ED-206

GUIDANCE ON SECURITY EVENT MANAGEMENT

06/2022

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 72 “Aeronautical System Security” and RTCA Special Committee 216 “Aeronautical System Security” and was approved by the Council of EUROCAE on 23 June 2022.
2. This document is technically identical to RTCA DO-392 Guidance on Security Event Management which has been achieved with RTCA SC-216 “Aeronautical System Security”.
3. EUROCAE, an international non-profit organization, is the European leader in the development of worldwide recognized standards for aviation. This is achieved by utilizing the expertise from our members and stakeholders across the global aviation community.
4. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
5. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
6. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
7. Copies of this document may be obtained from:

EUROCAE
9 – 23 rue Paul Lafargue
93200 Saint-Denis
France

Telephone: +33 1 49 46 19 65
Email: eurocae@eurocae.net
Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD I

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

This document provides guidance on security event management for various stakeholders in the aviation environment such as manufacturers, operators, maintainers, product suppliers, service providers, etc., to develop processes and procedures for identifying, responding to and reporting information security events impacting aviation safety. The guidelines in this document were developed with the intent to provide Acceptable Means of Compliance to EASA's proposed Part IS which intends to establish a regulation requiring approved organizations to implement an Information Security Management System including (Security) Occurrence Reporting analogous to Safety Management System with (Safety) Occurrence Reporting. Other regulations may also apply. Organizations may elect to apply Information Security Event Management processes for operational or other business needs.

Information Security Event Management addresses security events with actual or potential safety consequences. Security events could be malicious interactions (hacking), non-targeted attacks (malware), as well as flaws (vulnerabilities) in systems, components or procedures that could be exploited to cause safety consequences for the aircraft, its passengers or crew.

1.1 PURPOSE

This document is a resource for civil aviation authorities, government agencies (when applicable), and the aviation industry that need to address information security threats that can affect aviation safety. It addresses the management of security events that affect aviation safety and it supports the existing safety event management guidance. It provides guidance for detection, assessment and disposition, sharing information, reporting and other activities that need to be performed in response to information security events.

Aircraft manufacturers, operators, aviation service providers, maintenance repair and overhaul organizations (MRO), design, manufacturing, operation and regular maintenance of ground ATM/ANS equipment, industrial equipment manufacturing or supporting the production of aircraft and supporting systems and operators of information systems used for support of these functions and all other stakeholders of civil aviation can use this document for event management guidance.

This document is also intended to be a companion to other documents produced by EUROCAE WG-72 and RTCA SC-216 relating to Aeronautical Information System Security. This document is specifically intended for managing information security events that affect aviation safety but is also without prejudice as to its use in other contexts. It is intended to be used along with the safety event management processes defined by 14 CFR 21.3 (FAA), 14 CFR 135.415, 14 CFR 145.221 and Part 21.A.3A (EASA).

Regulatory agencies can publish additional guidance as well as point to existing industry standards, which may be used in combination with this document. Since aircraft information security requirements and regulations evolve, it is recommended that applicants monitor the applicable certification authority’s guidance.

1.2 SCOPE

This document provides guidance to the aviation sector for the management of information security events with actual or potential aviation safety consequences. This includes unwanted or unexpected events that are an indication of an actual adverse effect on information security, as well as gaining knowledge about security vulnerabilities in information systems that could be exploited to cause such incidents. In addition to the aircraft itself, this document also addresses ground IT, maintenance equipment, ATC, aviation services and design and manufacturing supply chain that

could cause a safety effect on the aircraft. Physical security attacks (e.g., sabotage, counterfeit parts, attacks with physical means) are not in scope of this document.

ED-201A / DO-391 discusses the relationship of this document to other aeronautical information security system guidance documents. This document addresses the organization and preparation, detection, analysis, response and recovery steps to information security events. This document also provides the reporting guidance necessary for an information security incident or vulnerability.

This document is not intended as a replacement for the existing occurrence reporting process. It provides guidance for the information security aspects of an event that could affect aviation safety and therefore could need to be included in those reporting chains as well. However, the guidance in this document can be used in any context of civil aviation.

Existing information security guidance (presented in ED202A / DO-326A) addresses information security concerns as Intentional Unauthorized Electronic Interaction (IUEI). IUEI is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes the consequences of malware and forged data and the effects of external systems on aircraft systems but does not include physical attacks or electromagnetic disturbance (reference EUROCAE ER-013 / RTCA 7-A-120-21-PMC-2151). This definition is provided for the reader to understand information security concerns but this document could be applied to any portion of the aviation ecosystem.

The security event management guidance in this document may be used to address relevant Aviation areas including:

- Aircraft development, production
- Aircraft operation (passenger and cargo) including pilots and other crew, maintenance repair and overhaul operations (MRO), continuing airworthiness management organizations (CAMO)
- Air traffic management organizations
- Airports and aviation service providers
- Design, manufacturing, operation and regular maintenance of ground ATM/ANS equipment
- Industrial equipment manufacturing or supporting the production of aircraft and supporting systems
- Aircraft decommissioning

This guidance extends as appropriate to the supply chains of these organizations.

1.2.1 Future Aircraft Information Security: Rationale and Needs

There are relatively few information security related capabilities for Information Security Event Management for aircraft systems (vs. safety-derived capabilities) currently deployed that are intended to work in real-time. However, nothing in this document should be interpreted as precluding deployment and use of real-time capabilities. Future revisions of this document should be expected to treat these subjects in more detail.

Aviation systems, including those onboard aircraft, continually increase in capability and interconnections with other systems. This provides more opportunities for attack but also more opportunity for detection and mitigation. Where possible, future capabilities and systems should look toward the ability to provide 1) real-time detection of attacks, 2) real-time mitigation, and 3) pilot notification and associated procedures for attacks. Having said that, human factors engineering should be considered in future capabilities. Any information provided to the pilot must be usable and actionable. Otherwise, it simply increases the pilot's workload with no added benefit.

Fundamentally, an attack on an aircraft system is a form of attempted sabotage and depending on the nature or objective of the attack, it may also be a form of virtual hijacking. ICAO Annex 2 and Annex 17 place requirements on the pilot-in-command to respond to unlawful interference. Further requirements may be imposed by national laws and aviation authorities; for example, United States law [US Code Chapter 49, Sections 1544.215 and 1544.303] designates the pilot-in-command (PIC) as the

security coordinator while the aircraft is in flight and requires the PIC to be notified of threats to the aircraft. The US Federal Aviation Administration has additionally observed:

"The modus operandi of terrorist organizations is to make coordinated, simultaneous attacks designed to confuse and overwhelm defenses. Events perceived by aircrews, as isolated to one aircraft, may be part of a broader scheme or the precursor to an elaborate attack. Therefore, the rapid exchange of information is paramount to ensure the security and integrity of the NAS." [FAA Advisory Circular AC90-103; superseded by other FAA documents and the operator's TSA approved security program].

As an example, it is possible that an information security attack on an aircraft system may be used as a distraction for a physical attack elsewhere on the aircraft (or vice-versa). External attacks on Communications, Navigation, and Surveillance (CNS) systems (e.g., "jamming" or "spoofing") are also attacks even if they do not compromise avionics internally.

As additional rationale for these real-time capabilities, current pilot procedures and training are based on the underlying philosophy that pilots need to trust their instruments and system indications. Attacks have the potential to undermine and invalidate this trust. Historically, system failures are annunciated, or otherwise are readily apparent (for example, jammed flight controls, smoke in the cockpit or cabin, inoperative interphone, etc.). In most cases, system failures have an associated Quick Reference Handbook (QRH) procedure and checklist, intended to guide the pilot to safely handle the situation.

As of this writing, pilots receive little or no training on aircraft information security. Yet if an incident (either caused by information security or safety) occurs that degrades the state of the aircraft while in-flight, the pilot will still need to fly the aircraft for the remainder of the flight in its degraded condition or make an unscheduled landing at the nearest airfield depending on the severity of the degradation. Without detection and notification of degraded conditions, this task becomes harder as the pilot's trust can be broken in ways that are not readily apparent. With the development of in-flight detection, mitigation, and notification, pilot trust can be bolstered by helping the pilot understand which systems can be trusted, and heightened vigilance can be applied, for example, by more frequent cross-checking of the information produced by other systems and visual confirmation of aircraft state.

In addition, the QRH procedures may not have been designed to consider possible information security causes. As an example, there is no requirement to include in current flight manuals a description of how to identify and handle jamming or spoofing of Global Navigation Satellite System (GNSS) signals - these manuals implicitly treat GNSS to be "truth". Pilot manuals also vary in how much information they provide on how the Flight Management System manages and cross-checks various navigation sources.

Finally, as information security specific capabilities (for example, domain guard or data diode function) are deployed, the detection and alerting of failures in these systems should be considered. If in fact no safety effect is determined, then such failures could be communicated as maintenance actions required.

The first capability to be developed is real-time detection of an attack. Aircraft and system health monitoring capabilities could be extended to provide this function. Declaring an anomaly to be an attack is a difficult problem but may be possible in some cases (for example, jamming or spoofing on CNS systems.) This capability becomes more important as aircraft designs move toward more integration and connectivity with external entities. For example, functions that are separate systems in legacy aircraft are now running as applications on a more generalized computing architecture. Other examples are the use of commercially derived communications links that are much more complex than legacy capabilities like ARINC 429 data busses.

The second capability to be developed is real-time mitigation of attack. These capabilities are analogous to fault detection and isolation capabilities. Ideally aircraft architectures will allow fall back to a Fail-Operational state if a system becomes compromised by an attack. Beyond Fail-Operational are Fail-Safe and Fail-Secure in order of priority.

Finally, notification of pilots and development of associated pilot actions are needed to work with ICAO requirements and national laws and regulation for aircraft security. The

intent here is not to have pilots become troubleshooters of their systems or overwhelmed by nuisance alerts, but rather to ensure there is a standard and vetted response to information security related failures. It is a difficult problem to develop alerts and guidance to avoid nuisance alerts or undermine trust in the remaining uncompromised aircraft systems.

Even if an anomaly cannot be deemed an attack in real-time, the QRH procedure for systems should consider and mitigate possible information security causes. Human factors issues are significant, and regulatory and certification guidance may need to be revised as part of this.

For all of the above, existing frameworks for mitigating safety effects should be extended to include security effects. For example, 14 CFR 25.1309 and AC 25.1322-1 / AMC 25.1322 (or equivalent for other regulatory bodies) on crew alerting should be followed. The QRH model for handling failures should be used. Proper human factors engineering needs to be applied. If necessary, the aircraft Functional Hazard Assessment may need to be updated.

Finally, for attacks on CNS systems, post-event processes for communicating and handling these events should be developed.

In closing, the capabilities described above are needed as aircraft become more sophisticated and complex, and connectivity in real-time with external data becomes more prevalent. Future versions of this and other information security documents should treat these subjects in more detail.

1.2.2 Treatment of Legacy Aircraft and Systems

Newer aircraft systems will often have security assessments performed against them and detection methods in concert with their level of interconnectivity which can be used in the effective management of events. However, legacy aircraft and systems will not have these supporting assessments from which to work from, they also may not have the level of interconnectivity of newer systems. Legacy aircraft are defined as those aircraft without information security requirements as part of their applicable certification basis (TC or if modified later it will be identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC)). That said, event management is still a vital task necessary to ensure the safety of air traffic. This section addresses considerations for those aircraft and systems and the operator of such systems are encouraged to review this section as well as the overall document and determine the appropriate processes and regulatory interaction to manage events for legacy aircraft and systems.

This document discusses security events. In a general sense, for legacy aircraft and systems, these should be handled in the same manner as those for e-enabled aircraft and systems in that an event which is determined to be an incident or a vulnerability (with potential exploitation) that has a safety effect need to be reported. This is no different than if the event were discovered by some means other than in a security sense. To discover this, the operator monitors and performs an analysis of events in line with the guidance of this document but also considering that previous security assessments do not exist, and that detection and interconnectivity is not the same as e-enabled aircraft and systems. The guiding principle is that a legacy aircraft or system needs to account for and report incidents just like an e-enabled aircraft or system with the objective of performing due diligence for on a case-by-case basis.

A significant difference for legacy aircraft or systems from the e-enabled counterparts, is the lack of event detection methods specific to security related events. These include security logs, third party supplier monitoring, security functions detecting suspicious events, Design Approval Holder (DAH) analysis for events, etc. So although the reporting of safety effects is always required, the sources of these events on legacy aircraft and systems is reduced. However, this is offset by the lack of connectivity necessary to produce many of the same events. It is necessary that when such events are detected that they be analyzed sufficiently to determine if a safety effect exists. This includes voluntary monitoring by Operator and support from DAH when required, of material such as general vulnerability reports, or third-party supplier reports, as well as information from Information Sharing and Analysis Center (ISAC) bodies or other available sources.

Finally, if the event has a safety effect, it needs to be reported in line with regulatory requirements and the guidance in this document. The legacy aircraft or system will need to be returned to the Type Certification state if not already in that state. Vulnerabilities that have a safety effect and are deemed exploitable need to be reported and the appropriate process for mitigation determined with the regulator.

In summary, it is important to note that legacy aircraft and systems are not exempted from this guidance but it is recognized that these systems do not have the detection methods and assessments that e-enabled aircraft and systems possess so that this guidance considers those aspects when treating events for these aircraft and systems.

1.3 HOW TO USE THIS DOCUMENT

This document contains guidance material that can be considered by industry for use as Acceptable Means of Compliance. This is indicated by the objectives in Chapters 2-7. The objectives are the normative material in this document and the surrounding text describes how to interpret these objectives. Additional guidance material is also provided in this document to help the reader understand the issues with event management (considered informative material). The Guidance Material provides explanatory information that helps the applicant understand the background of the presented Acceptable Means of Compliance as well as support for any Alternative Method of Compliance (AMOC) an applicant may choose. This document also contains considerations for industry that are not to be interpreted as regulatory material.

This document is organized in 7 chapters plus informative appendices.

- Chapter 1 – Introduction
- Chapter 2 – Information Security Event Management Framework
- Chapter 3 – Organize and Prepare
- Chapter 4 – Detect Security Events
- Chapter 5 – Analyze
- Chapter 6 – Respond
- Chapter 7 – Recover
- Appendix A – ISEM Objectives
- Appendix B – Vulnerability Management Strategy Examples
- Appendix C – Guidance for CVSS Scoring
- Appendix D – Glossary of Terms
- Appendix E – Acronyms
- Appendix F – References
- Appendix G – WG-72 and SC-216 Membership

1.4 CONVENTIONS OF THIS DOCUMENT

Within this document, “should” is used for recommendations, “may” and “need not” are used for permission, “can” and “might not” are used for possibility, “cannot” is used for impossibility and “will” is used for an expectation arising from activities satisfying objectives from a referenced standard or regulation. The use of "must" and "shall" is avoided.

Other terms that are not defined in APPENDIX D and ER-013A / 7-A-120-21-PMC-2151 are intended to have their common dictionary meaning. This document recognizes that the guidance herein is not mandated by law but represents a consensus of the aviation community. It also recognizes that alternative methods to the ones described herein may be available to the applicant.

1.5 RELATIONSHIP TO OTHER DOCUMENTS

This document provides the guidance for the information security event management requirements stated in DO-355A / ED-204A, chapter 8 and is intended to fully meet those requirements. Any other mention of documents within this document is for information only. Thus, it is expected that the cited documents are often used in the development and airworthiness certification of aircraft. APPENDIX F presents a list of cited documents.

CHAPTER 2

INFORMATION SECURITY EVENT MANAGEMENT FRAMEWORK

2.1 Introduction

2.1.1 Terminology

This section provides further explanations for understanding essential terms in this document. Definitions for key terms are listed in Appendix D and ER-013A.

'Asset' is defined in ED-201A as 'what has value to the organization and which therefore requires protection'. In the context of this document, the value is understood as aviation safety. Assets are those systems, procedures, policies, data and information that are required to produce, deliver or maintain aviation safety. IT/OT systems can be assets if they store or process safety relevant data, provide safety relevant functions, or used in the manufacturing or maintenance of a safety relevant component (for example, CNC machine software used to produce mechanical parts for aircraft). Assets also include those elements needed by other assets to function or that protect other assets from unwanted interactions. Assets have associated threat conditions identifying the impacts in case of loss of integrity, availability or confidentiality of the asset.

'Security measure' is used to mitigate or control a threat condition. Security measures may be features, functions or procedures, both onboard and off board. Security measures can be technical, operational, or management. They are assets used to protect the confidentiality, integrity or availability of the asset.

'Information security event' is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be relevant for information security. In this document, the terms 'security incident' and 'information security incident' are used synonymously

Information security events are indicators for a breach or vulnerability and need to be analyzed to confirm whether a breach or vulnerability has actually occurred. Many events will turn out to be legitimate (e.g., a planned configuration change) or not relevant for further investigation (e.g., failed login due to human error). This first analysis of information security events is called **event screening** in this document. By screening, the **suspicious security events** are identified for further analysis.

Information security events are not always observable but can provide information about a potential security relevant situation. Thus, activities like vulnerability monitoring, threat intelligence, audits or information received from 3rd parties may be sources for security events. 'Security event' is therefore best understood as an item for further investigation, which could range from a suspicious record in a security log up to a presentation made at a security conference.

'Information security incident' is defined as a single or a series of unwanted or unexpected information security events having an actual adverse effect on information security. Unlike a vulnerability, the incident has already caused unwanted effects. The term 'security' refers to the loss or reduction of the security attributes, e.g., confidentiality, integrity, or availability of other assets. In this document, the terms 'security incident' and 'information security incident' are used synonymously

Information security Incidents on assets like security measures may not trigger a safety effect, but reduce the security performance thus increasing the risk for future security incidents.

Security incidents are by definition caused by intentional activity. Incidents from other causes (e.g., software failure, human error) affecting security measures are not considered security incidents but may impose vulnerabilities. For example: the unauthorized manipulation of a firewall rules table is a security incident (unauthorized modification) AND a vulnerability (ineffective IP filtering), whereas the involuntary misconfiguration of the rules table is a vulnerability (ineffective IP filtering), but not a security incident.

'Security vulnerability' is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited resulting in a breach or violation of the information security policy (i.e., a security incident). To cause an incident, the attacker could either directly exploit the vulnerability, or the vulnerability could be accidentally triggered, allowing the attacker to stage his attack.

2.1.2 Relationship Between Security Incidents and Security Vulnerabilities

The security architecture, procedures and policies have been set up to prevent security incidents. Thus, any security incident always exposes one or more security vulnerabilities that allowed the incident to happen. Identification of these vulnerabilities is part of the incident analysis.

A security vulnerability is not necessarily linked to a security incident. Vulnerabilities can increase the risk for certain security incidents, independent of their actual occurrence. However, when a given vulnerability is detected, it is often unknown whether it has already been exploited or not. Thus, analysis of vulnerabilities should include the identification of indicators for an exploitation, and forward and retrospective analysis should be done to identify potential undetected security incidents.

Note that, although linked, security incidents and security vulnerabilities should be treated as separate items, both with their respective analysis and treatment process. The incident response process will correct the unauthorized modifications from an incident and resume normal operations, whereas the vulnerability response process will correct vulnerabilities on all affected assets, independent of exploitation.

2.1.3 Information Security Event Management process

The Information Security Event Management (ISEM) process is detecting and handling security events, indicating a security breach or a change of security risk. It is executed mainly during the in-service phase of an asset but needs to be prepared during the asset's specification and development phase. The actual implementation of the ISEM policies, processes, tools and resources in an organization is called the ISMS.

The ISEM process does not handle the whole lifecycle of the asset. It interfaces with other processes such as asset management, configuration and change management, event management, and patch management. For some assets and events, it can also interface with various other processes like crisis management, airworthiness and safety management, supplier management, customer management etc.

The following diagram shows an example of how the ISEM process can interact with other processes.

