provider's roles, deliverables, and performance criteria, emphasizing compliance with aviation safety standards.

In contrast, supply chain information security addresses the broader risks posed by all suppliers, emphasizing securing dependencies in systems, processes, and data interactions. It focuses on ensuring that suppliers' practices do not introduce vulnerabilities, requiring assessments, audits, and continuous monitoring. Unlike contracted information security activities, which can be scoped and specialized, supply chain information security involves the systemic application of controls across diverse supplier relationships, reflecting its interconnected nature.

Organisations need to independently assess their supply chains' information security implications, align supplier practices with Part-IS requirements, and address risks proportional to their impact on aviation safety.

1.1.3 Information Security Risk Assessment for Part-IS

An information security risk assessment identifies and assesses the risks for information assets from information security threats. Scenarios typically consist of an information

 ©2025, RTCA, Inc.

security threat, an information asset, a threat vector exposing the information asset to the threat, and a threat condition triggered on the information asset. Threat conditions are commonly expressed as the loss of a security attribute (confidentiality, integrity, availability) which is associated with an impact for the assessing organization.

Part-IS risk assessments study impacts on aviation safety and bring two important extensions to this basic concept:

(1) The link between the information security threat condition and the safety consequence can be conveyed through a functional chain.

(2) The functional chain can span across several organizations.

In consequence, the safety impact can occur delayed and/or within a different organization than the organization responsible for the compromised information asset. There can also be risk mitigating measures on the functional chain that reduce the risk for a safety effect but activate after the information asset compromise. For example, an unstable part produced from compromised production data can be rejected in a quality test down the production chain.

This interdependency between information security and aviation safety is expressed with a bow-tie diagram, Figure 1-2.

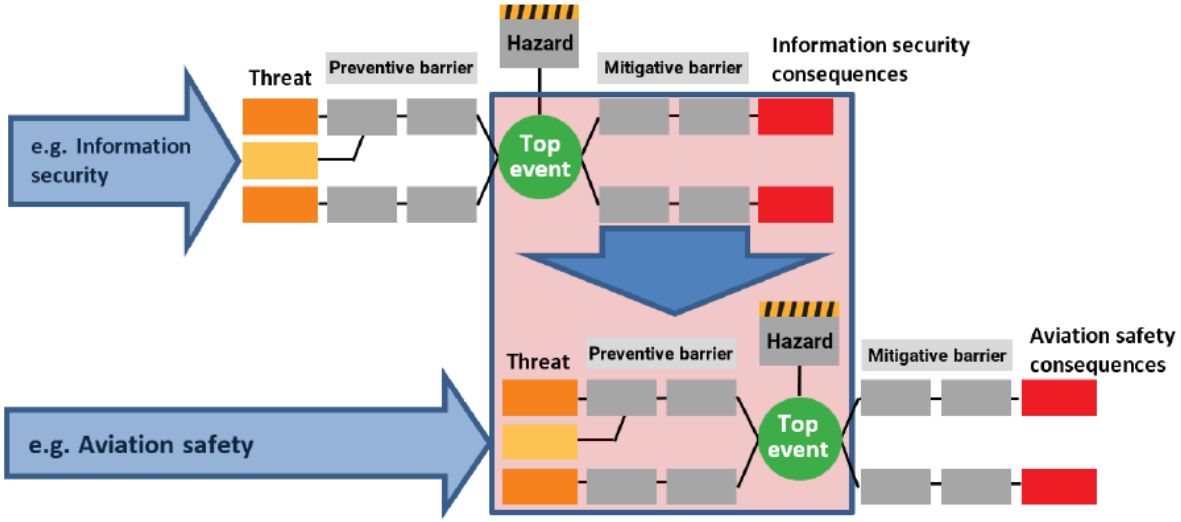


FIGURE 1-2 BOW-TIE REPRESENTATION OF MANAGEMENT OF AVIATION SAFETY RISKS POSED BY INFORMATION SECURITY THREATS [SOURCE: EASA EASY ACCESS RULES FOR INFORMATION SECURITY (REGULATIONS (EU) 2023/203 AND 2022/1645)]

1.2 Scope

Aviation Organizations: There is already guidance for ISMS under International Organization for Standardization (ISO) 27001. However, that guidance is focused on ground-based IT systems and business risk. It does not provide the coverage needed for aviation organizations and safety risk. Therefore, this report is established for aviation organizations so that they can show compliance with Part-IS and provide consistent security solutions throughout the aviation ecosystem.

Information Security with Safety Impact: The scope of this report is to uncover areas where information security risk can impact safety. ISMS can interface with the existing SMS with safety as the priority.

Aviation Stakeholders: There is a diverse set of aviation organizations under Part-IS and the aviation ecosystem in general. Chapter 6 will cover considerations for different aviation stakeholders. These stakeholders include design, manufacturing, maintenance, airlines/operators, airports, training organizations, and Air Traffic Management / Air Navigation Systems (ATM/ANS).