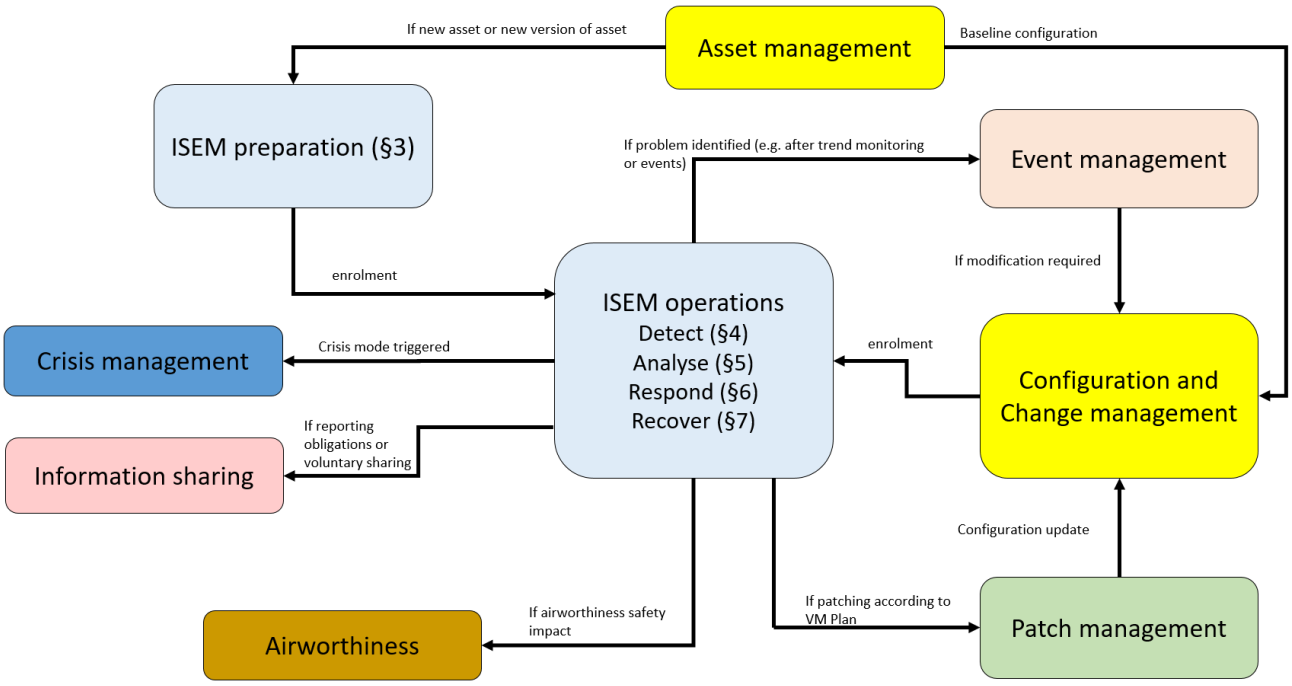

FIGURE 2-1: ISEM PROCESS INTERFACING EXAMPLE

The ISEM process can be split into several phases:

Organize and prepare phase (see CHAPTER 3)

- Establish a common set of roles and responsibilities in the stakeholder's key organizations.
- Establish policies that will guide the development of the ISEM plan.
- Utilize security risk assessments to prepare for ISEM activities.
- Identify internal and external organizations for information sharing.
- Establish a Security Incident Response Team.
- Establish a Vulnerability Monitoring Team.
- Prepare tools and support processes for ISEM.

Detect phase (see CHAPTER 4)

- Monitor data sources and collect events.
- Screen events to identify suspicious events.

Analysis phase (see CHAPTER 5)

- Analyze the event and confirm security incident or relevant vulnerability.
- Analyze the situation to determine impacts and risks.

Respond phase (see CHAPTER 6)

- Report to relevant authorities.
- Inform relevant stakeholders.
- Decide on response plan.
- Deploy measures to contain the incident and mitigate imminent risks.
- .
- Voluntary sharing and disclosure.

Recover phase (see CHAPTER 7)

- Deploy final measures for risk mitigation.
- Resume normal operations.
- Collect Lessons Learned and manage improvements.

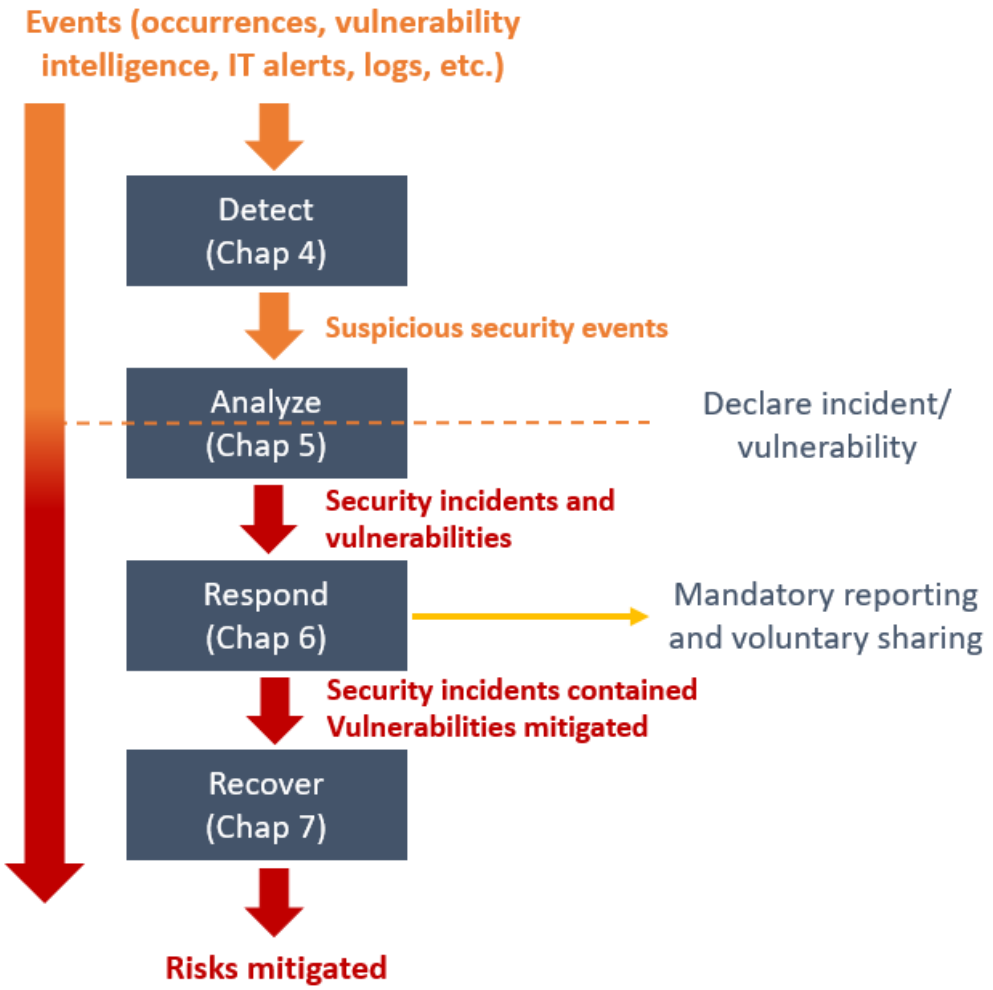

FIGURE 2-2: INFORMATION SECURITY EVENT MANAGEMENT OPERATION PROCESS

NOTE: *FIGURE 2-2 provides the global order of information security event management framework but is not a strict sequencing. Some activities in different phases could be performed simultaneously, for instance an initial response to an incident can be started before the end of the analysis.*

2.2 Aviation Stakeholders

The following aviation stakeholders may be involved in information security event management:

- **Manufacturers** of Aircraft and ground based systems, Control Centers and Systems (further referred to as “system”).
- **Operators** of Aircraft, Control Centers and Systems: Airlines, Air Navigation Service Providers (ANSPs), Airports, UAS and UTM etc.
- **Maintainers** of Aircraft, Control Centers and Systems: Maintenance and Repair Organizations (MROs), Airlines, Airports, etc.
- **Aircraft Parts and Products Suppliers** whose items are integrated into aircraft and systems, including engines, propellers, avionics, Electronic Flight Bags (EFBs), ground based automation systems used for ATM and UTM operation, etc.
- **Service Providers**: Air Navigation, Communication, Passenger & Cargo Handling, Aeronautical Information Service Providers, etc.

- **Governance Bodies:** Legislators, Regulators, Auditors, etc.
- **Standards Bodies:** Industry, Treaty organizations.
- **Military aviation stakeholders:** representing multiple roles simultaneously, particularly, Air Defense / Air Traffic Control / Air Navigation Service Provider, Governance entities, Government entities, Standardization Organizations, Maintenance Organizations, Air Operators Organizations and Product Suppliers.

2.3 Risks Sharing Aspects

Due to the interconnectivity of organizations in aviation an incident in one organization may have consequences or impose a risk on other organizations as well. It is thus necessary to identify where this can be the case and to ensure that Information Security Event Management processes include the communication of any impacts and risks potentially impacting other organizations. External agreements, as defined in ED-201A / DO-391, should be put in place to clarify roles and responsibilities across interfaces and ensure that information security events are handled appropriately across interfacing organizations. If no agreement is in place with a connected organization, potential events from such organization should be monitored in a proactive manner, utilizing available information sources and requesting a statement in case of unverified information about security events.

The analysis and response to security events can also require the support of organizations outside of the aviation sector, like manufacturers, software vendors or IT service providers. In these cases, event analysis and remediation support should be defined in mutual agreements. If this is not possible or the support is discontinued, the consequences in case of an event or vulnerability should be assessed and remediation measures put in place to be able to detect and react to security incidents and vulnerabilities in an appropriate manner.

In addition to sharing across impacted organizations, an organization may also voluntarily share information on security events, to help other organizations to prepare for and handle similar cases in an efficient way. The best practices captured from actual aviation incidents should be shared within aviation community through standards bodies and ISAC/ECCSA.

2.4 Interfacing with Safety Reporting System

All National Authorities of the ICAO member states are required to provide mandatory reporting systems to ensure collection of data on faults, malfunctions, defects or other occurrences that cause adverse effect on the continuing airworthiness of the aircraft. These may be complemented by voluntary reporting systems used to facilitate the collection and handling of occurrences and safety-related information not subject to mandatory reporting.

The ISEM interfaces with Safety Management Systems in two ways: a safety incident may have been caused by Intentional Unauthorized Electronic Interactions (IUEI). In this case the Safety Management System should be capable to understand the security aspects and risks related to the incident. On the other hand, a security incident may have been detected by the ISEM with safety consequences not yet detected or reported through the Safety Management System. In this case the ISEM Process should be aware of potential safety and continuing airworthiness impacts of the incident or vulnerability and trigger the Safety Management Process for evaluation and coordinated response. Information passed to the Safety Management Process should be sanitized and free of sensitive content. If sensitive information needs to be shared, specific precautions should be taken and handling guidance provided to prevent involuntary disclosure.

Organizations with a safety incident reporting system should define the interfaces between ISEM and the Safety Management System to ensure that safety incidents are recognized as a potential source for security events and vice versa. If a security event falls into both management systems, a coordinated approach is needed to utilize the expertise of both fields and ensure consistent reporting to relevant authorities.

2.5 Interfacing with IT Security

When setting up an ISEM process for aviation related security events, organizations could already have teams and processes in place to handle general IT events or IT Security events as part of their IT organization, including specialized teams e.g., for industrial systems (OT). These teams can contribute to or take care of certain activities in the context of aviation related security events.

Event collection

IT security organization could have event sensors already deployed across the organization's IT systems, which could assist with detecting relevant events.

Event identification

Events collected by the IT organization should be assessed for their potential relevance for aviation safety to trigger the ISEM process where appropriate.

Incident analysis

The IT security organization will be best suited to analyze an incident on the organization's corporate IT systems, as they will have the knowledge of the architecture as well as the required expertise and access to the organization's IT resources.

Response and recovery

Response activities impacting an organization's IT resources should be closely coordinated with the IT organization, which will have the means to plan, deploy and monitor the measures.

Lessons learned

Lessons learned collection should include IT and IT Security teams to detect unwanted side effects and improve the collaboration.

2.6 Documentation and Record Keeping

O2.1: Security risk assessments along with the residual risk acceptance are archived.

O2.2: Relevant security incident data and analysis results are archived.

O2.3: Relevant vulnerability data and assessment results are archived.

O2.4: Relevant security event data is retained according to the risk-based retention plan.

Information Security Event Management is part of the Information Security Management System (ISMS) and subject to record keeping obligations. More information on ISMS in aviation contexts is available in ED-201A/DO-391. In addition to documentation associated to the ISMS, an organization should archive the following information in a traceable way:

- ISEM key processes and methods,
- Security Risk Assessments along with associated security measures and residual risk acceptance,
- records of security incidents and security vulnerabilities, their assessments, ISEM key processes and methods used, decisions taken, and actions performed,
- records of suspicious security events

The term 'relevant data' in the objectives should be understood as all data that influenced the resolution of the incident or vulnerability. This includes the decisions taken at the different steps as well as the data basis for these decisions. E.g., indicators of compromise that led to detecting the incident, received information about a vulnerability, assessment results used for scoping, categorization and prioritization, decisions and actions taken with their rationale, reports shared with internal or external parties, and verification results for performed actions. 'Relevant' is understood as the minimum data needed to understand why a certain decision has been taken. Organizations may decide to keep more data, e.g., for further analysis, forensic evidence keeping or process optimization.

For record keeping and for efficient management of security events, vulnerabilities and incidents, a repository and appropriate tooling is recommended, to register suspicious events, store associated data collected during the event's analysis, trace related actions

and their status, and eventually close and archive the related incident and vulnerabilities. The repository can interface with the tools for event collection and screening, allowing for creation of a case file on suspicious events or vulnerabilities, which then can be allocated to analysis and response teams for further enrichment of the case data. Central data management will ensure all ISEM functions have a clear understanding of the situation and access to its latest related information. Every relevant step taken from the time the event was detected to the final resolution should be documented and timestamped. Use of a status is recommended to indicate the current step (e.g., detect, analyze, respond, recover).

Each analysis case entry should include pertinent information including a history of who updated it and when it was updated. All relevant evidence, information, decisions and actions regarding the event should be recorded. The event case repository should be capable of storing raw data collected during the case analysis in a way that data cannot be modified afterwards.

The case repository should be accessible to all persons and organizations involved in the analysis and resolution of the case. As it may contain confidential information not relevant to all actors, access rights should be managed per case and based on user roles, e.g. to distinguish between analysis teams and response teams. An access control model with fine granularity on case objects (e.g., status, evidence item, action item) will help to protect relevant information from disclosure and unauthorized modifications.

Various data could be collected during incident investigation, which may be subject to restrictions from authorities (law enforcement, personal data protection) as well as company policies (intellectual property, sensitive data). An organization should identify all applicable rules and regulations and define and document the rules for data management prior to collecting incident data. Taxonomies like in the ENISA Incident Classification Taxonomy or in NIST SP.800-61 can help to record information in a structured way.

Records should be classified according to the organization’s policy and stored in a way to ensure the confidentiality, integrity and availability of the data. Uploads and modifications should be traceable and the history of all objects should be kept. A data model related to phase transitions can support data governance and ensure team members have access to the latest and most accurate information.

Records of risk assessments, security incidents and relevant vulnerabilities should be archived for at least 5 years after the closure. This should include records of the nature of the security incident or vulnerability, the affected assets, involved personnel, assessment results, taken decisions and actions. Records could include raw data or other information collected during the investigation, but as data volume can be excessive, these should only be kept for specific reasons, e.g., to preserve forensic evidence.

Event data that has been assessed as not relevant (i.e., that did not lead to opening an incident or vulnerability) may still become relevant at a later point in time. E.g., when a system compromise is detected, it may be important to review older log files to investigate when and how the system was compromised and what unauthorized activities may have been performed since then.

For such data collection recording, organizations should define appropriate policies addressing data classification, handling and retention, based on the affected assets’ participation, on threat scenario severity and on the volume of data. The severity criteria should be based on relevant regulation.

CHAPTER 3

ORGANIZE AND PREPARE

This chapter provides guidance and considerations on the first stage of Information Security Event Management (ISEM) framework to allow for recurrent security event management process to be performed:

- Establish a common set of key roles and responsibilities.
- Establish policies that will guide the development of the ISEM plan.
- Utilize security risk assessments to prepare for ISEM activities.
- Identify internal and external organizations for information sharing.
- Establish a Security Incident Response Team.
- Prepare tools and support processes for ISEM.

3.1 ORGANIZATION & KEY PEOPLE IDENTIFICATION

This section describes the roles and responsibilities of the ISEM actors involved in an organization's ISEM process. The purpose of defining roles and responsibilities is to create a cross-functional team that includes technical expertise in event management. The ISEM roles can be divided into:

- ISEM core roles
- Related supporting roles

The roles and responsibilities associated with the core team can include:

- **Management Team:** is responsible for coordinating among various stakeholders, establishing ISEM budget, and staffing. Management Team is also responsible for strategic and business-related decisions. The accountable manager or suitably authorized delegate is included in the management team.
- **Security Incident Response Team (SIRT) Leader**: is responsible for operating the overall ISEM process. The SIRT leader establishes procedures, policies and develops the communication strategy to enable seamless communication that is validated by the management team. During incidents or vulnerabilities, the SIRT leader oversees activities and keeps contact with main stakeholders.
- **Monitoring team**: is responsible for security events monitoring activities, identification of relevant events, recording of security events and tracking of vulnerabilities and incidents.
- **Operations teams:** are responsible for operating the various IT systems in the ISEM scope. They implement and control technical security measures, approve changes to the IT infrastructure and support the analysis and response to incidents and vulnerabilities.
- **Vulnerability Management team**: is responsible for the analysis and mitigation or correction of vulnerabilities.
- **Security Incident Response Team (SIRT):** is responsible for handling incidents when they occur, and for performing in-depth analysis and mitigating the damage of incidents. The SIRT may require several roles to ensure that incidents are managed and coordinated effectively.
- **Safety manager:** is responsible for managing security incidents that may have potential safety impacts, and for ensuring an effective safety event management process.
- **Accountable manager:** is responsible for coordinating with authorities and ensuring that the whole ISEM process is effectively managed (i.e., resourced and skilled appropriately).
- **Product engineering teams:** are responsible for the design, development, verification, and maintenance of assets in the ISEM scope. They implement technical security measures in products, assess the impact of changes, and implement remediation in response to incidents and vulnerabilities.
- **Communication team:** may be involved to define and establish an information sharing program between the different stakeholders

The roles and responsibilities associated with the supporting team (optional) may include:

- **Audits and risk management team:** may be involved in identifying the assets to be monitored within the ISEM scope.
- **Legal/Regulator expert team:** may be involved to ensure that an organization's legal and regulatory compliance is well protected even in the case of a security incident.
- **Crisis management team, business continuity team:** these teams may be involved when there is a crisis situation due to a security incident. A crisis being a situation in which Hazardous or Catastrophic conditions exist with the service or product.

NOTE:

- The Organizational structure can lead to differences in naming conventions for ISEM-related roles and how specific responsibilities are allocated among organizational personnel. For example, the Accountable manager for a DOA is often referenced as Head of Design Office in Europe.
- Organization may define other roles as needed to support the ISEM process.
- The term 'team' is used to indicate that larger organizations will commonly have several people assigned to the respective role. In small organizations, a single person can take several roles.
- Within an organization, effective internal communication is essential to ensure the proper sharing of information. This can be achieved by setting up an information sharing program involving all team members, including core teams and related roles. The information sharing program can also include the communications with other stakeholders. It should be coordinated with or integrated in existing teams (e.g., Aircraft Information Security Center as defined in ED-204A/DO-355A).

3.2 INFORMATION SECURITY EVENT MANAGEMENT POLICY

O3.1: The ISEM scope, objectives, organization and processes are defined.

O3.2: The processes for information security event detection, analysis, response and recovery are established and managed.

O3.3: The methods and tools for information security event detection, analysis, response and recovery are defined and deployed, including:

- **a)** Asset inventories and associated technical documentation,
- **b)** Risk assessment method,
- **c)** Security event sources, collection and screening methods and tools,
- **d)** Information sources and assessment methods for investigation,
- **e)** Response plans,
- **f)** Recovery plans,
- **g)** Lessons learned capture and continuous improvement.

An organization should implement an information security event management policy that defines the ISEM scope, objectives, organization and processes. In addition, the organization's ISEM policy should be consistent with their other policies.

The information security event management policy is typically at a high level, specifying high level objectives. It is part of the ISEM deployment plan and is then complemented by artifacts that further specify the ISEM architecture and processes. An organization should manage changes to ensure that all related ISEM artifacts reflect the latest organizational structure, processes, technologies and implemented technical solution. An organization needs to ensure that its security event management policy content addresses the following key elements:

- Statement of management commitment.
- The purposes, objectives and the scope of the policy.
- The Scope of the systems considered.

- A reference to the artifact describing information categorization rules for security incidents and vulnerabilities.
- A high-level overview or visualization of the incident and vulnerability management process flow from preparation, through detection, analysis, response, and recovery.
- A definition of roles and responsibilities for each phase of the information security event management process.
- A reference to the artifact describing the sharing, disclosure and communication of information.
- A reference to the artifact describing the tools that will support the security events management.
- A reference to other relevant policies, e.g., information security policies.
- References to the artifacts describing the methods used for:
  - Security risk assessment,
  - Security event collection and screening,
  - Incident investigation,
  - Continuous improvement,
  - Containment plans,
  - Response plans,
  - Recovery plans
- Lessons learned capture and continuous improvement.

An existing standard, such of ISO 27035, could be used as the basis for an information security event management policy with appropriate consideration for aviation.

3.3 SECURITY RISK MANAGEMENT CONTRIBUTION TO ISEM

3.3.1 Introduction

O3.4: Assets are identified.

O3.5: Interfaces with connected organizations are identified.

O3.6: Threat scenarios for risks to aviation safety are identified.

O3.7: Information Security risks for aviation safety are identified.

O3.8: Event detectors are in place to detect security events related to the identified threat scenarios.

O3.9: The risk assessment criteria allows comparability and compatibility with connected organizations.

O3.10: Maximum acceptable lead times are defined for:

a) Time between the occurrence and the detection of an event (time to detect)

b) Time between the detection of an event and the declaration of an incident or vulnerability (time to identify)

c) Time between the identification of a security incident or vulnerability and the notification to authorities (time to report)

d) Time between the identification of a security incident or vulnerability and the mitigation of associated risk to an acceptable level (time to fix)

Information Security Event Management is based on the expected outcomes of Security Risk Assessments (e.g., assets, security measures, threat scenarios, etc.). Security risk assessment standards could be applied for aircraft (recommended by ED-203A / DO-356A), or for aviation systems in scope of the document. The security risk assessment method should be documented and referenced in the ISEM policy.

The security risk assessment is the initial step to evaluating and identifying risks and consequences associated with vulnerabilities and incidents. Security events have to be continuously monitored so that proper arrangements can be made for dispositioning a security event. Security risk assessments need to be kept up to date and reviewed with the experience from incidents to adequately identify the risks.

An organization should define and deploy event collection (e.g., logging policies) and detection capabilities based on the results of the security risk assessments. Detection

capabilities support the detection of vulnerabilities in the security architecture, as well as detection of early signals when a threat scenario materializes.

The ISEM process is a core security infrastructure component with access to data from systems across the aviation environment (including the aircraft and interconnected systems). Use cases for generating data for use by the ISEM process should be risk-driven, and therefore built with outcomes from risk assessments. Avoid building a complex security monitoring system that delivers very low value to the ISEM process.

Section 3.3.2 provides a reference model to do a simplified assessment of the risk for organizations or assets which do not have one. For those who have a risk assessment, section 3.3.3 helps to facilitate the alignment, coverage, and artifacts from security risk assessment to the ISEM process.

3.3.2 Preparation without Security Risk Assessment Inputs for ISEM Process

A security risk assessment is necessary to build an efficient ISEM process. In fact, the risk assessment brings essential information about vulnerabilities and security aspects of the monitored system.

These enablers are prerequisites for ISEM. The goal of this section is not to complete a security risk assessment, but to provide guidance on the minimum security information needed for ISEM.

The minimal elements required for ISEM should include the identification of assets, threat sources and attack paths.

Threat sources are any intent and method targeted at the intentional exploitation of a vulnerability.

Attack paths are the paths, interfaces, and actions by which an attacker executes an attack.

Identifying attack paths, assets and threat sources helps in providing input for vulnerability management and in identifying the assets that need to be monitored and the vulnerability management strategy associated with them. In case of an incident, knowing the affected assets and their dependencies will help with scope identification and containment of the incident. Threat sources and attack paths support the understanding of incident root cause and propagation. Asset classification will help rating the incident's severity and triggering appropriate response.

Information on attack paths, assets and threat sources will also help in developing the detection strategy as presented in chapter 4. The detection strategy contains the information about the detection scope, potential threats and security information to collect and log.

These elements will also be used, as described in chapter 5, to evaluate vulnerabilities in relation with the security context. This evaluation will help to classify the vulnerabilities.

More aviation related guidance about obtaining the information can be found in AMC 20-42 Product Information Security Risk Assessment (PISRA) for aircraft, ED-201A SRA comparability, ED-202A for aircraft risk assessment, ARINC 811 for aircraft operator, ED-205A for ATM/ANS, CANSO Cyber Security and Risk Assessment Guide for air navigation.

3.3.3 Preparation with Security Risk Assessment Inputs for ISEM Process

NOTE: *Risk assessment methods should follow a common set of principles as described in ED-201A / DO-391 chapter 4.*

The structure of a threat scenario contains multiple elements (see FIGURE 3-1):

- Threat sources: a list of threat sources (attacker and attack vector selected from the security environment) that may perform such a threat scenario
  - Attacker; whether human or automated (bots, worms, etc.) and
- Attack Path: a path, interface and actions used to reach the target, including the target itself, and including the assets of the preventive/deterrent security measures that have been by-passed or tampered to get through the attack path

- Vulnerabilities that allow an attack to succeed with the result of a threat condition

- Security measures: a list of the security measures that could mitigate or prevent the attack at each stage of the attack path
- Threat condition: threat condition triggered by the threat scenario.

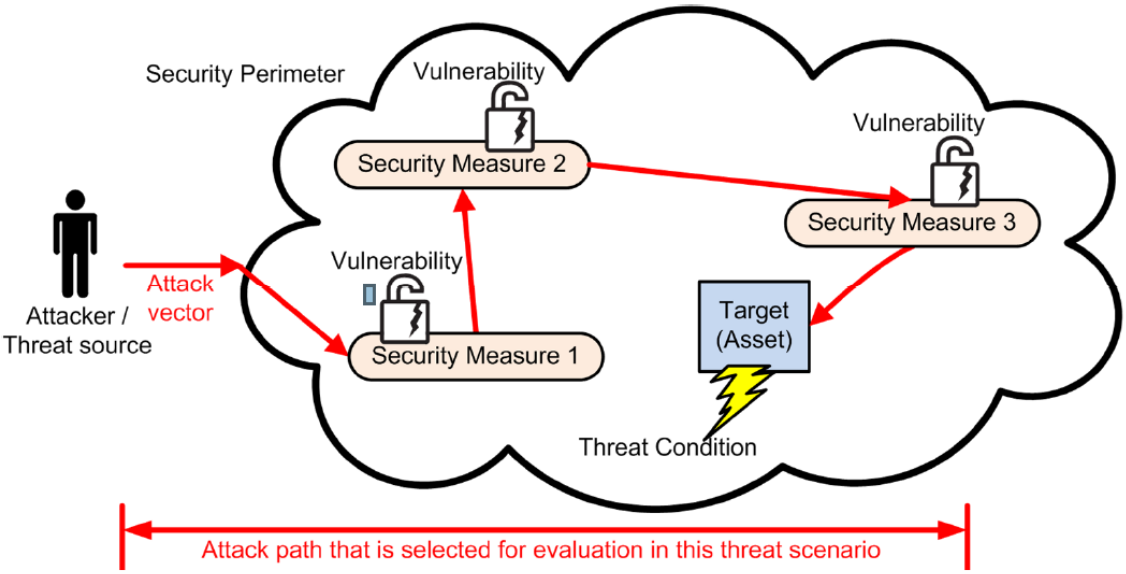

FIGURE 3-1 THREAT SCENARIO VISUALIZATION

Risk assessment will be used as input for vulnerability management by helping to identify the assets to be monitored and the vulnerability management strategy to be associated to them.

The knowledge of the attack paths, security measures, entry points and assets will help to establish the detection means and where additional detection means can be placed. This is part of the detection strategy described in chapter 4. The detection strategy will contain further information to identify the security information to be collected and logged. In case of an incident, knowing the assets and their dependencies will help with scope identification and containment of the incident. Threat sources and attack paths support the understanding of incident root cause and propagation. Asset categorization will help rating the incident's severity and triggering appropriate response.

As described in chapter 5, the risk assessment will also play a role in the analysis of potential effects of vulnerabilities and security events.

3.4 VULNERABILITY MANAGEMENT CONSIDERATION

3.4.1 Vulnerability Management Overview

Per section 2.1.1, Security Vulnerabilities are flaws or weaknesses in system security procedures, design, implementation, or internal controls that could be exploited and result in a breach or violation of the information security policy (i.e. a security incident). The goal of vulnerability management is to support aggregation of information in a structured and consistent way and to assist in mapping of vulnerabilities, their effect and possible consequences in a given environment. Vulnerability Management is the process by which such vulnerabilities are identified, assessed, reported (when necessary), and treated.

3.4.2 Vulnerability Management Strategy

O3.11: The plan to detect and respond to vulnerabilities is established for each asset, including:

a) method and frequency for detecting vulnerabilities is defined

b) the conditions that trigger an action for the concerned asset

c) patching criteria and process are established

d) acceptable lead times for fixing vulnerabilities is defined

The patching criteria and process define which patches are be applied to the asset and how patches are deployed.

O3.12: Organization has means to receive external notifications of vulnerabilities and input these into the vulnerability management program.

3.4.2.1 Identification of Assets subject to Vulnerability Management

Risk assessments (section 3.3.3) identify the security measures contributing to the protection of assets. It is important that once assets are identified, appropriate vulnerability management strategy components are specified, depending on their threat level exposure. For instance, an exposed security asset will require more stringent vulnerability management than a deeply buried asset that is protected by multiple layers of security measures. It is also important to consider assets implementing security measures, as well as assets without their own measures. For example, an attacker may use an asset as a relay to perform other attacks.

3.4.2.2 Identification of Vulnerability Management Strategies

An appropriate vulnerability management strategy depends on the type of asset. In the aviation domain, vulnerability management can apply to a wide variety of type of assets. This includes standard IT systems, airborne systems, industrial control systems and other operational technology, or aviation specific ground systems (ground radar, etc.). These assets implement very different technologies, lifecycles and support models (e.g., COTS software, bespoke systems, etc.). Thus, it is unlikely that a single vulnerability management strategy can be applied across all diverse types of assets. Instead, it is preferable to tailor a vulnerability management strategy appropriate for each class of asset.

For instance, the number of known vulnerabilities for an asset depends on the types of technologies its components are based on.

- For widely used COTS (such as Windows, Linux, etc.), there might be hundreds of known vulnerabilities for a given version, with a high rate of new vulnerabilities.
- For specialized COTS (e.g., COTS specifically developed for a particular sector, such as aviation), there might be a much lower number of known vulnerabilities.
- For bespoke developments, vulnerabilities are generally not known by the public. For example, the vulnerability may not be registered in public vulnerability databases, such as the National Vulnerability Database (NVD), or be known to Computer Emergency Response Teams (CERTs).
- For obsolete or unsupported components, known vulnerabilities are no longer corrected.

Consequently, the vulnerability management strategy needs to be adapted to the type of assets and its components, balancing risk and lifecycle considerations. Examples of vulnerability management strategies are provided in the Appendix B.

To optimize the overall workload of vulnerability management and only perform impact analysis in pertinent situations, the principle is to, in advance, define the enrollment dossier for the vulnerability management strategy using the components of an asset. The vulnerability management strategy of a component may consist of a set of periodic and / or on-event conditions, each associated with rules of what actions to perform. For instance, vulnerability management strategy for an asset may include rules for:

- Identifying vulnerabilities affecting the asset, including where several vulnerabilities along an attack path (chain of vulnerabilities) may aggregate and result in other vulnerabilities or more severe outcomes,
- Identifying applicable patches,
- Performing (or not performing) impact assessment using the “vulnerability analysis” methodology described in section 5.4,

- Implementing workaround and / or precautionary measures, within specified timeframes depending on impact assessment (if applicable),
- Implementing remediation measures, within specified timeframes depending on impact assessment (if applicable),
- Performing regression tests.

In order to ease the specification of vulnerability management strategies of different asset components in the enrollment dossier, it may be useful to define generic strategy templates, and refer to them in the enrollment dossier.

3.4.2.3 Enrollment Dossier

The enrollment dossier should contain all relevant and useful information to maintain security for the concerned asset in its ISMS context. The content may be adapted to the type and context of the asset (e.g., for aircraft or embedded systems, the operator's responsibility may be limited to ensuring the correct configuration and access protection of the asset). For instance, the enrollment dossier could contain:

- The asset identification (name, version, …)
- The owner of the asset in the organization
- The description of the reference configuration of the asset, including:
  - List of hardware components
  - List of software components (for instance using Common Platform Enumeration (CPE))
  - List of reference documents: all relevant documents useful for in-service security of the asset (installation guide, administration guide, …)
  - Summary of the architecture
  - List of prerequisites components
  - List of development tools used to develop the asset (when applicable)
  - List of installed security fixes
  - List of corrected vulnerabilities (CVE)
  - List of residual vulnerabilities
  - CVSS profile for the asset in its environment: CVSS Environment metrics for a first level of impact analysis
  - Vulnerability management strategy for each component of the asset, for instance by referring to vulnerability management strategy templates

The enrollment dossier should be built on or integrated into already available company resources (e.g., IT asset inventory or product Configuration Index) and maintained consistently.

3.4.2.4 Severity Determination

Security vulnerabilities should be associated with quantitative or qualitative means to identify the criticality of the vulnerability in relation to its impact and ease of exploitation, and ultimately reflect its severity to aviation safety. The means should permit prioritization, consistent communication, and like-for-like comparison of vulnerabilities between stakeholders. Section 5.4.4 provides further details.

3.4.2.5 Interfacing with Patch Management

Organizations can have a patch management process deployed which regularly or on demand updates systems with security patches. Typically, vendor recommended patches are installed after a technical evaluation to maintain desired functionality and security. In cloud and service-based IT environments, system updates may even be deployed without specific requests from the user organization. Moreover, many software vendors only support the latest patch level of their product, raising the need for an organization to maintain their software to the latest level regardless of associated security risks.

In the context of a regular patching process (such as for IT environments), any risk assessment of patches should be integrated into that process. Structure the patching process to avoid delays in deployment. Organizations should define maximum

acceptable patch intervals for relevant assets internally and in external agreements where applicable, as defined according to objective **O3.11**. Best practice suggests to not exceed 30 days patching window after a vulnerability has been made public unless additional factors make a vulnerability exploitation unlikely (e.g., if the system is not connected to a network).

Where a system cannot be patched in an acceptable timeframe, e.g., due to no patch available, technical issues with the patch or the system is subject to strict configuration controls, a risk assessment should be done to identify the risks and determine the acceptable treatment. Patch criteria are generated using this information to define how patching will be evaluated for a system, how it will be applied and validated and how often it needs to be performed. Patch processes should also account for issues during the patch deployment, e.g., target systems not online or unforeseen technical issues, and ensure that patching is traceable for each target system. The process should also account for systems where the patch could not be successfully deployed are identified and treated.

Addressing defects and flaws in airborne software follows a different process than the patching seen in most other sectors. Any change in airborne software or data parameters must be accompanied by a change impact analysis and aligned with the associated assurance activities (DAL/SAL). The DAH should provide the operator with a recommendation for the associated incorporation timing for a software release based on the severity of the risk of any included addressed vulnerabilities. Naturally, any safety relevant items are expected to follow the appropriate airworthiness processes.

3.4.3 Vulnerability Disclosure

An organization can optionally set-up a Vulnerability Disclosure Policy (VDP) to benefit from the general public report on suspected vulnerabilities impacting the organization's own assets through a secured channel and process.

This disclosure program is not intended to collect reports from customers, suppliers, or contractors of the company for which other communication means are set.

The VDP program needs to be easily accessible by security researchers and the company website contact page can be a good hosting place.

The following information is expected to be given to the researcher:

- VDP program scope: Assets impacted by this VDP program.
- Legal notice: to remind security researchers that infringing laws, intellectual property, or harmful and intrusive testing is forbidden.
- Responsible disclosure: it is expected that security researchers do not to publicly disclose uncorrected vulnerabilities to minimize the risk of exploit.
- Submission method: the data transmission in between parties should use secured channels.
- Reporting: vulnerability description, details needed to reproduce the vulnerability, discovery timeline, impacted product or services.
- Acknowledge response time to provide an initial response.

ISO29147:2018 can be used as it provides relevant guidance on establishing a vulnerability disclosure policy.

3.5 INFORMATION SHARING

3.5.1 Purpose

An effective measure to address the information security challenges of organizations is to share security related information between organizations in a timely and rapid manner. It is also an efficient approach for those organizations in support of managing the collaborative security risk in a domain such as the aviation sector where the security threat landscape is constantly shifting.

Rather than attempting to establish information sharing agreements during an active security incident, organizations should plan in advance and have agreements in place with external parties before incidents occur. Such advanced planning helps ensure that participating organizations establish trusted relationships and understand their roles, responsibilities, and information handling requirements. Examples of external parties

include other incident response teams, law enforcement agencies, certification authorities, internet service providers, and constituents and customers. An external agreement as defined in ED-201A / DO-391 helps ensure that all parties know their roles and that effective lines of communication are established. The organization needs to consult their legal department before initiating any coordination efforts. There could be contracts or other agreements that need to be put into place before discussions occur for the establishment of this external agreement.

Events that impact aviation safety are likely to be required to be reported per existing regulations such as EU Regulation 376/2014, EASA part 21.A.3, future EASA Part-IS and FAA 14 CFR 21.3.

After agreeing on guiding principles and rules of engagement, it is also important to agree on how to apply them in the specific environment of the “originator” or “recipient” organization. Therefore, best practices, dedicated steps and guidance for consideration are:

- Define and recognize actors and their environment
- Set and accept guidelines, rules of engagement or policies (3.5.2.1 & 3.5.2.2)
- Pre-define the costs per actor and for the entire process
- Acknowledge the benefits and goals
- Define the communications strategy (3.5.2.3)
- Define and accept the formats of the TLPs (3.5.3.1)
- Setup rules to review and accept the sharing process and tools (3.5.3.2)
- Setup routine tests to ensure that the technical infrastructure needed for information sharing is still secure
- Perform routine exercises to ensure processes are effective and that the level of cyber hygiene is understood by all actors
- Define rules to establish the credibility and reliability of the information (3.5.3.3)
- Define the type of information to be shared
- Establish a detailed contact list of the organizations and information security contact persons
- Select the information types (3.5.3.3)

3.5.2 Guiding Principles (general)

Technical guidelines and principles (see 3.5.3) are important to build up a solid foundation for information sharing, however it has been noticed that general guiding principles further harden the process and methods.

3.5.2.1 Rules of Engagement/ NDA

The establishment of rules of engagement or a Non-Disclosure Agreement (NDA) is important especially when a more formal legal agreement/contract is not in place with all the parties. Through these mechanisms, the parties agree not to disclose security information or non-public business information. An NDA creates a specific legal relationship between the parties, typically to protect any type of confidential and proprietary information or trade secrets.

3.5.2.2 Legal Protection

Legal protections exist in certain jurisdictions, to protect organizations from liability if they share information security data. These protections address an organization’s concerns around liability, as well as encourage organizations to participate in sharing efforts by reducing the risk of sharing.

3.5.2.3 Communication

Communication within the information sharing community, or using information sharing platform, can be time-intensive. Communications activities are drafting and distribution of bulletins and reports across organizations, exchanging with public media, providing further technical analysis or denying fake news. The burden can be reduced by using some good practices: using pre-built templates, gathering different information in the same communication and create awareness of time needed to perform activities. Requirements may be cascaded to external organizations such as suppliers, service

providers and vendors to facilitate: the detection of security events; the analysis of vulnerabilities; and to improve the efficiency of incident handling.

3.5.3 Guiding Principles (technical)

The primary aim of information sharing of information security events, incidents and vulnerabilities, is to notify potentially affected organizations about the event and allow them to assess and remediate the effects. In addition, other organizations may benefit from the experience gained during an event and share best practices for handling them.

To facilitate the sharing of information between two or more organizations, it is paramount that the “originator” organization and the “recipient” organization(s) agree on certain terms of reference for the exchange, as described in more details in this section. In many cases, the information exchange between parties is voluntary. It is possible that the information to be shared deals with an attack that is still ongoing. In this case, in order to prevent disclosure from any stakeholders taking part in the information exchange, the issuing organization can use a special formatting like the Permissible Actions Protocol from the MISP project to indicate how the received information should be used.

3.5.3.1 Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) is a set of descriptions used to ensure that sensitive information is shared with the appropriate recipients, in a well categorized manner. To be able to indicate the expected sharing boundaries, the TLP categories uses four colors determined by its Originator to signal how widely or narrowly, they want their information to be circulated to its recipients. Through selective redactions by the Originator (or with its agreement) the original TLP can as well be downgraded.

The TLP does not prescribe the way or the tools to handle the information exchange, it does not imply any process for security clearance or prior approval other than the assignment from the recipient’s organization. Neither is the TLP categorization, a formal scheme of classifying information according to secret or sensitivity based upon “harm to the organization”.

TABLE 3-1 TRAFFIC LIGHT PROTOCOL (TLP) DESCRIPTION

TLP:WHITE	**Disclosure is not limited** Information may be **distributed without restriction** and is subject to standard copyright rules
TLP:GREEN	**Limited disclosure, restricted to the community** Information may be **shared with peers and partner organizations** within their sector or community, but not via publicly accessible channels
TLP:AMBER	**Limited disclosure, restricted to participants’ organizations** Information may **only be shared with members of their own organization**, and with clients or customers who need to know the information to protect themselves or prevent further harm
TLP:RED	**Not for disclosure, restricted to participants only** Information may **not be shared with any parties** outside of the specific exchange, meeting, or conversation in which it was originally disclosed

3.5.3.2 Tools

Sharing digital information will not always be within a secured SOC (Security Operation Center) network but can be carried out on a peer-to-peer basis in a specific shared network. Therefore, (depending on the TLP description) a secure exchange through email encryption, secured tools or platforms is very important to build up trust and confidence. To ensure the confidentiality of shared information, use email encryption such as S/MIME or PGP, or secure messengers such as CryptoGraf, Signal or Riot. To

share threat intelligence, use structured formats and platforms such as STIX or MISP and restrict access to web portals, forums and shared drives.

3.5.3.3 Credibility and Reliability of Information

In order to properly manage incoming information received by the organization from different sources like VDP or threat intelligence, the organizations may develop a source evaluation and information reliability information methodology that could help throughout the ISEM process until the external sharing or reporting. The Naval Intelligence Division (NID) model can be used for that purpose.

3.6 SECURITY INCIDENT RESPONSE TEAM

A Security Incident Response Team (SIRT) is responsible for handling incidents when they occur, performing in-depth analysis, and containing and mitigating damage from incidents. The SIRT could further facilitate incident prevention and management with audits and making proposals for incident mitigation. A properly organized SIRT is part of the organization's broader secure engineering initiative.
Preferably, an organization would have a dedicated Security Incident Response Team, independent from teams in charge of development and operations of the assets, but this is not always possible. The SIRT function can be partially or completely outsourced.