The scope will be different based on the individual company. Since this impacts all aviation stakeholders, there may be overlap in coverage, e.g. operators and Original Equipment Manufacturers (OEMs). There are shared and/or shifted responsibilities between organisations such as OEM and Operators. See Part-IS OR.205(b) and Chapter 6 of this document. The operator does not have control over certified aspects or risk assessment done under certification. However, the operator may perform risk assessment as part of other regulations like those from the Transportation Security Administration (TSA) or compliance to Part-IS. There are also different considerations for large versus small organizations. Each organization can document these caveats and how they address the objectives.

Legacy and e-Enabled: Both legacy aircraft and e-enabled aircraft (airplanes equipped with advanced technologies that allow for real-time communication and data transfer between the aircraft and ground stations), present their own unique security architecture. The scope covered in this report should include systems that support them both, e.g. ground systems. There is security risk with legacy aircraft, though it will be different from that of e-enabled. There should be secure software distribution, weight and balance calculations, etc. regardless of aircraft type. OEMs and avionics manufacturers want to protect their design data.

Certification: This document does not address the aspects of information security within aircraft certification, avionics system certification, or airworthiness approvals. That is already covered via the RTCA/EUROCAE airworthiness security standards: DO-326B/ED-202B Airworthiness Security Process Specification, DO-356A/ED-203A Airworthiness Security Methods and Considerations, and DO-355A/ED-204A Information Security Guidance for Continuing Airworthiness.

Operational Disruptions: Operational disruptions impacting an organization need to be considered for safety impact. The potential impacts of disruptions of ATM organizations are one example and are therefore in scope.

1.3 How to use this Report

To best use this report, especially if the organization is subject to Part-IS, the organization should first become familiar with Part-IS AMC & GM. This report is not intended to duplicate Part-IS AMC & GM. This report is intended to provide best practices for the organization to utilize regardless of regulations. In addition, this report is not intended to duplicate SMS and safety best practices; rather, this report is intended to supplement and leverage SMS where appropriate.

1.4 Relationship to Other Documents

This report ISMS should not drive a revision to another RTCA/EUROCAE standard. Having said that, there are topics that intersect DO-392/ED-206 Information Security Event Management Guidance and Report on Aviation Data Security.

In addition to these two reports developed by RTCA SC-216 and EUROCAE WG-72, the following documents may be referenced:

 ©2025, RTCA, Inc.

- SM-0001 Issue B The International Standard for Implementing a Safety Management System (SMS) for Design, Manufacturing and Maintenance Providers
- ISO 27000: 2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO 27001: 2022: Information Security Management (ISMS)
- ICAO Doc 10204 Manual on Aviation Information Security
- IEC62443: Industrial communication networks – Network and system security (Operational Technology (OT))
- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- NIST CSF / NIST IR 8183: Cybersecurity Framework Manufacturing Profile (IT and OT)
- CIS Top 18 / ETSI 103 305: CYBER; Critical Security Controls for Effective Cyber Defence (IT)
- NIST SP 800-82: Guide to Operational Technology (OT) Security
- ISO 27036: Cybersecurity — Supplier relationships (Supply Chain)
- NIST IR 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (Supply Chain)
- NIST SP 800-30 Guide for Conducting Risk Assessments
- NIST SP 800-37 RMF for Information Systems and Organizations
- NIST SP 800-39 Managing Information Security Risk
- NIST SP 800-171A Assessing Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-172A Assessing Enhanced Security Requirements for Controlled Unclassified Information
- CANSO Safety Data Governance
- CANSO Standard of excellence in cybersecurity
- CANSO Safety Cybersecurity Risk Assessment Guide
- CANSO Cyber Security and Risk Assessment Guide
- ENISA Transport Threat Landscape
- ENISA Threat Landscape and Good Practice Guide for Internet Infrastructure
- ENISA Strategies for incident response and cyber crisis cooperation
- ANSSI EBIOS Risk Manager – The Method

1.5 Term & Concepts

The largest chapter of this ISMS report is 4 INFORMATION SECURITY RISK MANAGEMENT. For ease of reading, terms and concepts related to information security risk assessment are introduced here, much earlier, to ensure the reader has this in mind when reviewing the considerations of how to build an ISMS and how this ISMS may (or may not) interact with other management systems. It is important to understand how the information security risk assessment piece weaves into other aspects of ISMS in the context of aviation organizations.

1.5.1 Terminology

A precise and well-defined terminology is essential for an effective and consistent risk management approach within aviation ISMS. Table 1-1 establishes key definitions that underpin the classification and assessment of risk, ensuring alignment between security and safety considerations. The terminology introduced here supports the iterative risk management processes by clarifying how different components contribute to safety outcomes, enabling a systematic evaluation of risk propagation and mitigation strategies.

Please refer to ER-013A Aeronautical Information System Security Glossary for terms and definitions understood by RTCA SC-216 / EUROCAE WG-72 and used in their standards and reports.