3.6.1 Team Roles and Definitions

Organizations should document their SIRT model, members, processes, methods and tools in their ISEM policy, or in a specific SIRT charter referenced in the policy.

SIRT should involve people with different roles to operate properly. Not all roles are mandatory for all teams, except Incident responder role. All other roles are based on organizational needs. SIRT roles and the definition of each role is listed below.

- **Incident responder:** responsible for first response to security incidents, coordinating activities, preparing and executing incident response plan.
- **Communication Focal point:** responsible for communicating with internal and external stakeholders.
- **Forensic Analyst:** responsible for preserving, collecting and analyzing digital evidence from systems affected from security incidents.
- **Malware analyst:** responsible for analyzing malware samples involved in incidents.
- **Cyber Threat Intelligence Analyst:** responsible for collecting, analyzing, validating and distributing cyber threat intelligence related to incidents.

There is no single one-size fits all product security incident response strategy or team template for all organizations to follow. However, three SIRT models are used by most companies:

- Distributed
- Centralized
- Hybrid

Depending on the size and the structure of an organization, different models for SIRT organization can be applied. Smaller organizations may choose to have one central SIRT, whereas bigger organizations, with multiple sites or diverse IT systems may have several SIRTs covering different scopes. In case of multiple SIRTs, a coordinating team should be set up to advice and coordinate between the SIRTs.

3.6.2 Capability Building for Security Incident Response Teams

Preplanning should establish the types of incidents, thresholds and/or risk levels that prescribe what activities or actions need to be taken. For example, some incidents are unacceptable and may mean immediate grounding of one or many aircraft. Such decisions are much easier to make if there are predetermined strategies and procedures for classifying and containing the incident. Organizations should define acceptable risks in dealing with incidents in accordance with the application regulation for the organization and developing strategies accordingly. Organizations should create tailored containment strategies for each major incident type, with criteria documented

clearly to facilitate decision-making. For example, for an aircraft system that impacts flight safety, a fail-safe strategy should take priority over a fail-secure one.

SIRT staff should build and continuously improve their capabilities with practice and routinely exercise their incident response, malware analysis, and network forensics. During periods with no detected incidents, practical exercise / simulation should be encouraged so that skills and competences remain up to date.

Lab workshops: SIRT staff should improve their practical information security skills with lab exercises and workshops. Exercises and security drills can be either table-top exercises or hands-on technical exercises.

3.7 TOOLING

Tools can be used throughout the ISEM process. The identifications of tools to support ISEM is crucial.

- Collection tools could be used to collect the logs and other data sources. The logs can then be processed using other analysis tools or stored for conservation.
- Parsing tools could be used to transform raw data into usable data for automatic processing by other tools
- Detection tools could be used to analyze the logs and detect if a security event has occurred based on the content of the data.
- Forensic tools could be used to investigate the logs and find useful information for event categorization and to understand the impact of a security incident.
- Vulnerability management tools could be used to manage the knowledge of vulnerability and help in classifying them, tracking them and evaluating their impact in relation to a security context.
- Ticketing tools could be used to enhance the communication with the different actors and to track the status of a security event or a security incident during its whole lifecycle including archiving.
- A case repository or database for security events could be used to ensure proper record keeping and archiving by registering relevant events, storing associated data and tracking related actions.
- A maturity model, like the CSIRT SIM3 model, can be used to have access to indicators about the different implemented process.

CHAPTER 4

DETECT SECURITY EVENTS

Detecting security events is the process of discovering evidence of possible security incidents and vulnerabilities. Detecting security events cannot prevent security attacks but does assist in forensic investigations and can be used to improve the security design.

Detecting security events is the first step so that incidents can be dealt with appropriately. Every organization needs to do it for assets in their scope. Interconnection in aviation means that joint efforts are needed.

Event detection is enabled and managed through a joint effort between producers, operators and maintainers of avionics systems. For aircraft, this can include the Design Approval Holder (DAH), Production Approval Holder (PAH), aircraft operator and suppliers of aircraft information services. For air traffic management systems, this can include the system suppliers, the system integrator, and the ANSP.

Security events are observed or discovered by monitoring event sources that need to be defined and/or implemented according to the detection strategy. Additional considerations are discussed in section 4.2 of this document. For industrial systems, OEMs, vendors, and integrators can be included.

4.1 General

Security event detection involves the observation of any relevant occurrence of an anomaly that is relevant to information security. The process of security event detection comprises the collection of events from several sources, the identification of security relevant events, the application of rules to determine event criticality and the triggering of adequate response processes. The detection scope is defined through security risk assessments, identifying the assets to protect and the relevant threat scenarios.

Security event detection includes:

- Collection of events
- Identification of relevant events
- Dispatch to the appropriate team

In general, all relevant assets identified in the risk assessment should be monitored for events. The details of event sources to monitor, events to collect and screening rules should be documented in the detection strategy, explained in section 4.2.2 of this document.

Each security event should be evaluated with respect to its potential criticality. Security events that are evaluated critical, exceed predefined thresholds, or are otherwise suspicious, should undergo analysis as defined in chapter 5. Such a security event should be evaluated as a possible security incident as described in the security event triage section.

4.2 Detection Strategy

O4.1: Security events are collected and screened that indicate deviations from predetermined functional performance baselines.

Section 3.3 discusses security risk management as a contribution to the ISEM organize and prepare process. The following text expands on the concepts in greater detail for clarity regarding the ISEM detection process.

An organization should define and document their event detection strategy. It should be structured into clearly defined goals or objectives.

Developing an efficient detection strategy for security events is about establishing the monitoring of variable/evolving elements associated to security risks. Security risk level is determined by likelihood (Level of threat condition) and impact. The enrollment dossier should be reviewed for relevant information concerning vulnerabilities and impact. Reference section 3.4.2.3 Enrollment Dossier.

One method is to consider all risks identified by a security risk assessment and according to the enrollment dossier. Each risk is defined within the context of use cases or scenarios. That is, each risk associated with an asset should be analyzed and described against each of the three attributes of security risk, Confidentiality, Integrity, and Availability (CIA). For each of these attributes, a use case can be described that demonstrates how the attribute was identified by the risk assessment. For example, for each asset defined in the risk assessment:

- Vulnerability - Consider the likelihood that the vulnerability would be exploited, that a vulnerability-threat pairing would be realized. Consider which security attributes need to be protected and what are the potential consequences of each compromised asset.
- Security Events – What are the possible scenarios that could describe the details of events and method of detecting each possible security event?
- Security Events – Implement event triage and consider the possible scenarios that are consistent with the indications of the event. Determine if the event is a security incident.

For the detection of security events, the strategy should define use cases for detection. Each of these would describe a detection scenario in a way that demonstrates rules used to define the event as suspicious. Things to consider for each scenario are as follows:

- Event source (with respect to the assets under evaluation)
- Event type (based on predefined classification categories)
- Syntax of the rule within a specific security information and event management (SIEM) system

There are two possible general cases to consider when detection strategy is defined. For each asset:

- Case 1 – The asset Original Equipment Manufacturer (OEM) has provided guidance or instructions to monitor security during the operation phase.
- Case 2 - Event detection needs are derived from a security risk assessment.

4.2.1 Case 1 – The asset Original Equipment Manufacturer (OEM) has provided guidance or instructions to monitor security during the operation phase.

Section 3.3.2 discusses preparation without security risk assessment Inputs for ISEM process. The following text expands on the concepts in greater detail for clarity regarding the ISEM detection process.

When full coverage of the information security methodology and practices have been put in place by the asset OEM, and the security event detection strategy is defined:

- The perimeter to monitor is formally identified.
- The assets' identifications are established.
- The security risk assessment and associated elements like security risks list, related threat scenarios, and underlying associated vulnerabilities are identified.

In addition to the assets for which the monitoring strategy is defined by the OEM, an organization should identify any other relevant assets and verify prerequisites and assumptions made by the OEM. These elements together define the monitoring perimeter of the asset. See FIGURE 4-1.

The OEM will provide recommendations and instructions on how to securely operate the asset, but this may include technical and operational security measures to be defined and deployed at the user organization level (e.g., Ground Support Equipment (GSE) should be free from malware, software installed/operated in a trusted environment, etc.).

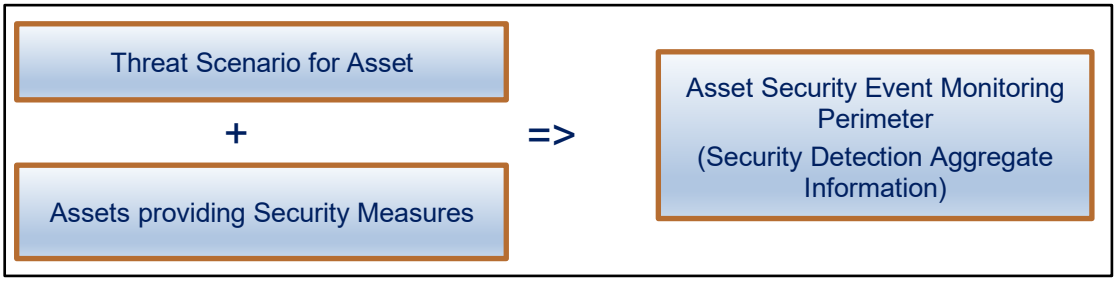

FIGURE 4-1: ASSET EVENT MONITORING PERIMETER

4.2.2 Case 2 - Event detection needs are derived from a security risk assessment

Section 3.3.3 discusses preparation with security risk assessment inputs for ISEM process. The following text expands on the concepts in greater detail for clarity regarding the ISEM detection process.

When full coverage of the information security methodology and practices is not put in place by the OEM during design and development of assets, the security event detection strategy is not previously defined and readily available to help end user organizations develop their detection strategy process. The OEM has not provided the necessary elements to fully describe the asset security detection perimeter. Therefore, steps should be taken by the end user organization to establish the security detection perimeter. This can be done using two steps.

- Identify assets to define the security perimeter to monitor
- Identify possible threat scenarios for the asset

4.2.2.1 Collect and use available key elements defining the security perimeter to monitor

If no security information has been provided by the OEM for some assets, the organization should determine which of these assets needs to be considered. This can be done by listing all assets which have no associated OEM provided information security management guidance. List all the external digital interfaces of the asset, and for each of them use generic threat scenario lists. Use generic threat scenario lists to assess the security vulnerabilities of each asset and identify all assets that have a significant risk scenario, and therefore a significant security risk that should be considered. From this list of at-risk assets, determine and prioritize the security measures for each asset. Finally, use generic threat scenario knowledge base lists to evaluate the potential risk. See FIGURE 4-2 for an illustration of the process.

As information security monitoring should be implemented even though pre-requisite elements were not provided, the following points are considered.

- The perimeter to monitor for security risks can be established.
- The perimeter elements associated with each asset can be listed and include functions, applications, and services.
- In this case, a security risk assessment is not formally available. This means the threat scenario, and underlying associated vulnerabilities are not formally listed for the identified perimeter and sector of use.

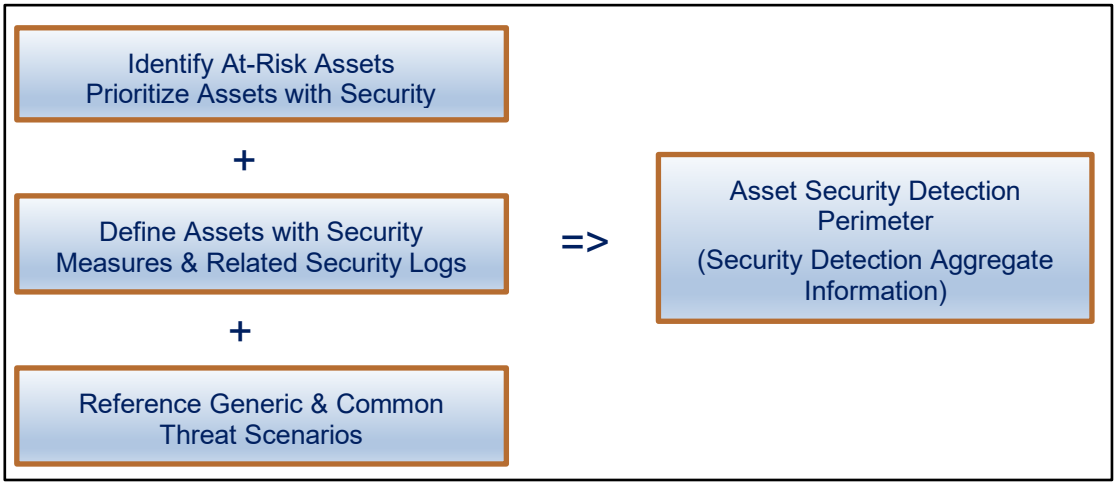

FIGURE 4-2: TOP-DOWN APPROACH TO BUILD THE SECURITY EVENT MONITORING PERIMETER

Evaluating the assets providing security measures and other support for risk requires conducting a 2-step approach:

The first step is to identify the critical elements to consider (data, network, etc.):

For each element:

- Identify the assets within the perimeter and identify the list of associated assets providing security measures and other support.
- Once this list of assets is identified, then identify the security logs available in these elements for each asset. Refer to section 4.3.1 for more information regarding security logs.
- Information from other log sources such as maintenance logs and operational logs should be considered when available. Although some automatic data collection logs may not be referenced as security logs, they may provide useful information related to threat scenarios.

The second step is to establish a possible list of threat scenarios.

4.2.2.2 Identify possible threat scenarios for the asset

Using a recognized threat scenario knowledge bases, an organization can assess how the assets identified in the first step can represent vulnerable entry points and which data elements they should monitor within these assets.

Following this, the organization identifies possible threat scenarios for the asset using generic threat scenario lists. There are several security documents that can provide scenarios to consider during evaluation of asset risk assessments.

Based on identified assets in the risk assessment as performed in section 3.3, detection measures should be deployed to detect relevant threat scenarios where possible. This should include vulnerability monitoring for any exposed assets, as well as assets used for security measures. Vulnerability monitoring should also include the detection of compromises for assets. Associating detection measures to the related threat scenarios will support the criticality assessment of incidents and vulnerabilities.

If from the threat scenario the connection between the asset's threat condition and the feared safety consequence is not immediate, detection measures should allow for an early detection of compromise to give organizations sufficient time to analyze and correct the situation. Furthermore, detection measures deployed behind a security measure can help monitoring the effectiveness of the measure and detect potential breaches.

In addition to technical measures, organizational measures should be considered, e.g., user awareness for detecting and reporting suspicious observations or the monitoring of security conferences for new attack methods and vulnerabilities.

Context information should be considered to determine if a given event is a legitimate event. For example, as operational policies such as an approved log change are implemented, the interpretation of a log analysis would be a changed context.

4.3 Security Event Information Sources to Monitor

Evidence of information security events can be observed and noted from several different sources. The Monitoring Team should establish and monitor all relevant sources for security events identified by the risk assessment. Some sources may be defined without a risk assessment using the enrollment dossier (see event sources list below in this chapter). However, a minimum set of internal sources are determined by risk assessments. Additional sources such as vulnerable data feeds can be monitored also.

Many sources are identified by the risk assessment as described in sections 3.3.3 and 4.2.2. However, some sources may be defined without a risk assessment. See sections 3.3.2, 4.2.1, and event sources list below within this chapter.

Additionally, organizations should foster a security culture with governance established by organizational management. The SIRT leader should establish guidance of what people can look for that may indicate suspicion of security risks.

The following are typical sources to monitor for security events. Most items in the list point to a section where the security risk source is described in detail:

- Event detection notifications from security event detection software tools. Some systems, especially ground systems, have intrusion detection and prevention systems (IDPSs) that alert security personnel if there is an anomaly indicating the presence of a security event
- Embedded information system security Log File Data. Refer to section 4.3.1
- External Notification from system manufacturers, DAHs, or other users regarding events and/or incidents specific to systems, system components, and software. Refer to section 4.3.2
- Unexplained system failure if root cause is not found. Refer to section 4.3.3
- Physical evidence of possible tampering, hacking, intrusion. Refer to section 4.3.4
- Other sources (Media report, Organizational feedback, etc.). Refer to section 4.3.5
- Vulnerability databases and other vulnerability information sources, including Common Vulnerabilities and Exposures (CVE) programs, that provide collections of vulnerabilities that have been identified and publicly disclosed. Many sources also provide Common Platform Enumerations (CPEs) that associate CVEs to products. These databases typically provide live data feeds that can be used to automate some aspects of vulnerability monitoring. Refer to section 4.3.6.
- Vendor bulletins, which may indicate discovered vulnerabilities and if they have been remediated as part of a new release. The bulletins may also describe the characteristic or abnormality associated with the vulnerability.
- Vulnerability scan reports, which may be provided by the OEM and others during development. These can also be provided by internal or external security audit centers. These can provide information regarding discovery of new vulnerabilities.
- Test and audit findings performed by the audit team generate reports that could indicate vulnerability to attacks.
- Operational and incident reports generated by organizations such as operators, MROs and OEMs, provide current and historical information that can be used to indicate possible sources.

4.3.1 System Security Log File Data

System log files are created and maintained by embedded log file functionality within ground and aircraft information systems to trace system activities. Some systems may produce dedicated security logs or audit logs, whereas other systems may only provide

operational logs. They may be used to confirm that all system actions can be attributed to an authenticated identity of a person or automated process. Some systems are configured to maintain log files that record specific information such as failed access attempts and systems modifications. Logs can have many uses, such as intrusion detection, determining the root cause of a system failure, or simply tracking the use of a particular resource. System log files can contain a mix of information in which some are not relevant to security analysis. System log files are retained and analyzed for indications of suspicious activity, possibly consistent with a security event. In the case of onboard aircraft security log files, they are typically downloaded and retained for analysis using ground tools.

The log file data may be analyzed using security information and event management (SIEM) ground systems to discover security events. The organization should include within its information security plan guidance to manage, analyze, and record security events discovered in security log files.

The acronym SIEM is not to be confused with Information Security Event Management. ISEM is the overall process of detecting and managing security events and security incidents. It is the title and focus of this document.

Security Information and Event Management (SIEM) systems are log management systems specifically tasked to collect log data from several servers or other network devices for the purpose of interpreting, filtering, correlating, analyzing, storing, and reporting the data.

SIEM is a combination of Security Event Management (SEM) and Security Information Management (SIM). SEM is an analysis of log and event data in real time to provide threat monitoring, event correlation and incident response. SIM collects, analyzes, and reports on log data. The SIM and SEM parts of the SIEM, are computer security disciplines that use data inspection tools to centralize the storage and interpretation of logs or events that are generated by other software running on a system or network.

During analysis, SIM systems can correlate event information from multiple log files from multiple systems via event time stamp information (Coordinated Universal Time (UTC) or processor cycles and power on time) that is embedded within the log files. This feature can be useful in providing cross system event relationships during the analysis of security log file data.

4.3.1.1 Log File Technical Information and Management Guidance

The system manufacturer should provide the necessary technical information regarding the security log files to support the development of an effective security information and event management (SIEM) system. The following are examples of required technical information:

- Names and locations of log files
- Maintenance instructions and tools for download of log files
- Structure and content of log files
- Description of all relevant data fields

The security log file definition and structure are specific to each aircraft or ground system type and should be supplied by the DAH or ground system OEM.

The DAH or ground system OEM should supply the following information regarding security log files:

- Recommendations around triggers or frequencies for acquisition and analysis of log files
- Recommendations around transferring, storing and safeguarding log files (to maintain applicable confidentiality, integrity, authenticity, and availability)
- Recommendations around retention times for log files
- Documentation and guidance for review and analysis of log files (including event signatures, associated root causes, recommendations for reaction and categorization of security events)

In the case of an aircraft, system or equipment DAH, this information could be conveyed in the form of integration guidance, instructions for continued airworthiness, operator guidance or other material (see DO-356A/ED-203A and DO-355A/ED-204A).

Some elements, such as storage needs or retention times for log files, could be impacted by regulations applicable to the organization operating the asset. Asset operators should ensure an asset's logging capability is able to meet any applicable regulations.

Additional detailed guidance for using, scanning, and processing aircraft log file data can be found in ARINC Report 852: "Guidance for Security Event Logging in an IP Environment". Ground system log file data should be processed according to guidance provided by the system OEM.

Aircraft information security events should primarily be determined by inspection of the aircraft security log. When additional investigation is warranted, additional sources of relevant data may also be considered, such as specific system logs, physical access logs, connected network systems, among other sources.

Aircraft security log file definitions of normal and abnormal field data for each security related function are defined and provided by the DAH. The DAH should provide the following information regarding aircraft security logs:

- Definition of abnormal data event parameters
- Threshold value assigned, indicating a minimum or maximum number of events allowed for each function as appropriate for the data

Examples of security log event indication parameters are:

- Failure of authentication signature checks
- Presence of unfamiliar files
- Presence of unknown programs or processes
- Unusual or unexpected consumption of computer resources
- Unusual or unexpected system crashes

4.3.2 External Notification

Notification from system equipment OEMs, or from other organization's experiences regarding security events specific to system type, system equipment, component assets, etc. should be monitored, reviewed, and addressed. External information from sources such as the Aviation Information Sharing and Analysis Center (A-ISAC) can indicate possible vulnerabilities that are not currently in the scope of the security event monitoring program. Refer to section 3.5 for information sharing guidance.

Information about security events along with their associated security incidents and vulnerabilities, threat intelligence, changes in security environment, or other security relevant information, can be received from various sources. They come in the form of notifications/reports, requests/review items, and advisories/directives from relevant organizations such as national security agencies, regulatory authorities, commercial security services, operators, the DAH, supply chain partners, external service providers, and other supporting organizations.

For connected organizations an interface agreement should define the channels and rules of communication for both parties. For communication with unspecific parties like independent researchers, a Vulnerability Disclosure Program could be implemented to structure information exchange. See section 3.4.3 for more information.

A security notification is timely information involving the report of vulnerabilities, threat intelligence, or changes in security environment which can, or has, affected the security posture of the aircraft or ground systems. Analysis of security notifications may result in identification of a security issue.

4.3.3 Unexplained System Failures (Aircraft and Ground Systems)

4.3.3.1 Unexplained System Failures (Aircraft Specific)

Onboard electronic aircraft systems are contained within the aircraft and are comprised of several components such as Line Replaceable Units (LRU), Line Replaceable

Modules (LRM), and interconnecting wiring. An anomaly within a component can occur as a flight deck effect, an event indication on a log file analysis or other means.

An aircraft system or component anomaly or failure that cannot be explained as a hardware failure could be an indication of a possible event. When an aircraft component is suspected of causing a system fault, the component is replaced. If replacing the component remedies the system fault, then the component is assumed to have an internal failure. The aircraft need not be grounded since the system fault was caused by the component. This failure can be of software or hardware origin within the component. The failed component is sent to an MRO component maintenance facility or to the OEM facility.

If during diagnostic investigation there is no hardware failure discovered that is consistent with the component's reported failure, then the software or firmware may be corrupted. There are too many possible examples to list here. However, any anomaly as a flight deck effect or failure mode that appears to have a directed intent is suspect of intentional tampering.

The avionics component may be processed as having an event suspect if no reasonable explanation for the component anomaly was found in this case, the component should be tested in the shop for corrupted program memory, especially if there are many no fault found events for a component or component type. The security log and maintenance logs can be used to reveal patterns.

If shop testing reveals that there is no problem with corrupted software or firmware, and there is no problem with hardware, and the component test indicates complete operational integrity, then the reported problem may be due to another part of the aircraft system.

If there appears to be no pattern suggesting intentional tampering, the corrupted software would likely be due to an intermittent hardware failure. The component should also be checked to have the correct version of software installed.

If testing determines that the component's software memory image is different from the correct software program memory image, then forensic investigation can be performed to see if the component's memory data corruption was random, or if the data changed in the component represents a directed attempt to change the function of the component.

If the failure mode indicates or suggests intentional tampering with the operational function of the component, then a possible security event may be indicated.

Forensic memory image investigations need to be performed by the OEM, or someone that has access to the component's design information and program source code. This type of investigation should be performed by specialists that have adequate knowledge of the component's internal hardware and software function specification. This information is generally proprietary and restricted by the OEM.

Things to consider in classifying a component as a suspected event are:

- Is the same system failing on multiple aircraft?
- Was an LRU identified as cause of system failure?
- Was the LRU failure due to hardware failure?
- Was the LRU failure due to corrupted software?
- Are there related fault reports?
- Is there a related event in the maintenance log file if one is available?

If there are any unexplained suspicious events from any of these considerations, they should be forwarded to the analysis team for further investigation.

4.3.3.2 Reporting Unexplained System Failures (Aircraft Specific)

When a system failure or anomaly occurs, and the reason or cause cannot be attributed to any detectable or otherwise known event, then further action should be taken. Such occurrences would be entered into the security event log database for analysis. Detection of repetitive occurrences may give cause to escalate an investigation to the OEM or other appropriate information security organization. Detection of repetitive occurrences during the event detection process may be ascertained from aircraft

logbooks or indicated by system diagnostic indication functions when present. Refer to section 6.4 for detailed escalation guidance.

4.3.3.3 Unexplained System Failure (Ground Systems)

All other systems that are part of the aviation ecosystem, including ground systems, may experience unexplained system failures. These systems are generally comprised of several components that form a network. Some of the general network components include computer workstations, file servers, switches, routers, gateways, modems, repeaters, wireless digital communication links and access points.

For many aviation ground and ecosystem components, elements of general components are used in specialized aviation systems such as Air Traffic Management (ATM) systems, satellite communications, navigation and surveillance (CNS) systems, software loading and data distribution systems, and all terrestrial based CNS systems, such as the Airport Instrument Landing Systems (ILS).

Some of these system components have intrusion detection hardware and software that provide alarms for real-time intrusion notification, and software logs that can be analyzed for intrusion events. Intrusion detection may not be available on all systems but should be monitored if it exists.

When an unexplained anomaly is detected or experienced, the cause could be a hardware failure within the system. If the anomaly is related to an intrusion that is software related, intrusion detection capability, if available should be consulted. Failures in communications links, wired and wireless, should be observed and analyzed for possible attack.

If the anomaly cannot be explained by any of these methods, then deeper analysis should be performed to capture possible changes in the system that were not captured by the intrusion detection in place. This may require custom forensic actions that probe deeper into system components and stored log files.

4.3.3.4 Reporting Unexplained System Failure (Ground Systems)

When a system failure or anomaly occurs, and the reason or cause cannot be attributed to any detectable or known event, then further action should be taken. Such occurrences would be reported to the organization's security team, who may escalate an investigation to the OEM or other appropriate information security organization.

The following should be reported to the security team and recorded into the security event database log:

- A list of specific functions affected by the dysfunction
- The nature of the dysfunction
- The time limit allowed to perform the reporting to the organization

4.3.4 Physical Evidence of Event

A physical security breach that could lead to Information security incident should be considered as an event.

Information security events may also be detectable by physical evidence. The operator organization should therefore also monitor physical security events. Examples of these are:

- Unauthorized access to restricted zones
- Failure or damage of physical access controls, locks, seals
- Loss of equipment
- Unauthorized connected devices
- Unauthorized changes to cabling
- Damages on casing, coating, or packaging

Observations on such elements should have an associated reporting process to notify the organization’s security team of violations.

Additionally, observations by all organizational personnel can contribute to the detection of information security events. All personnel that work in various areas around IT and

system assets should be aware of indications that could be possible security threats. Some examples of possible threat indicators are:

- Unauthorized USB Stick found plugged into a server or other system components.
- Suspicious person activity observed in a sensitive area accessible to assets.

Some examples of possible threat indicators related to aircraft are:

- Aircraft related ground equipment (GSE, PED, Maintenance Laptops) having physical evidence of alteration (i.e., tamper tabs, disassembled, altered assembly, etc.
- Information system or aircraft wiring appears to have been tampered with or spliced into
- Indications of unauthorized access to sensitive equipment and assets. Examples are secure rooms containing servers and workstations and the aircraft electronics bay left open at airport terminal.

4.3.5 Threat Intelligence (Media report, Organizational Feedback…)

While the volume of public information relative to event sources is massive and the processing effort is huge, a monitoring and filtering strategy should be used to select only relevant event sources.

There are many potential sources of public information to monitor including but not limited to:

- **Mass media**: newspapers, magazines, radio and TV broadcast, podcasts,
- **Internet**: online publications, blogs, news group, social networks,
- **National sources of data**: governmental reports, press conferences, official websites,
- **International membership associations** sharing threats, vulnerabilities and incidents, technology watch, sectorial news:
  1. IT InfoSec newsletter publication notifying all stakeholders about recent corporate system security attacks
  2. Computer Security Incident Response Teams (CSIRT) / Computer Emergency Response Teams (CERT). They can be national, private, general IT or sectorial (like Eurocontrol EATM-CERT)
  3. Non-profit organizations providing collective support in dealing with security incident resources like ECCSA (**European Centre for Cybersecurity in Aviation)**
  4. Information Sharing and Analysis Centers (ISACs) like Aviation-ISAC provides a centralized industry-specific resource for gathering information on security threats
- **Academic / research publications:** thesis, proceedings, conferences,
- **Public corporate and commercial information,**
- **Intellectual property information**: patents, defensive publications,
- **Cybersecurity events**: DefCon, Black Hat, etc.
- **General industry information.**

Open-source intelligence can also be complemented by government-restricted information given in a discretionary fashion to civil aviation actors on-demand.

Additionally, other transportation industries (e.g., rail, maritime) or other industrial sectors (e.g., energy, finance) can use technologies and information systems similar to those used in aviation. These industries and sectors could be a source of information on events, vulnerabilities, or threats to monitor.

4.3.6 Vulnerability Monitoring

O4.2: Vulnerabilities affecting assets are collected and screened according to the vulnerability management plan.

O4.3: Security vulnerabilities that will not be treated according to the vulnerability management plan are identified for further analysis.

The vulnerability management strategy is defined in section 3.4.2.

It is important to include vulnerability monitoring as a source of event information. Some of the aspects of vulnerability monitoring are described in section 4.3.

If the vulnerability exposes a clear safety risk, it should be assigned a high priority for immediate action as defined in the vulnerability management strategy

Test and audit findings performed by the audit team generate reports that could indicate vulnerability to attacks

4.4 Recording Events Case Information

Relevant detected events should be entered into the event log record keeping database with all pertinent information already available as described in section 2.6. Security event data needs to be retained to help detect patterns or the re-occurrence of identical events. It includes the date and time, the system related to the detected event, the system description, the means of detection, and the apparent effects of the event anomaly. When starting an investigation, the team should immediately record all facts and preserve evidence regarding the case.

CHAPTER 5

ANALYSE

5.1 Introduction on Security Event Analysis

When a suspicious event or relevant vulnerability has been detected, previous risk analyses should be revisited to identify the threat scenarios associated with the impacted assets and threat conditions. Additional analysis of the asset's threat vectors can help to identify the extent of the event and which assets are potentially impacted.

Depending on the nature of the event, the function of the affected assets, their position within the security architecture and the level of threat, security events can be more or less critical. The criticality reflects the risk level imposed by the incident or vulnerability and can be expressed in classes (typically low/ medium/high or green/yellow/red) or with a score (typically ranging from 1 to 10). Criticality can also be a binary evaluation, in that some incidents are at an unacceptable level of criticality if they exist.

Incidents and vulnerabilities are related in that an incident occurs due to the existence of an exploited vulnerability. An exploitable vulnerability may exist only as a risk of an incident if the incident has not yet occurred. Vulnerabilities and their associated incidents carry the same criticality levels.

Definition of criticality levels is up to each organization. Section 5.3.4, section 5.4.3 and section 5.4.4 give additional guidance and section 5.4.5 states that (for vulnerabilities), organizations using a method with a different scale [than in table 5-1] should define and document the way to translate risk scales into the table.

This risk level can be used for prioritizing actions, triggering specific responses (e.g., emergency procedures), or determining acceptable response times or reporting threshold.

For reportability decisions, a score using levels of safety impact verses levels of threat is sufficient for scoring and prioritization. See Table 5-1.

The reporting threshold strikes a balance to ensure authorities receive all important reports that require actions but are not overwhelmed by all the reports for low severity incidents and vulnerabilities.

Aviation uses extensive supply chains and analysis of incidents and vulnerabilities needs to ensure the supply chain is involved for timely and complete analysis. In order for the organizations that are mandated to provide reports to fulfil their obligations, the use of a consistent classification mechanism can ensure equal application throughout the supply chain up to the reporting organization. A common measurement will also support industry efforts in voluntary sharing to increase security across the sector.

Assessment of incidents and vulnerabilities are described separately in this document. However, they are related topics. A threat typically exploits a vulnerability for an incident to occur. Therefore, a vulnerability can be understood as an enabler for an incident to occur.

A common measurement based on predefined decision trees and algorithms can be used to ensure that all organizations report incidents and vulnerabilities using identical or similar parameters that translate to identical values and meanings.

Using appropriate automation and tooling can aid in providing an accelerated triaging process. As a result, the process can comply with a safety occurrence 72-hour window when required by the regulatory authority. The process can provide upper bounds for developing and implementing temporary and permanent solutions for vulnerabilities, including those already exploited within an incident.

Security incidents and vulnerabilities should be initially classified regarding safety impacts. However, when the organization identifies the need, other impact areas such as operation, branding, financial, etc. could be considered.

5.2 Security Event Triage

O5.1: Suspicious security events are analyzed.

All relevant events should be analyzed for the possibility of exposing or discovering a previously unknown vulnerability in the system.

Attributes to include during event analysis should include the nature of the event, the function of the affected assets, their position within the security architecture, and the level of threat

Suspicious security events should be analyzed, classified, and evaluated to determine if they are events that are also incidents. Events are classified as:

- Benign - causing no potential disruption of the system
- Unwanted - in which it could directly or indirectly affect the system function

If the anomaly that called attention to the event can be justified as conforming to the system design and its security policy, and otherwise expected actions, then the event is classified as legitimate, and evaluated to be benign.

If an event is classified as unwanted, the event is then investigated for possible negative effects such as causing a safety effect, a system malfunction, a reduction in system performance, or exposing a previously unknown vulnerability. In each of these cases, the event becomes classified as an incident.

Analysis of detected events is often performed using detection tools that are implemented at various sections and components within the system in question. The tools can indicate the characteristics of the event, enabling further analysis to determine if the event is an incident.

It is possible that detection tools could discover exfiltration / corruption of data that does not apparently affect the system operation.

5.3 Security Incident Analysis

O5.2: The cause and contributing factors that lead to the security incident are evaluated.

O5.3: Relevant connected organizations are informed about security incidents with potential impact on them.

When the Security Incident Response Team (SIRT) believes that an incident has occurred, the team should rapidly perform an initial analysis to determine if it is security related, and if so, whether the incident could impair aviation safety if not corrected or addressed.

This initial analysis should be done as early as possible since it determines priority. In order to perform the initial analysis, it is important to identify impacts, damage, and exploited vulnerabilities, so they can be addressed.

5.3.1 Extent of Incident

The team should identify the boundaries of the incident, such as which networks, systems, or applications are affected and understand how the threat propagates, in order to decide current criticality and risk of further spreading. The initial analysis should provide enough information for the team to classify the incident (covered in section 5.3.4), prioritize subsequent activities, such as containment of the incident and schedule a deeper analysis of the effects of the incident, and how to reproduce the event.

Incidents should first be contained before a damage assessment is done. Once contained, all compromised assets should be identified. This should include an active search for compromised assets and security measures, based on identified indicators (e.g., a malware infection may be detectable through the infected system trying to access certain internet servers).

5.3.2 Gather Incident Facts

The team should have a clear understanding of the objectives and limits of the investigations. In particular, the need to preserve forensic evidence and any restrictions on data access (e.g., from legal or company policy) should be known before the investigation starts.

It may be required to quickly restore systems to ensure safe operations. Incident analysis teams should be aware of such constraints and restoration of safe condition should take precedence over preserving evidence. There is a tradeoff between

operational continuity needed for safety of aviation and forensic evidence. Forensic evidence is secondary to safety. Systems should be designed, where possible, to allow fast restoration while preserving evidence (e.g., have a shadow system that can be switched to while the affected primary system is isolated). It may be possible to swap the equipment to accommodate safe operation and forensic capability.

The investigation team should keep records of all relevant actions, how and from where information or data was received, what analysis has been done and to what results. Conclusions should be distinguished from data analysis results and copies of the original data kept where possible. The investigation team should disconnect the equipment from network (if possible) to avoid propagation but not switch off the equipment as important information about the attack may be present in live memory.

The team could have certain limitations on its ability to access and use certain types of data. These limitations could be the result of legal restrictions (e.g., data privacy considerations) or company policy restrictions. The ISEM policy may describe any data access limitations in place, and any escalation paths available to waive those limitations.

5.3.3 Investigate Log Files

Evidence of an incident may have been captured in several logs where each contain different types of data. A firewall log may have the source IP address that was used, whereas an application log may contain a username. A network intrusion detection system may detect that an attack was launched against a specific host, but it may not know if the attack was successful. The team may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable for deeper investigation. This will likely be difficult for embedded systems, so this is where preplanning can help identify the tools and processes that would be used for collecting and reviewing event logs if available when an incident occurs. In planning for log file investigation, it is necessary to investigate the required tools and resources, to analyze and investigate all relevant security log file data, and to include tools and resources along with guidance and objectives. (See section 3.7)

If it is determined that the security log file mechanism does not provide enough information to correlate with an event or explain the cause of an event within a system, the OEM should be informed so that improvements can be made to the log file function of the system.

5.3.4 Assess Security Incident

O5.4: The vulnerabilities exploited in an incident are identified when possible.

O5.5: The actual damage and the damage potential from the security incident are evaluated.

O5.6: The criticality for aviation safety of security incidents is assessed.

The criticality of a security incident should be based on the potential damage of the incident. In addition to the actual damage, organizations should also assess the damage the incident could have caused under adverse circumstances (worst case analysis) in order to reflect the damage potential.

An incident also exposes vulnerabilities that have been exploited to cause the incident. During the incident analysis these vulnerabilities should be identified and assessed according to the vulnerability assessment method. This could lead to reportable vulnerabilities independent of the incident under analysis.

The following factors should be considered when assessing an incident:

- Confirmed impact caused by the incident
- Potential but unconfirmed impact caused by the incident
- Potential future impact if the incident is not contained and corrected
- Potential maximum impact the attacker could have caused

The last 3 bullets are examples of exposed vulnerabilities where no actual impact occurred or not fully realized. These are evaluated for potential safety effects.

Incident damage classification is based on safety damage (actual and potential) at minimum. Impacts on assets used as security measures should be expressed in terms of the safety impact potential for the assets they protect.

From the list of compromised assets and security measures, a list of all assets exposed to the incident should be generated. Exposed assets and security measures are all those assets that the incident could have impacted under adverse conditions, regardless of whether for the actual incident, any impact was verified. The identification of exposed asset should consider connectivity and dependencies between assets, and the attack paths identified in security risk assessments. If a security measure exists between the compromised asset and another asset and this security measure would have blocked (or has blocked) further spreading of the incident, then this other asset is considered not exposed.

All exposed assets should be evaluated to verify their correct configuration and function.

With view of safety occurrence reporting requirements, the security incident reporting criteria need to be consistent. Considerations about incident reporting is provided in section 6.4. Different cases can be distinguished:

Incidents on airborne systems

- Incidents that could lead to an unsafe condition should be reported as a threat condition
- Incidents on airborne security measures should be reported if the remaining security measures are insufficient to mitigate the risk for an unsafe condition to an acceptable level.

Incidents on ground assets with direct safety impact

- Incidents on ground systems and associated processes that directly contribute to aviation safety should be reported if the incident could lead to an unsafe condition. This includes ground-based installations required for the safe operation of flights, like radar, takeoff and landing aids, radio communication, navigation & weather data, etc. They may affect flight safety directly or indirectly.

Incidents on GSE and aircraft connected assets

- Incidents on Ground Support Equipment should be reported if the incident could lead to an unsafe condition.
- Incidents on IT Systems exchanging data with airborne systems should be reported, if there is no security measure between the affected system and the airborne system, and the incident could lead to an unsafe condition. This applies to data connections via trusted interfaces or where the ground system is a trusted endpoint, or subject to a security related ICA issued by the DAH. It also applies to connections to airborne systems that were not designed to protect against compromised or malicious activity, except if a prior agreement for acceptability of this risk has been concluded between the DAH and the Authority justifying no reporting obligations. A security measure often used may be PKI infrastructure the enables adequate encryption and non-repudiation to ensure secure data exchange. If the security measure is impacted or compromised, then it should be reported as part of an incident. This includes ground-based installations required for the safe operation of flights, like radar, takeoff and landing aids, radio communication, navigation & weather data, etc. They may affect flight safety directly or indirectly. If the security measure between the connected system and the aircraft is impacted within the incident, then information regarding the compromised security measure should be included in the incident report
- Incidents affecting procedures, documents, data, or other assets used to maintain or service the aircraft should be reported, if these assets would be considered trusted by an operator and could cause an unsafe condition. This requires the asset to be actually compromised, not just exposed to the incident. It does not apply to assets that are subject to integrity validation before use, e.g., digitally signed data loads.

Incidents on assets with potential indirect safety impact

- Incidents on assets that could lead to an unsafe condition only under adverse conditions, e.g., if the incident is not detected or other security measures fail, should be reported, if there is an indication that the attack targeted aviation safety. This applies to all assets where a threat scenario with safety consequence exists but would need a sophisticated and targeted attack to materialize. For example,

the compromise of a PC where the user has write access to Design Data, Field Loadable Software (FLS) loads, Maintenance Procedures or other assets that could lead to a safety impact, is only reportable if investigation reveals that the attacker tried to or actually manipulated those assets. Write access means that the associated files are not protected from being changed by anyone who has login access to the PC or asset. Note that in such case, the integrity and validity of exposed assets should still be verified, but the incident should only be reported to relevant authorities if one of the exposed assets was found compromised, or other indications exist that the incident was targeting aviation safety. If the attack accessed or compromised an asset but did not perform any actions that indicate a targeted attack, then a potential to perform an attack was demonstrated, which may be a vulnerability with potential safety impact. See section 5.4.