TABLE 1-1 ISMS RISK MANAGEMENT TERMINOLOGY

Term	Definition
Asset	The logical and physical resources of the aircraft which contribute to the airworthiness of the aircraft, including functions, systems, items, data, interfaces, processes and information.
Asset Safety Significance	The classification (High, Moderate, Low) of the safety significance of elements, where direct pathways that result in safety significant conditions are risk assessed and addressed with the highest assurance rigor, while indirect or multi-step pathways that result in lower or no safety consequence are treated with standardised security policies.
Attack Path	The path, interface, and actions by which an attacker executes an attack.
Business Asset	An important component for accomplishing the mission of the approved organization. This can be a service, support function, a step in a process and any associated information. A business asset needs to be protected.
Contingent Propagation	The security threat condition that can increase the risk of a safety effect (e.g. disclosure of cockpit access code).
Direct Propagation	The security threat condition that can lead to a safety effect (e.g. malicious Field Loadable Software (FLS)).
Element	A functional chain, process, service or facility within an ISMS that contributes to operational capabilities and may have a direct or indirect impact on safety. Note: Elements are often referred to as primary assets or business assets in more general security ISMS frameworks. For aviation-specific ISMS elements are assessed based on their safety significance and their potential for propagating risk.

©2025, RTCA, Inc.

Term	Definition
Indirect Propagation	The security threat condition that can contribute to a safety effect (e.g. failure to detect a safety issue).
Maximum safety consequence	The most severe safety outcome the element can lead to, including hazardous or catastrophic conditions.
Propagation Path	The mechanism by which an element's failure or compromise leads to a safety significant condition, considering both direct and indirect pathways. This includes the number of intermediary steps, dependencies, or failures required for the unsafe condition to materialise. Note: The propagation path is influenced by system interactions, dependencies, operational states and external conditions. Propagation can occur even without an active attacker. Weak security controls may inadvertently allow cascading effects.
Propagation to Safety Consequence	The mechanism by which an element's failure or compromise leads to a safety significant condition, considering both direct and indirect pathways.
Path Complexity	The number of intermediary steps, barriers, or mitigations that influence whether a failure propagates to a hazardous or catastrophic outcome.
Refutation Testing	A set of assurance activities beyond analysis and requirements. As an alternative to exhaustive testing, refutation can be used to provide evidence that an unwanted behaviour has been precluded to an acceptable level of confidence. Refutation testing encompasses activities such as security penetration testing, fuzzing, static and dynamic code analysis, and formal proofs. Additional information about refutation can be found in ED-203A/DO-356A.
Safety Significance	The impact potential of an element or interface on aviation safety, measured in a classification schema, defined by • Maximum safety consequence • Propagation path
Safety Significant Condition	A state in which an aircraft, system, or operational environment leads to a Hazardous or Catastrophic safety consequences. Note: In the Part-IS AMC/GM, this is what is meant by “unsafe condition”.
Supporting Asset	An information asset, system, hardware, software, communication or operational resource that enables or supports an element’s function but does not, by itself, have a direct aviation safety impact. Supporting assets contribute to integrity, availability and authenticity of safety-relevant elements.

Term	Definition
Threat Condition	A condition having a effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more acts of intentional unauthorised electronic interaction, involving cyber threats, considering flight phase and relevant adverse operational or environmental conditions. [from ED-203A/DO-356A]

1.5.2 Core Concepts

Figure 1-3 represents how threat conditions, propagation paths and security controls interact with safety-significant elements and ultimately affect safety related functions. It illustrates the layered relationship between security and safety risk management within an ISMS framework, showing how threat conditions can either contribute to or mitigate safety risks. Figure 1-3 and the explanations in this section clarify how vulnerabilities, risk propagation and mitigation interact within an ISMS framework. Security is not a separate function but a critical component of risk management that continuously supports safety outcomes.

Note: Safety hazards that could be introduced by cyber threats could also be mitigated via architecture design changes when applicable and not just security controls.

©2025, RTCA, Inc.