- Detection of multiple untargeted attempts to access an asset should be analyzed to see if security measures are in place and sufficient to avoid unauthorized access. A high number of attempts could be classified as an incident on an asset.
- Incidents on industrial assets ensuring or supporting the production of an aircraft.

5.4 Vulnerability analysis

5.4.1 Introduction

O5.7: All assets affected by a vulnerability are identified.

O5.8: Risks for aviation safety from exploiting a vulnerability are assessed according to the Vulnerability Management Strategy for the asset.

O5.9: Relevant connected organizations are informed about vulnerabilities with potential impact on them according to the Vulnerability Management Strategy for the asset.

Vulnerabilities can appear in any software, hardware or system and be derived from weaknesses in software coding or hardware design, architecture, or even can be derived from non-technical areas (processes and organizations). Exploitability of vulnerabilities is dependent on installation and use; vulnerabilities in software that is reused in multiple products may have different exploitability and impacts associated with each case. Vulnerabilities can exist in all aviation systems and processes, including ground systems, ground industrial development and manufacturing systems, and aircraft systems. Nevertheless, their exploitability should be assessed.

There is an increasing trend for using software or hardware from products developed in other industries in aviation products, and reuse of aviation products across different aircraft. The same software or hardware may also be used within multiple parts of the aviation ecosystem, such as in on-aircraft and ground support equipment.

This generates a challenge in identifying vulnerabilities, assessing impacts in each use case, and communicating to necessary stakeholders. Also, it is possible that no stakeholder has the complete picture necessary to independently perform an assessment.

For example, a ground support equipment supplier might not have a clear concept or understanding of how vulnerabilities may exist in their product, and the exploitability of the vulnerability, when used for a safety critical aviation system.

For aircraft, the top tiers in the supply chain, e.g., the approved organizations and/or Design Approval Holders, will have an understanding of the overall architecture and operational use but will not have details of specific implementation of software and hardware where a vulnerability is found. Likewise, the lower tier suppliers responsible for the affected software or hardware could either be commodity vendors not involved in aviation or could only have visibility of their direct design. The lower tier suppliers can provide information about the impact of the vulnerability in their domain but might not understand the impact on the overall system or system of systems.

Vulnerability analysis can be split into 3 main steps:

1. Triage (section 5.4.3), to perform an initial first look at a vulnerability and quickly evaluate the assets effected, the vulnerability severity, and prioritize accordingly. For some assets, per their vulnerability management plan, no action may be necessary. For example, the plan may permit periodic patching according to

vendor assessed risk and additional action is necessary only if the vulnerability cannot be patched within the defined timescales or exceeds a defined risk threshold.

2. Risk assessment (section 5.4.4), to perform a deeper investigation of the vulnerability, as needed, to refine understanding of severity for each impacted asset and to determine if the vulnerability poses an unacceptable risk for an unsafe condition.
3. Reporting (section 5.4.5), to provide awareness to stakeholders of vulnerabilities that pose an unacceptable risk for an unsafe condition.

Subsequent response and recovery actions are detailed in CHAPTER 6 and CHAPTER 7 respectively.

5.4.2 Vulnerability Scoring

Per section 3.4.2.4, security vulnerabilities should be associated with a quantitative or qualitative means to identify the criticality of the vulnerability in relation to its impact and ease of exploitation, and ultimately reflect its severity to aviation safety.

The Common Vulnerability Scoring System (CVSS) from https://www.first.org/ provides an open framework and method to capture vulnerability characteristics and produce a score to reflect severity. Most databases of publicly known vulnerabilities, such as https://nvd.nist.gov/, utilize the CVSS for their criticality assessment and scoring. CVSS supports severity score calculation with or without publicly disclosing the vulnerability. Using CVSS can facilitate compatibility and allow comparisons with other publicly disclosed and non-publicly disclosed vulnerabilities. This also allows triaging and prioritizing of vulnerabilities.

Note that the CVSS scores generally provided in public databases typically assume the vulnerable component is included in a piece of IT equipment that has ubiquitous internet access. The aviation safety criticality of an asset is also not considered. Tuning of the vulnerability characteristics, as supported by the CVSS tooling, is therefore necessary to better represent the specific asset type, design, connectivity, and operational environment. For example, the severity of a vulnerability in a software component used in a safety-critical embedded on-aircraft asset with no external access will likely have a different severity compared to the same software component when used in an internet-facing IT web server. To support application of CVSS in an aviation environment, Appendix C includes aviation-tailored guidance for temporal and environmental metrics for typical Aviation asset types. The base group metrics from CVSS are universally applicable.

5.4.3 Vulnerability Triage

A vulnerability should be triaged for each asset and security measure according to the rules defined in the vulnerability management strategy of the affected asset. The first step of the analysis should evaluate whether the asset or security measure is affected.

The following factors should be considered for a first triage:

- Can the vulnerability be exploited for the specific asset's configuration? (applicability)
- What is the threat level exposure of the vulnerability in the system's context? (exposure)
- What is the impact of an exploit on the affected system? (threat condition)

Vulnerabilities that are applicable to a system, exposed, and could impact a required security property (e.g., CIA triad), should be further assessed for their criticality.

In order to get an indicator of the severity of a vulnerability for a given asset (or collection thereof), organizations should use a scoring method based on characteristics of the vulnerability (base score), the exploit situation (temporal score) and the criticality of the affected asset (environmental score). The resulting vulnerability score will help organizations to prioritize vulnerability analysis and define acceptable response times. See section 5.4.2 for further details on scoring.

Many ground systems take part in patch management, which regularly or on demand deploys system updates. Patch management will typically deploy, after a technical validation, all vendor recommended patches, regardless of the criticality of the individual

patches for the organization. For such systems, no deep analysis of vulnerabilities is required, provided a patch is available and can be deployed in acceptable time. Patch management should include the validation that the patch effectively mitigates the vulnerability and the verification that the patch was successfully deployed on all vulnerable assets. Perform regression test to ensure the patch retains the required functionality and doesn't negatively impact performance.

If no patch is available, the vulnerable system cannot be patched or patch deployment would take too long with respect to the criticality of the vulnerability, organizations should perform a deeper analysis of the risks imposed by a vulnerability.

The following factors should be considered for a deeper analysis:

- How complex is an exploit, is exploit code available? (exploitability)
- How likely is an attack on this attack path? (likelihood)
- What existing security measures could prevent an attack?
- What is the maximum safety impact resulting from an attack? (e.g., consequence, severity)
- What existing security measures could prevent or mitigate the consequences?

See section 5.4.4 for further details on vulnerability analysis.

The vulnerability assessment strategy may be different for groups of assets and should be defined in the enrollment dossier.

5.4.4 Vulnerability Risk Assessment

The risk induced by a vulnerability depends not only on the characteristics of the vulnerability, but also on the function and position of the affected asset in the security architecture, other known vulnerabilities that could be used in combination, and the criticality of the overall threat scenario that an attack could trigger. In order to gain a full understanding of the risk, the level of threat resulting from the attack paths needs to be assessed.

The risk assessment related to a new vulnerability depends on available previous risk assessments for the area, as it would not be feasible to perform a new risk assessment for each new vulnerability. However, if security risk assessments exist that identify the attack paths and the contribution of individual security measures along the paths, the overall risk should be re-calculated, taking into account the reduced contribution of security measures affected by a vulnerability. This action provides a more accurate risk assessment as well as keeping the risk assessment up to date.

This process will require the resulting risk for the relevant threat scenarios for the vulnerability of concern to be re-assessed. The assessment should include all known and unmitigated vulnerabilities along the attack path, as an attacker could also exploit several vulnerabilities along the path to cause the maximum effect.

For each security measure, the effective security contribution should be evaluated and the resulting overall risk re-calculated. This calculation should consider the exposure of the affected asset, the complexity of vulnerability exploitation, the potential impacts on the vulnerable assets, and the potential safety consequences resulting from such impacts. The calculation should further take into account other known vulnerabilities on the threat path.

Vulnerability Risk Assessment for legacy aircraft is focused primarily on Software Data Loading, and Software Distribution. The main assets at risk are the Data Loader itself and the information systems that transfer software to the data loading equipment, including the transport security methods (e.g., PKI). These are generally protected by Digital Signature technology methods using PKI infrastructures. Any compromise of these software transfer methods could put all aircraft software at risk.

5.4.5 Vulnerability Reporting Thresholds

O5.10: Vulnerabilities are reported in accordance with defined reportability thresholds.

Like the security incident reporting process, vulnerability reporting thresholds need to be consistent. For that reason, all vulnerabilities imposing an unacceptable risk for an unsafe condition should be reported.

Depending on the area affected by the vulnerability, risk acceptance criteria may have already been established and agreed with the relevant authorities. If this is the case, the overall risk should be assessed following the agreed method, risk grid and reporting criteria.

If the vulnerability is in an area where no security risk assessments are available or no reporting obligations have been agreed with relevant authorities, the organization affected by the vulnerability should define and document the vulnerability assessment strategy (scoring and/or risk assessment) and use TABLE 5-1 to determine when to report. Organizations using a method with different scales should define and document a translation between their scale and the risk scales provided.

Organizations may use level of threat definitions that are in standards for aircraft (ED-203A/DO-356A) and ATM (ED-205A/DO-393) as reference to establish level of threat criteria. CVSS may also be used. Both are provided in TABLE 5-1.

Note that publicly available and vendor provided vulnerability severity scores are generally not tailored for specific assets and the implementation of security measures. These could lead to unnecessary reporting. For example, the positioning of security measures will not be considered for a particular asset by the base raw CVSS score. If the asset risk assessment (per section 3.3) demonstrates that the overall risk of the vulnerability is not reportable, this may override the CVSS score which otherwise would have resulted in the need to report. For example, the risk assessment may demonstrate there are sufficient remaining security measures on the attack paths by which the vulnerability could be exploited, and therefore the overall risk remains below the reportability threshold. The vulnerability management plan for the asset may already identify that no reporting or further vulnerability risk assessment (as detailed in section 5.4.4) is necessary. Additionally, the vulnerability plan may also identify permitted timescales for periodic patching of vulnerabilities (such as in IT environments), with reporting and vulnerability risk assessment necessary only if those timescales cannot be met or the vulnerability exceeds a defined risk threshold.

TABLE 5-1 REPORTABILITY THRESHOLDS

*Select based on vulnerability assessment methodology***		**Potential Safety Impact of vulnerability***				
Level of Threat (likelihood of safety impact)	**Final aviation adapted CVSS Score*** **	**No Effect**	**Minor**	**Major**	**Hazardous**	**Catastro-phic**
Very High	9.0 – 10.0	Not Reportable	Not Reportable	Reportable / Not Reportable*	Reportable	Reportable
High	8.0 – 8.9	Not Reportable	Not Reportable	Not Reportable	Reportable	Reportable
Moderate	6.0 – 7.9	Not Reportable	Not Reportable	Not Reportable	Reportable	Reportable
Low	3.5 – 5.9	Not Reportable	Not Reportable	Not Reportable	Not Reportable	Reportable
Extremely Low	0.0 – 3.4	Not Reportable	Not Reportable	Not Reportable	Not Reportable	Not Reportable

NOTES:

* *There may be cases where events can be considered as an unsafe condition such as more than one Major or if they occur too frequently (significantly beyond the applicable safety objectives) and could eventually lead to HAZ, even CAT, consequences in specific operating environments.*

** *Definition of criticality levels is up to each organization. Sections 5.3.4, 5.4.3 and 5.4.4 provide additional guidance. Organizations using a method with a different scale should define and document the way to translate risk scales into this table.*

*** *See Appendix C*

5.5 Analysis Time and Emergency Measures

O5.11: Security incident and vulnerabilities are treated within the defined maximum acceptable lead times.

Information recorded in the event log database should be regularly reviewed and updated during the investigation with all facts and evidence.

Acceptable time frames for analysis of an incident or vulnerability depend on the criticality of the event, but also on the availability of relevant information and the complexity of the analysis to be performed. Log files may have to be retrieved using specific procedures or specialist support may be needed for the analysis. Furthermore, depending on the detection capabilities, there is a delay between the time the event occurred, the time it was detected, and the time analysis starts. It is therefore not possible to define a common time frame for event analysis.

On the other hand, event analysis should be eventually conclusive and not delay in taking the necessary actions. Emergency measures and initial reporting may start before the analysis is completed, based on the best information available at the time.

If an analysis of the event indicates that an unsafe condition is likely, emergency or crisis plans as per the organization's enrollment dossier should be invoked.

An accepted guideline for environments where security log information is readily available, is to ensure the incident and vulnerability response process is triggered no later than 30 days after an event occurs. Different timeframes may be used if the

operational environment of an asset limits the availability of logs. Asset manufactures can also provide guidance on selection of this timeframe.

Organizations should define the steps and means of analysis for each asset and document e.g., in the enrollment dossier (see section 3.4.2.3). This should include criteria to invoke emergency or crisis plans early in the analysis, the standard analysis procedures and timeframe for the asset, supporting means for an extended analysis, and reporting frequency and stakeholders to be informed.

For incidents, the analysis should first focus on identifying the threat and its propagation and decide about the need for containment or other emergency measures to be invoked.

For vulnerabilities, the analysis may utilize threat intelligence to identify if an imminent threat exists and decide about the need for emergency measures, e.g., taking vulnerable assets off-line. Organizations may further use a scoring method to quickly rate the criticality of a vulnerability.

CHAPTER 6

RESPOND

6.1 GENERAL

The process of information security incident response involves the prioritization, containment, tracking and reporting, reviewing lessons learned, and the management of the event information. For vulnerability response, mitigating measures can reduce or prevent the exploitation of a vulnerability and information could be shared with other potentially impacted organizations. The following subsections cover each of these activities.

6.2 PRIORITIZATION

The amount of effort and necessary actions required to recover from an incident determines which possible responses may be taken when handling the incident. An incident or vulnerability that yields high functional impact and requires low effort to recover from is an ideal candidate for immediate action. However, some incidents may not have smooth recovery paths and may need to be queued for a more strategic-level response. The response to each incident should be prioritized based on an estimate of the impact to safety first and the impact on the business second. Refer to section 5.3.4 on scoring an incident and assigning a priority level.

6.3 Containment

O6.1: Security incidents are contained.

O6.2: Applicable response plans for security incidents are activated.

The purpose of the containment plan is to anticipate the occurrence and contain the security incident or improve response time and minimize the impact. Most incidents will require containment. Containment of an incidents' effects and preservation of evidence are important consideration early on during the handling of each incident. Containment prevents further damage and provides time needed for developing a tailored eradication and remediation plan. Thus, the containment actions should include both preventing the attack from spreading and preventing recovered systems from being re-infected. The initial phase of containment is in reaching the decision on how best to contain the incident (e.g., shut down a system, disconnect it from a network, or disable certain functions). A containment plan should be developed in advance that provides predetermined and tested procedures that could be safely followed in a timely manner for known plausible security events. If there are no appropriate existing procedures in the containment plan for a specific security event, it may be possible to adapt one of the existing procedures if it corresponds to a similar type of security event. In other words, having a containment plan developed in advance allows a security event to be contained more efficiently.

The affected system(s) should be isolated as soon as possible to avoid threat propagation on the network. However, another potential issue regarding containment is that some attacks may cause additional damage when they are contained. For example, a compromised host may run a malicious process that pings another host periodically. When the incident handler attempts to contain the incident by disconnecting the compromised host from the network, the subsequent pings will fail. Because of the failure, the malicious process could be designed to overwrite or encrypt all the data on the host's hard drive. Handlers should not assume that just because a host has been disconnected from the network, further damage to the host has now been prevented. Whether a containment plan is developed in advance or not, special care should be exercised to avoid or at least minimize the risk of potential collateral damage that could occur during containment.

Containment actions that are applicable to materialized incidents can be extended to prevent the risk of allowing other vulnerabilities to be exploited when the incident impact is assessed to be significant.

6.4 TRACKING AND REPORTING

O6.3: Reportable security incidents or vulnerabilities are notified to the relevant authorities in accordance with the regulatory lead time

O6.4: Decisions and actions related to a security incident or vulnerability are recorded and traceable.

O6.5: Security incidents and vulnerabilities are reported to the relevant stakeholders.

Relevant stakeholders include the DAH or Authorities.

6.4.1 Notify the Appropriate Individuals

When an incident or a vulnerability is analyzed and prioritized, the security incident response team (SIRT) needs to notify the appropriate individuals so that all who need to be involved can perform their respective roles. Response plans should contain provisions concerning incident or vulnerability reporting that include what needs to be reported and to whom, how soon they should be reported, and at what follow on times should reporting be done (e.g., initial notification, regular status updates). Incident or vulnerability reports should meet applicable reporting regulations and requirements.

6.4.2 Manage Reportable Security Incidents and Vulnerabilities

Organizations should consider which types of technical information should or should not be shared with various parties. For example, external indicators, such as the general characteristics of attacks and the identity of attacking hosts, are usually safe to share with others. However, there could be security and liability reasons why an organization would want to refrain from revealing the details of an exploited vulnerability. The SIRT needs to understand applicable jurisdictions, and which boundaries were crossed as a result of the incident since this will influence which parties need to be notified and what information needs to be shared. For example, the team members responsible for the technical details of the incident may wish to coordinate with their colleagues at partner organizations to share strategies for mitigating an attack that could span multiple organizations. As discussed in the next section, the SIRT may coordinate with its region's aviation information sharing and analysis organization to satisfy mutual self-interest reporting requirements and seek advice or additional resources for successfully responding to the incident.

6.4.2.1 Scope for reportable Security Incidents or Vulnerabilities

Security incidents and vulnerabilities may impact or put at risk other organizations. Therefore, information about the incident or vulnerability needs to be shared in a timely manner in order to allow for a quick response. Also, authorities may require mandatory reporting when an incident or vulnerability imposes a significant safety risk (See Table 5-1, Reportability Thresholds).

Shared information should be verified to be correct and related to actual risks. Sharing of unverified information or information based on insignificant risks could have adverse effects, as it consumes resources and undermines the trust in and importance of the shared information. It is therefore essential that the incident or vulnerability information that is shared with another organization be, as much as possible, correct, complete and relevant.

Any organization that reports a security incident or vulnerability should support applicable authority requests related to the analysis and resolution of the detected problem. This may be a response to information requests that encompasses sharing of analysis means (e.g., components involved in the analysis, test means, etc.).

Authorities can provide more specific definitions of reportable security incidents or vulnerabilities through the dissemination of lists or other published material.

Voluntary reporting is covered in section 6.4.3.

6.4.2.2 Reporting Timeline

Current applicable regulations require that known safety risks to be addressed within specific compliance times. Initial notification is required as soon as the vulnerability has been known to the organization and it is associated with a possible unsafe condition.

As a matter of fact, the FAA considers reporting rules for current occurrences to include security incidents and vulnerabilities. However, security incidents resulting in safety impacts will be reported through different processes that are distinct from existing safety processes.

Security incidents and vulnerabilities are often not easily detectable and need specific means for detection and analysis to verify the finding. Therefore, the initial reporting timeline target is understood as not delaying the reporting AFTER an organization has the knowledge that a reportable security incident or vulnerability occurred and has resulted in, or may result in, an unsafe condition. This should not prevent the organization from proceeding as quickly as possible to investigate and analyze the situation.

Sharing information between organizations does not have specific time constraints, unless mutually agreed upon. But the information should be shared as early as possible to allow other organizations time to investigate on their side. This may include suspicious events or unconfirmed information which should be marked as preliminary with updates provided as soon as available.

For incidents or vulnerabilities initially reported to an aviation authority, a follow-up report should be sent within 30 days of the initial notification in order to describe analysis and mitigations in additional detail.

When investigations have finished and no further updates are expected, a final report should be sent to the applicable authority. The final report submittal timeline can be negotiated with the applicable authorities. Figure 6-1 provides an example of a reporting timeline. Some incidents may need a longer time to be fully resolved.

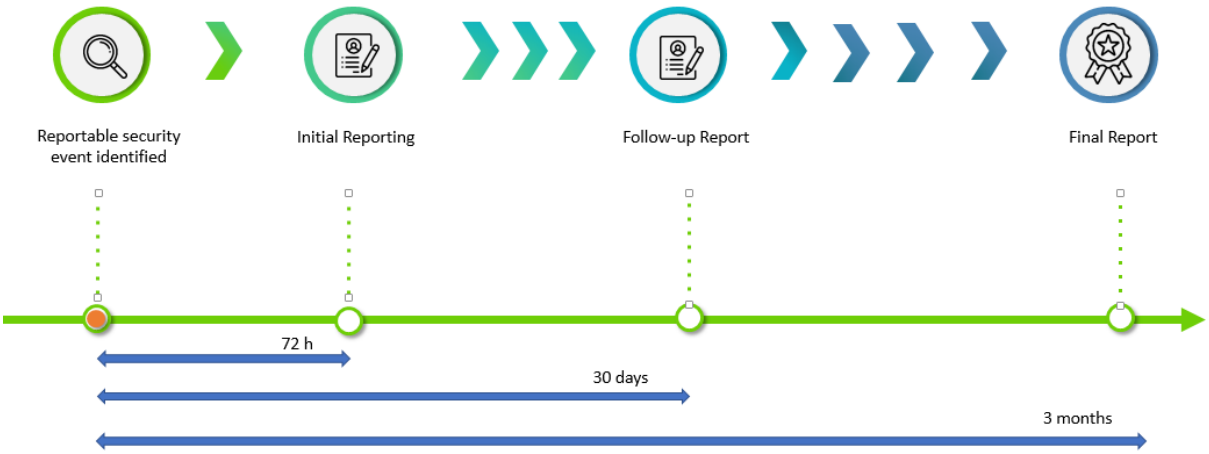

FIGURE 6-1 REPORTING TIMELINE

6.4.3 Voluntary Sharing to the Community

Some issues may need to be shared with the greater industry (beyond a “lessons learned” report), but not until the threat has been successfully mitigated, for fear they would be exploited by bad actors. An organization should establish goals and objectives that describe the desired outcomes of threat information sharing in terms of the organization’s business processes and security policies.
Ideally organizations should share only the necessary information with the appropriate parties to achieve broader cybersecurity situational awareness.
It can be advantageous for an organization to participate in multiple information sharing forums to meet its operational needs. Organizations should consider public and private sharing communities, government repositories, commercial security threat information feeds, and open sources such as public websites, blogs, and data feeds. The organization should identify and participate in those sharing activities that complement its existing threat information capabilities.