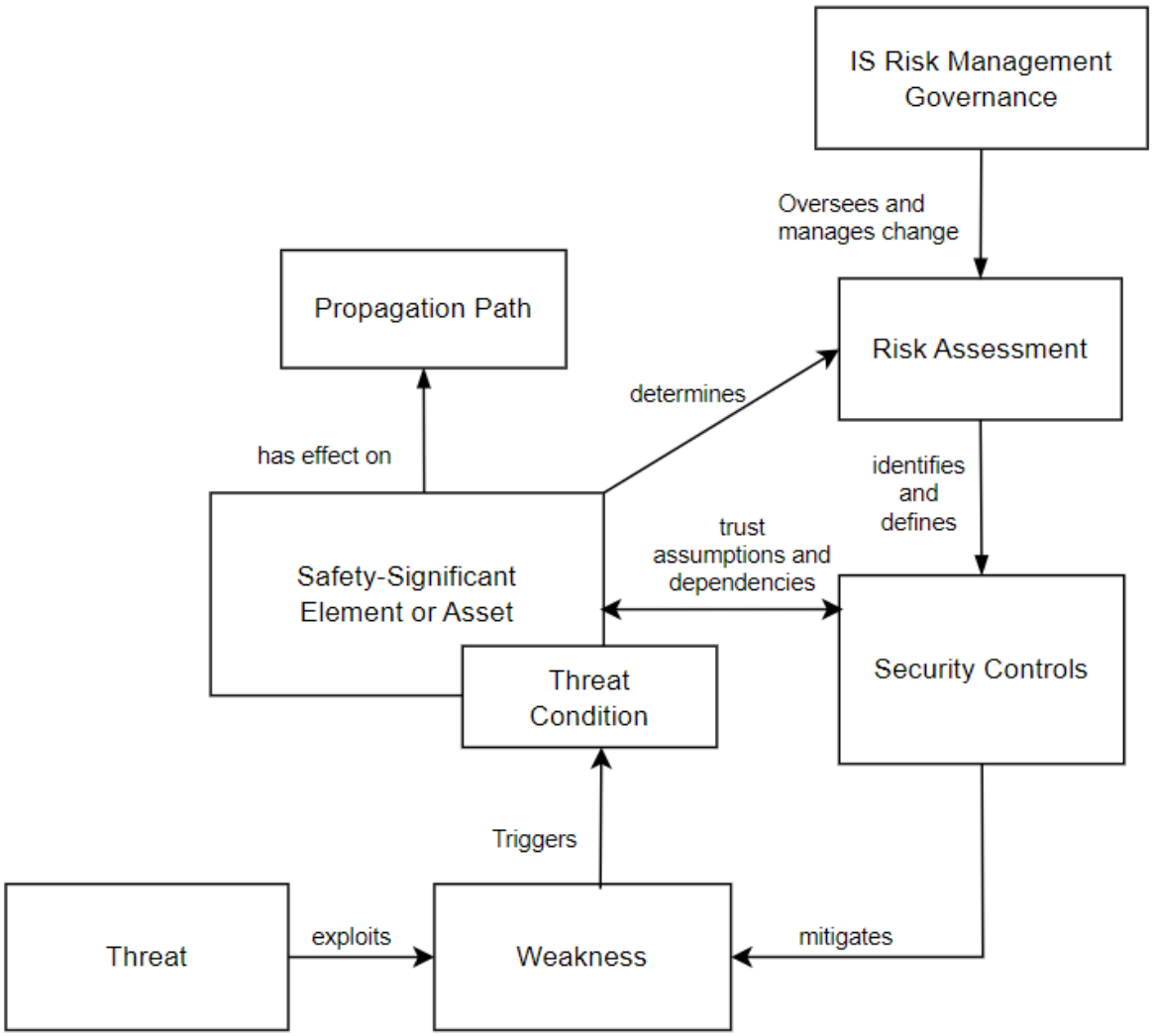


FIGURE 1-3 IS RISK MANAGEMENT CORE CONCEPTS AND RELATIONSHIPS

1.5.2.1 Core Entities in Safety-Oriented IS Risk Management

Safety-Significant Element or Asset

An information system, data, or function with a potential impact for aviation safety. If compromised, unavailable, or disclosed, it may reduce safety margins or cause safety significant conditions or expose safety related functions to security threats. This determines need for Risk Assessment.

Weakness

A deficiency in a safety-significant element or asset that could be exploited by threats or degrade system performance. These can be technical, procedural or systemic. Security controls mitigate weaknesses and prevent exploitation. The types of deficiencies security controls need to address include:

- Technical – software, hardware or network flaws, e.g. unpatched software or exposed interfaces.

- Procedural – gaps in policies or workflows, e.g. weak password policies.
- Interface – risks from third-party services or supply chains, e.g. reliance on an external IT provider.
- Cascading – failures that trigger secondary issues
- Environmental and Configuration – factors increasing failure risk, e.g. software vulnerabilities introduced during an update.

The Weakness → Threat Condition → Propagation Path relationship highlights how deficiencies interact with dependencies and influence risk propagation.

Propagation Path

The route through which security effects cascade to safety consequences. Influenced by system interactions, dependencies, operational states and external conditions. Propagation can occur even without an active attacker – weak security controls may inadvertently allow cascading effects.

Security Controls

Risk Assessment identifies and defines Security Controls. Measures that protect safety-significant elements by addressing security weaknesses. These include technical solutions like encryption or firewalls and procedural measures like audits or governance. Effective controls prevent security failures from cascading into safety risks.

IS Risk Management Governance

Oversees and manages change, utilizing the Risk Assessment. Oversees controls to ensure they support safety objectives and remain effective. Governance structures monitor, assess, and adapt controls in response to evolving risks and system dependencies.

1.5.2.2 Key Relationships and Dependencies

Mitigation Role of Controls

Security controls reduce the likelihood of security risks propagating to safety consequences, but their effectiveness depends on continuous validation, maintenance and monitoring. These controls span security, safety, quality and organisational risk management, ensuring a multi-layered defence against cascading failures.

Enrichment and Cascading Effects

Security risks are not static – feedback loops can amplify propagation. If threat conditions deteriorate due to weak maintenance, delayed updates or growing exposure, risks spread faster. Example: An attack on a flight planning system could introduce incorrect data leading to a Major safety consequence. While an isolated event may have minimal impact, repeated disruptions or unchecked vulnerabilities could accumulate into a significant safety risk or a safety significant condition.

Delay vs. Mitigation

Security controls may delay risk propagation, but delaying does not equal mitigation. Effective controls should neutralise or form barriers to threats rather than merely slow them.

Uncertainty of Safety Consequences

 ©2025, RTCA, Inc.

Not all incidents lead to deterministic outcomes. Risk assessments should consider probabilistic factors that can influence propagation or cause unplanned side effects. The Safety Significance accounts for these uncertainties in the Propagation Path.

Failures of Security Controls

Security failures can expose safety-significant assets and create conditions where security incidents become more likely. Vulnerabilities from weak security controls, misconfigurations or system failures can increase the risk of safety consequences. Example: A failure in identity management exposing critical systems to unauthorised access could be exploited by an attacker to manipulate safety relevant data.

Defence-in-Depth

Aviation safety requires defence-in-depth, ensuring no single failure leads to a safety significant condition. Layered protection models, such as the Bowtie model and Reason's Swiss Cheese model, strengthen resilience by:

- Implementing multiple diverse, independent and isolated layers of security
- Increasing confidence in security measures
- Reducing weaknesses and extending risk propagation time, allowing intervention

1.5.2.3 Safety-Oriented Information Security Risk Management

Safety-oriented IS risk management integrates safety and security by evaluating interconnected risks. This can be challenging due to layered risks, inherent complexity, and the need to understand propagation.

Note: For aircraft and aircraft systems security evaluations, the uncertainty and complexity of the propogation is significantly reduced by including the intermediate Threat Condition in ED-203A/DO-356A, which bridges safety and security. However, in an ISMS context bridging safety and security is more challenging.

To effectively show their implementation of IS risk management, Organisation risk management methods should account for the following relationships:

Safety Significance

The safety significance of an element is determined by its potential safety consequence and the probability of propagation.

Safety Significance = Safety Consequence x Probability of Propagation

$$SS = SCQ \times PP$$

Security Risk

Security Risk is determined by evaluating the security consequence of a potential compromise and the likelihood of a successful attack.

Security Risk = Security Consequence x Likelihood of Occurrence

$$SR = SCQ \times LO$$

Likelihood of Threat

Likelihood of Threat represents the likelihood of an end-to-end threat scenario propagation from a security event to a safety consequence. The probability of propagation – from the initial threat condition to the final safety outcome – is shaped by the attack path and the effectiveness of controls that mitigate cascading effects.

Security Risk influences Likelihood of Threat

$$SR \rightarrow LoT$$

Overall Safety-Oriented IS Risk

The overall safety-oriented information security risk integrates these two perspectives, combining the safety significance with likelihood.

Overall Safety-Oriented IS Risk = Safety Significance x Likelihood of Threat

$$SOIS\ Risk = SS \times LoT$$

Note 1: This overall safety-oriented IS risk evaluation does not account for compounding effects. Additional common cause analysis is recommended where security consequences (SCQ) may compound or cascade, amplifying safety consequences. For example: a Minor or Major safety consequence intentionally triggered across a fleet of aircraft could increase the safety significance of the involved elements or assets.

Note 2: The overall risk calculation considers both Safety Significance (SS) and Likelihood of Threat (LoT). SS already accounts for the Probability of Propagation (PP), while LoT represents the probability of a security event cascading to a safety consequence. This might seem like double-counting likelihood, but there is an important distinction:

- Likelihood of Occurrence (LO) applies specifically to security risk. It measures how likely a security event is to occur, based on factors such as threat intelligence, attack feasibility, exposure and vulnerability exploitation.
- Security Risk (SR) combines LO with Security Consequence (SCQ). When SR is high, it increases the likelihood that a security event could set off a chain reaction leading to safety consequences.
- Likelihood of Threat (LoT) extends beyond LO, incorporating both SR and the effectiveness of existing barrier controls. LoT reflects how likely a security risk is to cascade to a safety risk, shaped by factors such as attack paths, system resilience and mitigation measures.

©2025, RTCA, Inc.

This Page Intentionally Left Blank

2 ELEMENTS OF AN ISMS FOR AVIATION SAFETY

Establishing a well-defined ISMS risk scope, supporting asset classification and documentation ensures a comprehensive foundation enabling effective risk management. The recommendations for building an Information Security Management System as it applies to aviation safety are as follows:

Note: Some recommendations in this report are taken from DO-391/ED-201A, and their original numbers are retained. Other recommendations were developed in conjunction with this report, and their recommendation numbers correspond to the applicable sections of Part-IS AMC & GM, in particular Part-IS.I.OR and Part-IS.D.OR.