There are several security considerations that should be considered when planning information sharing. One is being able to designate who can see which pieces of incident information. The improper disclosure of such information could cause financial loss; violate laws, regulations, and contracts; be cause for legal action; or damage an organization's or individual's reputation. Accordingly, organizations should implement the necessary security and privacy controls and handling procedures to protect this information from unauthorized disclosure or modification.

6.4.4 Report Sequencing

The assessment and reporting activity should be time constrained. In case a complete assessment cannot be achieved in the available time, the reporting should be based on the current knowledge and be marked as preliminary. The assessment may continue after the initial reporting and provide later updates of the results.
The initial report should contain all relevant information related to the detection of the security incidents or vulnerabilities: date, location, system related information (category, serial number, description, etc.), information related to detection (type of operation, phase, detection means, CERT, etc.), information related to security incidents or exploitable vulnerabilities consequences (potential or actual).

The follow-up report should contain the preliminary results of the analysis performed and any preliminary mitigation actions to be taken.

The final report should contain the final assessment, descriptions of mitigations and their implementations, and recommendations for improvements and lessons learned.

6.4.5 Reporting Information Content

The reporting of a vulnerability should include as a minimum:

- Identification of reporting entity
- Unique ID and update sequence number
- Identification of affected components
- Description of vulnerability (include CVE and CVSS score, if available)
- Description of exploitation scenarios
- Description of potential effects of exploitation
- Date and means how the vulnerability was discovered
- Immediate and on-going actions taken to resolve the vulnerability
- An analysis and rating of the effectiveness of any action taken to resolve the vulnerability
- What verifications were performed during the assessment
- A summary of Lessons Learned
- Confidentiality classification (TLP)

Other information that may be relevant:

- Proposals for mitigation and/or correction, e.g.
  - correction of the origin of the vulnerability (e.g., COTS patch),
  - reduction of its exploitability by modifying the asset configuration to add a new security measure,
  - reduction of its impact by modifying the asset configuration to add a new mitigation means. Asset configuration modification only applies to non-certified products (e.g., Ground systems, etc.). For certified products, modifications are only required when applicable.
- Indicators to detect an exploitation
- Instructions how the vulnerability can be reproduced
- Screen captures or other illustrative documents
- Proof of concept code

In case of a security incident, the report should include as a minimum:

- Identification of reporting entity
- Unique ID and update sequence number

- Incident description
- Date, time (UTC) and place where the incident occurred
- Identification of affected components (impact verified)
- Identification of potentially affected components (if investigation is ongoing)
- Impact assessment (actual and potential)
- Date and indicators how the incident was detected
- What verifications were performed regarding received information
- Actions taken by all incident handlers
- Confidentiality classification (TLP)
- Status of incident (new, under analysis, contained, resolved, etc.)

Other information that may be relevant:

- Type of incident (e.g., malicious code, unauthorized access, compromise, DoS)
- Chronology of events
- Operational state of affected components when the incident occurred (e.g., in-flight, on ground, when performing specific tasks)
- Recommended checks in case of potential impacts on assets of other organization
- Next steps to be taken
- References to related incidents
- Chain of custody
- Contact information for involved parties
- List of evidence gathered

To ease information sharing, reports should remain at the lowest possible sensitivity level. Highly sensitive information such as detailed technical information on vulnerabilities and how to exploit them should be put in separate annex documents.

6.5 IMPROVEMENTS AND LESSONS LEARNED

O6.6: Security risk assessments are reviewed based on security events analysis.

O6.7: Lessons learned are captured and processes are improved where needed.

One of the most important parts of incident or vulnerability response is learning and improving. Holding a “lessons learned” meeting with all involved parties after a major incident or vulnerability discovery, and optionally after lesser incident or vulnerability as resources permit, can be extremely helpful in improving security measures and the incident or vulnerability handling process itself. These meetings afford an opportunity to achieve closure with respect to an incident or vulnerability by reviewing and documenting what is learned from what occurred, what was done to intervene, and how well intervention worked. Questions that should be asked and answered include:

Exactly what happened?

- Was there a safety impact? If so, what exactly was the impact to safety?
- How well did the incident response team perform?
- Are there any steps or actions that could be improved?
- Should information sharing be improved?
- What corrective actions can prevent or help mitigate similar incidents in the future?
- Are there any new indicators that should be watched in the future to detect similar incidents?
- Are there any change management steps that should be updated or added (such as checklist updates or process revisions) to help improve incident or vulnerability response performance?

- Should any updates be made to the security risk assessments or containment plan to improve response time and minimize impact if a similar incident occurs in the future?
- Has trend monitoring of the incident repository been performed? Does it include tracking of elements such as:
  - an increasing frequency of a particular type of incident?
  - any new types of incidents, etc.?
- Has trend monitoring detected a potential evolution of the threat level, and indicated what potential improvements should be identified and implemented to address it?

CHAPTER 7

RECOVER

7.1 INTRODUCTION

Recovery is an important element of the overall risk management process life cycle. The capabilities in the Recover function could have effects across a system or network that potentially include impact on safety of flight.

Recovery includes the development and implementation of plans, processes, procedures and training that are flexible and comprehensive enough for the recovery and full restoration of any capabilities or services that are impaired due to an information security incident, in a timely manner. The plans should be used to customize and address the unique type of attacks that an organization's certain technology, processes might be vulnerable to. The recovery plans should help in evaluating potential impact, planned response activities, and resulting recovery processes and procedures long before an actual information security event takes place.

Incident recovery should be managed through a joint effort of all stakeholders to get the affected system back to the defined safe and secure operational state. The SIRT should determine the minimum requirements to enable safe operations. The team could also be able to identify ways in which automation could aid in the recovery. Engaging stakeholders in this activity helps to ensure that recovery participants understand their responsibilities and improve repeatability and consistency of recovery processes. It is recommended that recovery procedures undergo regular periodic dry runs to ensure readiness and suitability.

Training helps exercise both technical and nontechnical aspects of recovery such as personnel considerations, legal concerns, and facility issues. Validating recovery capabilities ensures that the technologies, processes, and people involved in recovery efforts are well prepared, to work together to effectively and efficiently recover operations from disruptive information security events. Recovery activities should be communicated to internal and external stakeholders as well as executive and management teams. Recovery plans and procedures should be protected, due to the sensitive information that would normally be included in such plans.

7.2 Recovery Planning

Organizations need to be prepared to resume normal safe operations in a secure and timely fashion when information security incident occur. All planning and documents relating to information security incident recovery can be included in the organization's existing overall disaster recovery or contingency plan.

Recovery plans and procedures should include specific technical processes that are expected to be used during a recovery and may involve the following:

1. Identification of crisis management and incident management roles and associated personnel.
2. Identification of a minimum list of the assets that enables safe operations, along with all dependencies among these assets. (Understanding recovery objectives relies upon understanding the interdependencies among assets. By understanding how each asset affects the safe operations, the recovery team can prioritize recovery efforts to best optimize resilience.) This list can be created with cooperation of all applicable stakeholders.
3. Development of a procedure for repairing or replacing compromised assets and how to verify proper operation of recovered assets is recommended.
4. Exploring "what if" scenarios, which might be based largely on historic information security events that have negatively affected similar systems.
5. Identification of gaps in recovery process that can be addressed before a potential event, reducing its impact.

6. Communications considerations including identification of alternate communication channels, services, and facilities, should be fully integrated into recovery policies, plans, processes, and procedures.

Procedures should be automated as much as possible in order to reduce errors in a challenging operating environment, which is typical of recovery operations.

7.3 REACT

O7.1: The nominal configuration of assets is restored.

O7.2: Applicable recovery plans (Based on incident type and assets involved) for security incidents are triggered and implemented.

O7.3: Measures are deployed to prevent or mitigate the effects of future security incidents.

O7.4: The effectiveness of actions taken to eradicate an incident or fix a vulnerability is verified**.**

7.3.1 Recovery Action

The recovery action phase is largely achieved through the execution of a recovery playbook planned prior to an incident. While all assets are valuable, they do not all have the same potential impact on safety if they become unavailable or experience reduced capability. The prioritization of functions and assets that need to be recovered to support safe operations is critical and should be identified in the recovery plan. It is recommended to put security measures in place to automatically identify affected systems and alert personnel so that recovery and any other necessary actions can be initiated.

7.3.2 Restoring assets to a safe and secure state

The recovery plan should include processes and procedures that are presented in an actionable manner to effectively restore the essential functions of affected assets quickly and holistically. It should include contingency roles and responsibilities. Information on how to restore and verify that the affected asset is in a safe and secure state, should be made available. Recovery can include specific technical actions such as restoring assets from clean backups, replacing compromised files with clean versions, installing patches, remediating software misconfigurations, securing applications and services, changing passwords, increasing the intensity of monitoring, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control). Restoration activities should be coordinated with internal and external parties as determined necessary.

Recovery restoration activities can have many levels, and while operational status is progressing back to normal, occasionally a step backward will be needed before achieving other steps forward, such as taking a key asset offline to perform recovery measures before conducting recovery actions on other assets. Achieving resilience might mean that an asset can continue operation in a diminished capacity, such as during a denial-of-service attack or a destructive attack on a group of assets. Resilience can also mean containing adversary access or damage to a contained set of resources.

Incident detection and response policies, processes, and procedures should be adjusted to emphasize sufficient root cause determination in an efficient manner. Effective recovery depends on ensuring that all portions of an information security incident are addressed (i.e., detection, analysis, response and recovery) and verified that newly recovered assets are safe, secure and not infected back., so nothing is overlooked.

7.3.3 Restoring aircraft and associated ground services equipment

Once an attack is detected, protection and response processes, including containment, should be deployed to the affected aircraft system and any other interconnected systems, including affected ground services. This is done to minimize the attack’s propagation across the system, and to initiate recovery. Containment can potentially isolate compromised assets from unaffected and recovered assets. Refer to section 6.3 for details on containment activities.

The speed with which this response needs to occur should be set through a risk-based decision-making process that considers the potential negative impact of disrupting safe operations.

Recovery failures may permit portions of a compromise to remain on the aircraft system and associated ground services equipment, causing further damage even without further action from the adversary.

While the search for the root cause may be performed separately, recovery of ground service equipment integrity as well as aircraft systems integrity should be initiated before that cause is determined. The investigation of root cause can be valuable in identifying any previously unknown systemic weaknesses that should be addressed. An example of this is a previously unknown access path to an asset via a system management tool or security scanning service account. The plan should address eventual, full system restoration without deterioration of the original planned and implemented security safeguards.

It is important to emphasize that recovery plans after an attack differ from other recovery plans that are used after a failure or accidental disaster such as fire or flooding. The main reason is that the system recovery of affected or suspicious systems must be conducted in a way that prevents reinfection of newly recovered systems.

If an actual attack affects an aircraft or a ground certified system, the immediate consequence might be the loss of airworthiness. Before returning into service, the application of a recovery plan that is validated by the DAH should be implemented to bring the system back into an airworthy state. For an aircraft that has been certified with security requirements, some relevant recovery procedures may have been delivered by the DAH as part of the Aircraft security Operator guidance. For an aircraft that is certified without security requirements, the operator should not implicitly consider maintenance procedures such as reloading software are sufficient, because they may not have been designed with security in mind. In this situation, the DAH should be involved to help with developing recovery procedures for returning to an airworthy state.

7.3.4 When to fail secure vs. fail safe

If restoration is not possible, the system should be configured to a fail-secure state. However, the fail-secure behavior should not add unnecessary complexity to the security solution as this might decrease the robustness of the solution. More importantly, fail secure should not impact airworthiness.

7.3.5 Timeline to restore

Recovery metrics may help organizations measure and monitor their recovery performance over time. Prioritizing resources by their relative importance to safety objectives is an important driver for determining the sequence and timeline for restoration activities after an information security incident. This prioritization also helps the organization to consider categories of recovery, and to plan appropriate mitigation steps for each category. Understanding recovery safety objectives relies upon understanding the interdependencies among resources. These dependencies need to be considered when setting objectives for recovery time and establishing the sequence for recovering systems. Recovery planning includes the development of processes and procedures that are flexible enough to ensure timely restoration of systems and other assets affected by future information security incidents, and comprehensive enough to have modular components for frequently used procedures.

When affected assets returned to normal operational conditions, and precise monitoring reveals no security symptoms, the recovery can then be considered effective. However, after a potential safety-impact incident, monitoring should be implemented to verify the effectiveness of recovery. The return to a normal state should be confirmed and communicated.

7.4 Changes to the Information Security Management System (ISMS)

Effective recovery will include ongoing use and improvement of both technical and non-technical actions. If there was a safety impact, even if only potential, there should be communication with the safety team and update to SMS. The ISMS should be updated

using lessons learned, providing feedback and lessons learned to update the recovery strategy in the ISMS.

7.5 Recovery Communications

O7.5: Relevant stakeholders are informed about the final resolution of the security incident or vulnerability.

O7.6: Decisions and actions related to a security incident or vulnerability are recorded and traceable.

Planning for and implementing effective recovery communications are critical success factors for achieving resilience. The goal is for recovery activities to be coordinated with internal (e.g., top management, legal and communications departments, Safety Management System (SMS) team) and external stakeholders which can include regulators, customers, suppliers, etc. The recovery team should develop, obtain management approval on, verify, and maintain a comprehensive recovery communications plan. The recovery communications plan should be part of the incident management plan. There could be specific requirements regarding what is released to outside organizations, and the appropriate legal agreements that need to be in place to allow that release of information and ensure continued trust amongst stakeholders. Timing will also be an important factor depending on the impact (e.g., safety impact vs. economic impact).

Key stakeholders need to have sufficient information so that the respective responsibilities are understood during the recovery stage and confidence can be maintained regarding the recovery team's abilities. Planning, and ongoing improvement will help define the appropriate messaging for each type of stakeholder (e.g., external partners, management).

Agreement in advance on which stakeholders will be reporting information to constituents is a critical aspect of the communications plan. There should be a Security Incident Response Team (SIRT) Leader for each incident to act as a first point of contact and oversee recovery activities. For example, the • Security Incident Response Team (SIRT) Leader, or someone appointed by the accountable manager, may fulfill this role depending on the nature of the incident and recovery plan. For these reasons, teams need to plan in advance for recovery communications and ensure that lessons learned from internal and external events are integrated into the improvement processes. Communications considerations should be fully integrated into recovery policies, plans, processes, and procedures. The recovery team should consider establishing guidelines regarding what information may and/or should be shared with each type of constituent, and furthermore have the appropriate legal agreements in place to deter and/or prevent unauthorized disclosure of information by those constituents. When updates are delivered to enable decision making, the updates should contain the necessary actionable information that will help the organization more effectively reach the ultimate goal of resuming and maintaining normal operations.

Recovery teams should consider specific types of stakeholders regarding communications planning, including internal personnel and external parties. The organization should ensure that current points of contact for each type of stakeholder are established and maintained to minimize delays during the recovery process. It is important to note that for effective recovery, communications should occur continuously across the tactical and strategic phases.

Some methods of communications may be unavailable (or undesirable) during recovery activities. Recovery teams should be prepared for alternative means of secure and reliable communication and should practice such scenarios as part of ongoing improvement.

In summary, the communication plan has three stages in its lifecycle:

1. **Preparation**: Depending on the incident classification, the communication plan should identify the stakeholders to be engaged, establish the required level of detail for each stakeholder's needs (using a need-to-know principle), indicate the required level of confidentiality detail appropriate for each communication channel, specify message templates to be used, and establish internal and external focal points and time requirements (the speed with which communication

is initiated, and the cadence for updates to be flowed out). The communication plan should be approved by management and agreed upon by external stakeholders. Lastly, the teams need to exercise the communication procedures to ensure readiness when an incident occurs. See FIGURE 7-1 for an illustration of the preparation process.

2. **Execution**: the communication plan procedures are executed and records are generated for later analysis. When an incident occurs, the Response Team will execute the communication plan, notify management, and when required by the plan, issue a message to interested stakeholders. To issue the message it is necessary to use the template defined in the plan, classify the message according to the plan, and send the message thru the channels defined in the plan. All the actions taken need to be logged for further analysis and improvement of the plan. See FIGURE 7-2 for an illustration of the execution process.
3. **Post-Incident**: the communication plan records are analyzed to correct flaws and identify improvements. The "Response Team" reviews the execution log to identify gaps in the information provided by the "Risk Assessment Team" and fill in these gaps to improve the risk assessment process. The "Response Team" also identifies opportunities for improvement of the communication plan. After all the analyses are completed, it is necessary to brief management and interested stakeholders. See FIGURE 7-3 for an illustration of the Post-Incident process.