REC.001 The organization defines and operates a management system for Information Security in support of safety in an aviation framework.

REC.002 The scope of the ISMS is defined, covering necessary components of the organization, its facilities, processes, products, and services to ensure all relevant elements are included.

REC.003 Safety-relevant supporting assets are identified and assessed for their potential impact on aviation safety.

REC.004 Supporting assets are categorised based on their relevance to aviation safety as low, moderate, or high.

REC.005 The ISMS framework documents all identified elements, relevant supporting assets, interfaces and stakeholders (internal and external) to ensure a comprehensive risk assessment.

REC.006 The organisation maintains a documented methodology for classifying systems, risks and criticality levels consistently across its ISMS.

REC.007 Identify the scope of all assets and resources to be protected. [Ref. DO-391/ED-201A O1-1]

REC.008 Identify all applicable policies, processes and procedures the organization implements to provide management and oversight of the aviation assets through its security management system. [Ref. DO-391/ED-201A O1-2]

REC.009 Identify the processes used to ensure all policies, processes and procedures are evolved over their life-cycles to ensure they remain current and effective. [Ref. DO-391/ED-201A O1-3]

REC.010 The organization establishes an information security policy.

REC.011 The information security policy is endorsed by leadership. The information security policy is reviewed at planned intervals or if significant changes occur.

REC.012 In the information security policy, the organization provides guidance on the gathering and retention of metrics for the purpose of continuous improvement.

REC.013 The organization implements an internal audit process to periodically monitor compliance of the ISMS to applicable requirements.

REC.014 Availability, confidentiality, integrity, and authenticity of the information required by the ISMS is protected.

 ©2025, RTCA, Inc.

REC.015 The organization documentation includes:

a. external facing information security personnel roles and responsibilities
b. interfaces and coordination between the organization and other organizations that have safety impact, including contracted organizations
c. internal and external reporting schemes
d. types of information exchanged between organizations
e. risk sharing agreements

2.1 Guidance for Building an ISMS – Development

An Information Security Management System (ISMS) is a structured approach to managing an organization's information security, encompassing policies, procedures, and technologies to protect sensitive data. It aims to minimize risk and ensure business continuity by proactively limiting the impact of security breaches. An ISMS typically addresses employee processes as well as data and technology. In the context of an aviation organization, the ISMS should address aviation safety. Below are several considerations and initial steps for developing an ISMS.

Below are several considerations and initial steps for developing an ISMS. Each organization, however, should determine what is appropriate for them.

- Frame the risk
  - Identify applicable regulations (e.g. Part-IS, GDPR, NIS Directive, AVSEC Regulation, ISO 27001, ISO 27005, etc) and contractual obligations (e.g.: NDA, SLA, etc). See NIST SP 800-30 and NIST SP 800-39 for more information. See section 1.1 for more information on applicable regulations
- Context of the organisation
  - Identify organisationnel environnements (design, production, maintenance, etc.)
  - Identify all the stakeholder functions for the organization (Information Technology, Product Safety, Product Cybersecurity, Engineering, Quality, Operations, Supply Chain, Production)
  - Identify the objectives that the ISMS needs to comply with: list out the process and artifact requirements
  - Identify internal requirements
  - Identify the pertinent stakeholder functions for each of the objectives
  - Identify existing Management Systems (IT/Enterprise ISMS, Safety Management Systems, Quality Management Systems, etc.) if implemented. Determine how much ISMS should integrate with existing management systems
- Leadership
  - Obtain leadership and commitment of senior management in support of ISMS (top down approach)
  - This should include Accountable Manager / Head of Design Organisation
- Determine the Corporate Responsible Person (CRP) and ISMS Owner
  - If one ISMS intended across different parts of organisation, instantiate agreements and delegation (Part-IS example – Design Organisation Approval (DOA), Production Organisation Approval (POA), Maintenance Organisation Approval (MOA))
  - Get approval from senior leadership to proceed

- Planning
    - Establish current state: determine existing tools, systems, processes that can be leveraged
    - Perform a gap analysis against the current organizational and functional policy and procedure; conducting an as-is ISMS audit for information gathering
    - Create a compliance plan:
        - Objectives are being satisfied with current policies and procedures,
        - Gaps that would require new/updated policies and procedure
        - Compliance artifacts that need to be created
    - Create ISMS document structure to include where compliance data is documented
- Timelines for the drafts of the documents identified in the ISMS document structure
    - Primary documents where compliance data is documented:
        - Plan for safety asset identification and risk assessment
        - Create a draft outline for ISMS policy
        - Create a draft outline for the Information Security Management Manual (ISMM)
        - Changes to the information security management system
    - Engage regulator if needed
- Support
    - Get cross functional buy in
    - Identify activities and resources (e.g. ISMS suppliers/consultants – note: possible guidance on how to engage ISMS suppliers so that they are showing compliance to Part-IS for aviation safety rather than ISO27K for business risk)
- Evaluation Planning and Improvement
    - Determine the monitoring function for the ISMS
    - Determine responsibilities for audit and independence requirements

The Implement/Operate Model based on Part-IS shown in Figure 2-1 provides a means for establishing and initial approval of an ISMS as well continuously operating the ISMS. The Implement staging covers the policy aspects of an ISMS and the Operate staging covers specific activities. For initial approval, the Implement staging can be analysed and approved to ensure appropriate foundations before assessing full operational aspects.

©2025, RTCA, Inc.

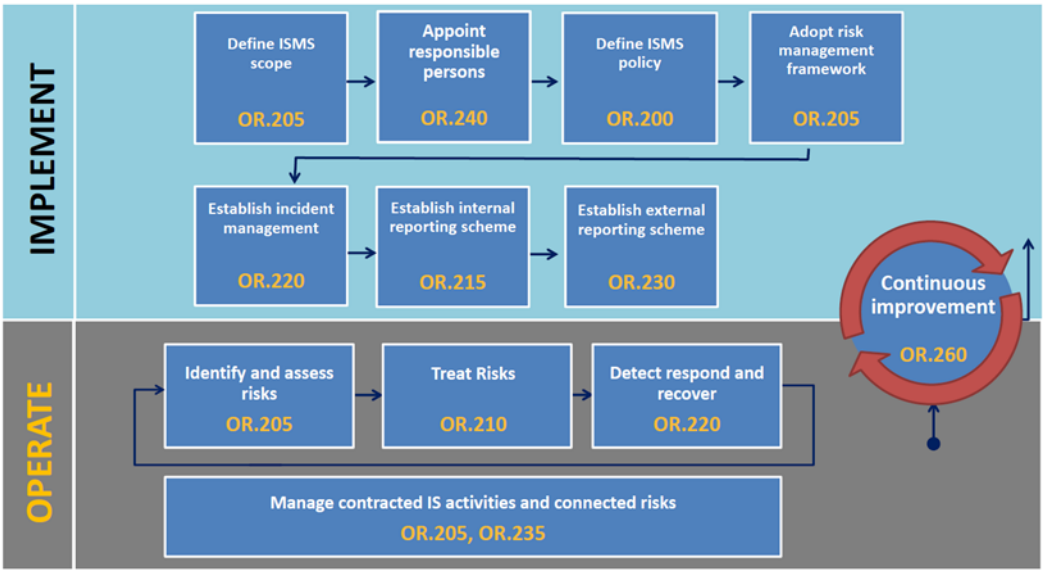


FIGURE 2-1 EASA IMPLEMENT/OPERATE MODEL

2.2 ISMS and ISEM Integration

It is recommended to include Information Security Event Management (ISEM) as part of the ISMS as follows. These recommendations cover Information Security Internal Reporting Scheme, Information Security Incidents, Vulnerability Management, and Information Security External Reporting Scheme.

- Establish a framework for incident and event management that meets the criteria described in ED-206/DO-392.
- Root cause analysis (similar to SMS) to make improvements and ensure vulnerabilities are not introduced to other assets is performed.
- To ensure consistent security throughout the supply chain, contract language on agreed to requirements for reporting of security vulnerabilities and incidents, consistent with applicable regulations is developed whenever possible.
- The means to detect information security incidents which may have a potential impact on safety are defined and implemented. See ED-206/DO-392.
- Guidance and / or criteria for the establishment of a maximum restoration time objective after an incident in relation to the safety impact is provided.
- An incident & vulnerability management process (to include detection, response and recovery) per the guidance in ED-206/DO-392 is established.
- After receipt of a notification from competent authority, a response is provided containing root cause(s), contributing factor(s), corrective action plan demonstration of correction effectiveness.
- Vulnerabilities and incidents that have a safety impact are reported to their design approval holder and/or authority per applicable regulatory requirements (21.3).

Many of the outputs of an ISMS feed into ISEM. These include asset identification and risk management. ISEM is recommended to include policies, processes, and tools as part of the ISMS. Organizations should ensure that the scope of security event monitoring is covering the scope of the ISMS, including event notifications received from external

parties. Guidance for establishing an ISEM framework is described in ED-206/DO-392. Below are some considerations specific to reporting.

The organisation can integrate reporting schemes with or utilize existing reporting schemes to reduce duplication of reporting requirements. Examples include utilizing Information Sharing & Analysis Centers (ISACs) or going through the applicable regulators or authorities, especially for situations where the organization is subject to Part-IS and the contracted organization may not be.

Establishing an incident response system that encourages reporting and analysis of safety related security incidents can enhance threat detection and response.

Organisations may be obliged to report information security incidents or vulnerabilities to different authorities or institutions depending on international or national laws and regulations.

Some examples:

- If the organisation is falling under a national regulation regarding "critical infrastructure" (in the European Union covered by Directive 2022/2555 "on measures for a high common level of cybersecurity across the Union" - NIS2-Directive), an external reporting scheme might be obligatory based on this regulation. Those reporting schemes are far beyond aviation, as they cover the whole scope of critical infrastructure in a state. For Europe, NIS2 encloses nearly the whole aviation sector in the scope of critical infrastructure.
- For the USA, NIST Special Publication 800-61 "Computer Security Incident Handling Guide" defines the rulebook for reporting to CISA (Cybersecurity and Infrastructure Security Agency).
- For the aviation sector, Part-IS (see Section 1.1.1) requires in IS.OR.230 an external reporting scheme in compliance with Regulation (EU) 376/2014 (Safety Occurrence Reporting Regulation). The reports based on this regulation are structured according to the ICAO ADREP-Taxonomy (ADREP = Accident/Incident Data Reporting). This taxonomy, which is implemented in the European Coordination Centre for Aviation Incident Reporting System (ECCAIRS) Software System, is used in many states, also outside Europe. EASA is developing an upgrade of the ECCAIRS-System (now "E2"), as well as the ADREP-Taxonomy to allow reporting of information security incidents and vulnerabilities.
- Another external reporting system is related to reports of data breaches of personal data (in Europe Regulation (EU) 2016/679). These reporting schemes are also based on national laws and regulations.

To comply with all requirements for external information security reporting, the organisation needs to assess the most convenient way to cover with as few as possible duplication of effort.

2.3 Personnel Requirements to Support ISMS

The recommendations for Personnel Requirements to support ISMS are as follows:

REC.042 Identify the functional roles in the organization that support information security with impact on aviation safety for the resources included within the scope of the competent approval and identify the type of security training required for each functional role. [Ref. DO-391/ED-201A O4-1]

 ©2025, RTCA, Inc.

REC.043 Identify a responsible contact accountable (i.e. accountable manager) to ensure that the security framework to protect aviation assets is effectively executed. [Ref. DO-391/ED-201A O4-2]

REC.044 Ensure that all relevant personnel have and maintain the necessary skills and competencies to perform their functional roles. [Ref. DO-391/ED-201A O4-3]

REC.045 The information security policy should be made readily available.

REC.046 The information security principles and applicable regulations should be made known throughout the organization.

REC.047 The vetting process and appropriate criteria to ensure that individuals can be trusted to perform their role are documented.

NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework), ENISA European Cybersecurity Skills Framework (ECSF) and EASA Application of the European Cybersecurity Skills Framework to Aviation can be used as reference to the objectives for personnel requirements to support ISMS.

2.4 Information Security Management Manual (ISMM)

The recommendations for creating an Information Security Management Manual (ISMM) are as follows:

REC.048 An Information Security Management Manual (ISMM) is documented.

REC.049 If the contents of the ISMM are in separate documents, then the ISMM references those separate documents (and those separate documents should be made readily available).

REC.050 Provide an outline of the corporate structure of the specific responsible security resources (internal and external) that will be used to manage and maintain the assets and resources included within the scope and approved by the appropriate leadership. [Ref. DO-391/ED-201A O5-1]

REC.051 Identify and define all relevant processes, procedures and reporting schemes. [Ref. DO-391/ED-201A O5-2]

REC.052 Identify all relevant sub-contractors used to implement the Information Security Management System. [Ref. DO-391/ED-201A O5-3]

REC.053 Identify and define the methods and processes that will be used to maintain compliance with the objectives over the life-cycle of the manual including how updates will be shared with the appropriate authority. [Ref. DO-391/ED-201A O5-4]

APPENDIX B of this report provides an example document structure for the ISMM to help the organization organize their processes and ensure the content is complete. The ISMM should be a good first point of contact for documenting ISMS information and contain references to other relevant processes.

2.5 Changes and Continuous Improvement

The recommendations for Changes to the Information Security Management System as well as Continuous Monitoring and Improvement are as follows:

REC.054 A change procedure to manage and notify changes to the competent authority is established.

REC.055 An agreement that changes to the ISMS can be implemented without prior approval as long as these changes are covered in a change procedure is established.

REC.056 If not covered by approved processes, it is recommended that organizations that need to apply for changes provide the following information:

a. the nature and purpose of the change,
b. the implementation plan of the change,
c. the verification plan of the change, and
d. the potential impact on aviation safety introduced by the change.

REC.057 A Continuous Improvement Process (CIP) to continuously improve the effectiveness, suitability and adequacy of the ISMS is implemented to:

a. Define and implement a structure to evaluate the effectiveness of security management activities.
b. Define and implement a structure to maintain the life-cycle change management.
c. Provide continuous monitoring of the effectiveness of security management activities and implement corrective actions for any identified deficiencies.

REC.058 The assessment associated with the CIP considers the maturity, adequacy, effectiveness, and efficiency of the ISMS.

REC.059 Improvement opportunities as a result of the CIP assessment are identified and documented.

REC.060 When a deficiency is identified, the organization reacts in a timely manner following a defined process leading to a managed status regarding the deficiency, its associated consequences and, if needed, the prevention of its future recurrence or occurrence elsewhere.

Note: See Part-IS or applicable regulations for timelines.

©2025, RTCA, Inc.