***NOTE**: If needed, more information about the communication plan can be in found in ISO/IEC 27003:2017.*

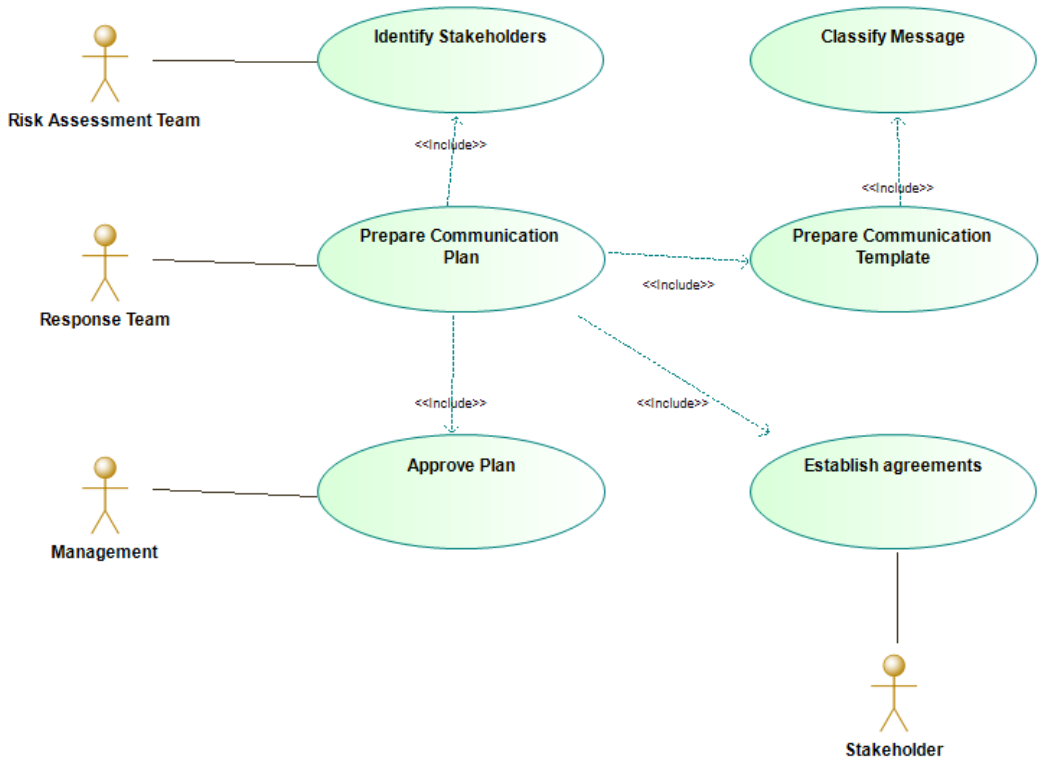

FIGURE 7-1: PREPARATION

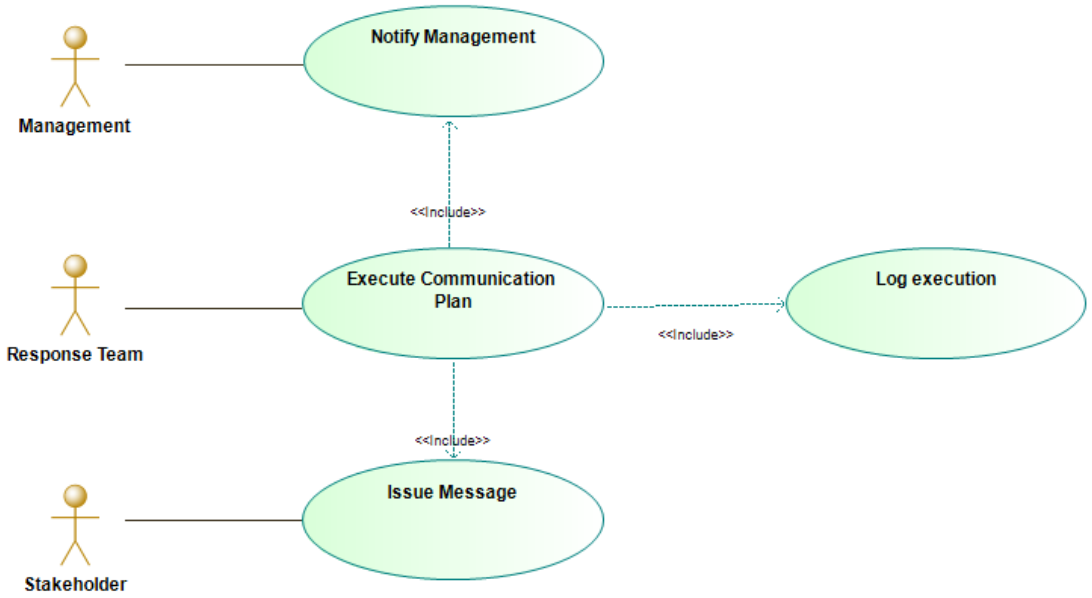

FIGURE 7-2: EXECUTION

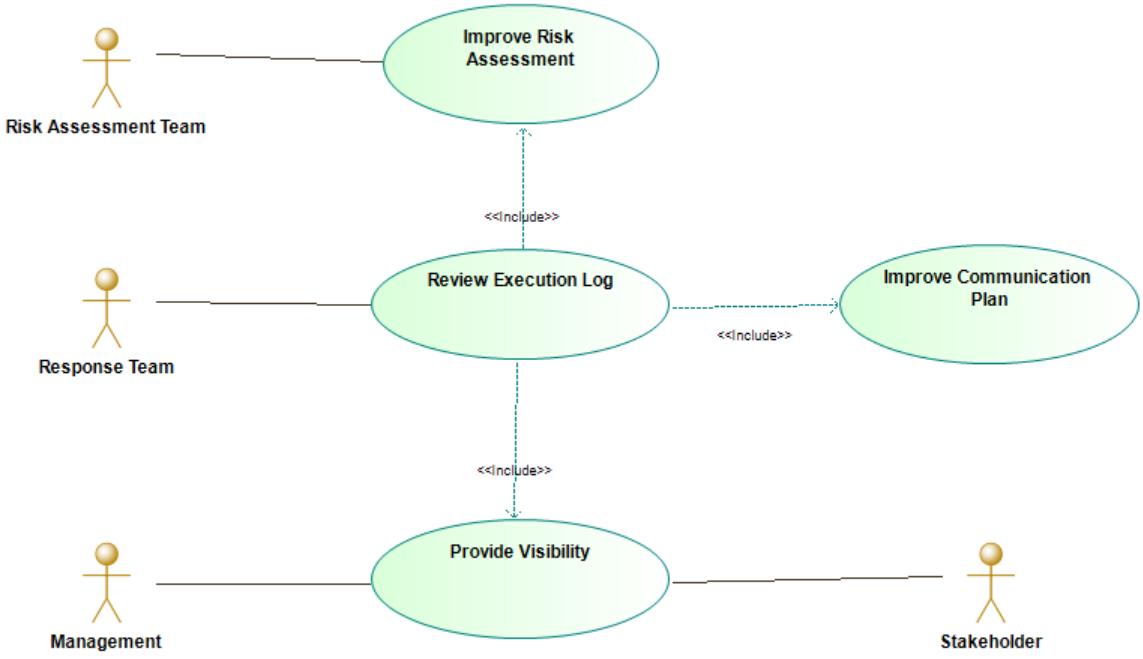

FIGURE 7-3: POST-INCIDENT

APPENDIX A

ISEM OBJECTIVES

(Normative)

The tables in this Appendix list ED-206 / DO-392 objectives.
Description of the tables in this Appendix:

Objectives

This column lists the objectives associated to the process.

ISEM Framework

Ref	Objectives
Documentation and Record Keeping Objectives	
O2.1	Security risk assessments along with the residual risk acceptance are archived.
O2.2	Relevant security incident data and analysis results are archived.
O2.3	Relevant vulnerability data and assessment results are archived.
O2.4	Relevant security event data is retained according to the risk-based retention plan.

ISEM Preparation

Ref	Objectives
Information Security Event Management Policy (ISEM)	
O3.1	The ISEM scope, objectives, organization and processes are defined.
Information Security Organization Objectives	
O3.2	The processes for information security event detection, analysis, response and recovery are established and managed.
O3.3	The methods and tools for information security event detection, analysis, response and recovery are defined and deployed, including: **a)** Asset inventories and associated technical documentation, **b)** Risk assessment method, **c)** Security event sources, collection and screening methods and tools, **d)** Information sources and assessment methods for investigation, **e)** Response plans, **f)** Recovery plans, **g)** Lessons learned capture and continuous improvement.
Information Security Risk Management Objectives	
O3.4	Assets are identified.
O3.5	Interfaces with connected organizations are identified.
O3.6	Threat scenarios for risks to aviation safety are identified.
O3.7	Information Security risks for aviation safety are identified.
O3.8	Event detectors are in place to detect security events related to the identified threat scenarios.

O3.9	The risk assessment criteria allows comparability and compatibility with connected organizations.
O3.10	Maximum acceptable lead times are defined for: **a)** Time between the occurrence and the detection of an event (time to detect) **b)** Time between the detection of an event and the declaration of an incident or vulnerability (time to identify) **c)** Time between the identification of a security incident or vulnerability and the notification to authorities (time to report) **d)** Time between the identification of a security incident or vulnerability and the mitigation of associated risk to an acceptable level (time to fix)
Vulnerability Management Strategy	
O3.11	The plan to detect and respond to vulnerabilities is established for each asset, including: **a)** method and frequency for detecting vulnerabilities is defined **b)** the conditions that trigger an action for the concerned asset **c)** patching criteria and process are established **d)** acceptable lead times for fixing vulnerabilities is defined
O3.12	Organization has means to receive external notifications of vulnerabilities and input these into the vulnerability management program.

Detection

Ref	Objectives
Detection strategy objectives	
O4.1	Security events are collected and screened that indicate deviations from predetermined functional performance baselines.
Vulnerability detection objectives	
O4.2	Vulnerabilities affecting assets are collected and screened according to the vulnerability management plan.
O4.3	Security vulnerabilities that will not be treated according to the vulnerability management plan are identified for further analysis.

Analyses

Ref	Objectives
Security Events Triage Objectives	
O5.1	Suspicious security events are analyzed.
Security Incidents Analysis Objectives	
O5.2	The cause and contributing factors that lead to the security incident are evaluated.
O5.3	Relevant connected organizations are informed about security incidents with potential impact on them.
O5.4	The vulnerabilities exploited in an incident are identified when possible.
O5.5	The actual damage and the damage potential from the security incident are evaluated.
O5.6	The criticality for aviation safety of security incidents is assessed.
Vulnerability Analysis Objectives	

O5.7	All assets affected by a vulnerability are identified.
O5.8	Risks for aviation safety from exploiting a vulnerability are assessed according to the Vulnerability Management Strategy for the asset.
O5.9	Relevant connected organizations are informed about vulnerabilities with potential impact on them according to the Vulnerability Management Strategy for the asset.
Vulnerability Reporting Thresholds Objectives	
O5.10	Vulnerabilities are reported in accordance with defined reportability thresholds.
Analysis Time, Emergency Measures and Record Keeping Objectives	
O5.11	Security incident and vulnerabilities are treated within the defined maximum acceptable lead times.

Respond

Ref	Objectives
Containment Objectives	
O6.1	Security incidents are contained.
O6.2	Applicable response plans for security incidents are activated.
Tracking and Reporting Objectives	
O6.3	Reportable security incidents or vulnerabilities are notified to the relevant authorities in accordance with the regulatory lead time.
O6.4	Decisions and actions related to a security incident or vulnerability are recorded and traceable.
O6.5	Security incidents and vulnerabilities are reported to the relevant stakeholders.
Improvements and Lessons Learned Objectives	
O6.6	Security risk assessments are reviewed based on security events analysis.
O6.7	Lessons learned are captured and processes are improved where needed.

Recover

Ref	Objectives
Reaction Objectives	
O7.1	The nominal configuration of assets is restored.
O7.2	Applicable recovery plans (Based on incident type and assets involved) for security incidents are triggered and implemented.
O7.3	Measures are deployed to prevent or mitigate the effects of future security incidents.
O7.4	The effectiveness of actions taken to eradicate an incident or fix a vulnerability is verified.
Recovery Communications Objectives	
O7.5	Relevant stakeholders are informed about the final resolution of the security incident or vulnerability.
O7.6	Decisions and actions related to a security incident or vulnerability are recorded and traceable.

APPENDIX B

VULNERABILITY MANAGEMENT STRATEGY EXAMPLES

(Informative)

Example 1: for widely used COTS on an IT ground system a vulnerability management strategy could be:

- Periodic treatment: every X month (X being consistent with the lifecycle constraints of the asset):
  - identify all known vulnerabilities known at X – 2 months (2 months being the delay to perform all the following actions)
  - don't perform any impact assessment
  - identify all corresponding patches
  - perform non regression tests at a given deepness suitable for the type of component (e.g., simple tests for a Windows patch, full functional tests for a patch on a critical component used to implement the main function of the asset, …).
  - Implement and deploy patches using standard configuration / change management processes.
- On-event treatment 1: in case of an alert from national security agency for a specific CVE, perform out of cycle treatment:
  - impact assessment using vulnerability analysis method as described in the section 5.4
  - Given the impact assessment, develop and deploy a workaround

  When a patch is available, perform non-regression tests at a given deepness suitable for the type of component, then deploy the patch using standard configuration / change management process.

Example 2: for specialized COTS or for a bespoke development vulnerability management strategy could be:

- Periodic treatment: none (rationale could include lack of publicly known CVEs or similar situation due to the unique nature of the product)
- On-event treatment 1: same as in previous example (patches should be addressed if they become available).

Example 3: for an obsolete component (alternate example)

- Periodic treatment: none
- On event treatment 1: in case of an alert from national security agency for a specific CVE:
  - impact assessment using vulnerability analysis method as described in the section 5.4
- Given the impact assessment, develop and deploy a workaround and / or precautionary measures

APPENDIX C

GUIDANCE FOR CVSS SCORING

(Informative)

C.1 Introduction

The CVSS is used to associate vulnerabilities with a severity metric score. The score is made up of three basic group scores, as is illustrated below in FIGURE C-1.

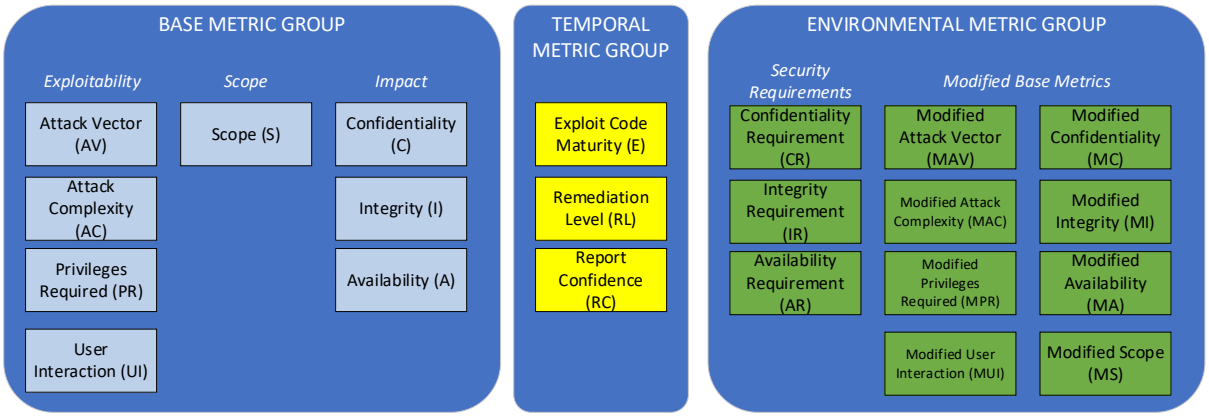

FIGURE C-1 COMMON VULNERABILITY SCORING SYSTEM (CVSS) METRIC GROUPS

The full specification for CVSS v3.1 can be found at https://www.first.org/cvss/v3.1/specification-document and a calculator for determining (or modifying) CVSS scores at https://www.first.org/cvss/calculator/3.1. Many public databases also have a similar calculator that can be used.

The following subsections provide additional aviation-specific guidance for interpreting each CVSS metric for aviation assets and environments.

C.2 Why use scoring

Scoring can provide an objective assessment of vulnerabilities and consistent communication of the risk associated with vulnerabilities. Performing assessments without a scoring mechanism could lead to inconsistent communication of the risk potentially causing differences in understanding the level of risk. With a well-defined scoring mechanism, different aspects of a vulnerability and the impact of proposed mitigations is better understood. Scores also allow vulnerabilities and mitigations to be compared and ranked thus allowing a prioritization of which vulnerabilities need to be addressed. Finally, having an industry agreed scoring mechanism ensures that a level playing field is established and that all approved organizations are held to the same standard whereas differences in measurement and analysis methods would lead to differing security performance.

The use of scoring also provides secondary benefits. With a consistent scoring used across all actors, better support can be established for all stakeholders such as providing databases with common packages scored for vulnerabilities and communicated in the community and tools to assist in scoring vulnerabilities or matching known vulnerabilities to inventories. General vulnerability management can be aided by jointly improving process and process descriptions. The simple scoring mechanism aids rapid impact assessment by all aviation participants. A common scoring scheme also allows better management of suppliers for sharing reporting and remediation responsibilities and simpler integration of inputs from diverse suppliers. Likewise, for

suppliers, a common scoring scheme ensures that suppliers do not have to manage multiple scoring and reporting schemes across product lines.

C.3 Aviation Guidance for Base Metrics selection

The Base Metric Group has three sub-groupings:

1. Exploitability Metrics, which relate to vulnerability and comprises four components: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI)
2. Impact Metrics, which measures the impact of the impacted system against Confidentiality I, Integrity (I) and Availability (A)
3. Scope (S), which is a determination of whether a vulnerability can have an impact to another system or component

The base group produces a score ranging from 0 to 10 which can then be modified by scoring the Temporal and Environmental metric groups. The base group metrics from CVSS are universally applicable and generally require no modification for different asset types.

C.4 Aviation Guidance for Temporal Metrics selection

The Temporal Metric Group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it. The temporal group comprises three metrics concerning:

1. Exploit code maturiI(E) – answers the use and availability of the exploit
2. Remediation Level (RL) – answers the availability and maturity of a patch for fixing the vulnerability
3. Report Confidence (RC) – answers the confidence level that the vulnerability actually exists

The temporal metrics measure the current state of exploit techniques or code availability. Since the change lifecycles of airborne products are typically long, the temporal value should always be assumed to be worst case unless there is valid reason otherwise. Temporal metrics only bring down the CVSS score and therefore should be selected as “Not Defined (X)” for these product types. The score will then be based on the base score and the environmental score only.

C.5 Aviation Guidance for Environmental Metrics selection

The Environmental Metric Group represents the characteristics of a vulnerability that are relevant and unique to a particular user’s environment. Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure. The metrics are modified Base Metrics plus Security environment:

1. Modified Base metrics – Modifies the base metrics to consider the environment for the item and system in question, so can take into account the operating environment, security measures
2. Security environment – provides an indication of the criticality of an asset in terms of Confidentiality, Integrity and Availability

This guidance can be used to set the environmental metrics of a CVE to calculate a more realistic aviation related CVSS score. Many of these values can be calculated in advance and automatically applied to any new CVEs that apply to a specific asset. If the guidance does not cover the specific asset type, use the general concepts described and work with your certifying authority to determine an acceptable methodology for that asset. The guidance provided consists of examples only and does not attempt to cover every possibility or type of asset.

The values used here would be for initial triage and determination of urgency to analyze (see section 5.4.3). Further risk assessment of the vulnerability (see section 5.4.4) could lead to changing of the environmental values based on the results of the analysis and

that would yield the final CVSS score for that specific product and installation. The final CVSS value would be used to determine if reporting is required per TABLE 5-1.

Note: If the aviation guidance leads to a “reduce to” action, review the guidance for that new level to determine if there should be any further reduction.

C.5.1 Security Requirements

The security requirements are set based on the Design Assurance Level (DAL) and the Security Assurance Level (SAL) of the product and would remain the same even after analysis of the CVE. Organization can supplement the guidance provided for non-airworthiness considerations as appropriate, however a separate score should be maintained for other competing regulations.

Confidentiality Requirement (CR)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.
Low (L)	Loss of Confidentiality is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	Set to Low unless the product has security mitigations that could lose effectiveness due to a confidentiality impact (e.g. password compromise).
Medium (M)	Loss of Confidentiality is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	Set to Low unless the product has security mitigations that could lose effectiveness due to a confidentiality impact (e.g. password compromise).
High (H)	Loss of Confidentiality is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	Set to Low unless the product has security mitigations that could lose effectiveness due to a confidentiality impact (e.g. password compromise).

Integrity Requirement (IR)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.
Low (L)	Loss of Integrity is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	**On Aircraft:** • DAL E • SAL 0 **Off Aircraft:** • Product does not affect the safety of an aircraft
Medium (M)	Loss of Integrity is likely to have a serious adverse effect on the organization or	**On Aircraft:** • DAL C or D • SAL 1

	individuals associated with the organization (e.g., employees, customers).	**Off Aircraft:** • Product indirectly affects the safety of an aircraft (PDLs, EFBs, etc.)
High (H)	Loss of Integrity is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	**On Aircraft:** • DAL A or B • SAL 2 or 3 **Off Aircraft:** • Product directly affects the safety of an aircraft (i.e.: ATM, Aircraft Maintenance, etc.)

Availability Requirement (AR)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score, i.e., it has the same effect on scoring as assigning Medium.
Low (L)	Loss of Availability is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	**On Aircraft:** • DAL E • SAL 0 **Off Aircraft:** • Product does not affect the safety of an aircraft
Medium (M)	Loss of Availability is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	**On Aircraft:** • DAL C or D • SAL 1 **Off Aircraft:** • Product indirectly affects the safety of an aircraft (PDLs, EFBs, etc.)
High (H)	Loss of Availability is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).	**On Aircraft:** • DAL A or B • SAL 2 or 3 **Off Aircraft:** • Product directly affects the safety of an aircraft (i.e.: ATM, Aircraft Maintenance, etc.)

C.5.2 Modified Exploitability Metrics

The Modified Exploitability Metrics are initially set based on the information known during vulnerability triage and are refined as necessary during vulnerability assessment.

Modified Attack Vector (MAV)

Metric Value	Standard Description	Aviation Guidance
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to override the base value with one of the other values and has no impact on the overall CVSS Value.
Network (N)	The vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed below, up to and including the entire Internet. Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet across a wide area network (e.g., CVE-2004-0230).	The vulnerable component is logically accessible by an outsider from the internet, without approvals required. For example: **On Aircraft:** • LRU is on a network accessible from the internet (e.g., Passenger Information and Entertainment Services Domain, other offboard connections such as Satcom, radio, ACARS, etc.) • Accessible to public including accessible via passenger access **Off Aircraft:** • The product is exposed to the internet (i.e.: in a DMZ)
Adjacent (A)	The vulnerable component is bound to the network stack, but the attack is limited at the protocol level to a logically adjacent topology. This can mean an attack must be launched from the same shared physical (e.g., Bluetooth or IEEE 802.11) or logical (e.g., local IP subnet) network, or from within a secure or otherwise limited administrative domain (e.g., MPLS, secure VPN to an administrative network zone). One example of an Adjacent attack would be an aRP (IPv4) or neighbor discovery (IPv6) flood leading to a denial of service on the local LAN segment (e.g., CVE-2013-6014).	The vulnerable component is logically accessible by an outsider, with weak protections/restrictions. For example: **On Aircraft:** • There is an effective, independent separation from the internet (i.e.: logical firewall and avionic specific bus like ARINC-429). **Off Aircraft:** • There is an effective, independent separation from the internet (i.e.: multiple firewalls, air-gapped network).
Local (L)	The vulnerable component is not bound to the network stack and the attacker's path is via read/write/execute capabilities. Either: • the attacker exploits the vulnerability by accessing the target system locally (e.g., keyboard, console), or remotely (e.g., SSH); or • the attacker relies on User Interaction by another person to perform actions required to exploit the vulnerability (e.g., using social engineering techniques to trick a legitimate user into opening a malicious document).	The vulnerability requires an insider with approved access (physical/logical) to the system, with general privileges. For example: **On Aircraft:** • The LRU is dependent upon another LRU or User that is trusted and must be compromised to be successful. This may include discrete signals or serial interfaces with another device in the same control domain. A pilot or user that is trusted to have access to the domain. **Off Aircraft:**

		• The product or service is vulnerable within a local domain
Physical (P)	The attack requires the attacker to physically touch or manipulate the vulnerable component. Physical interaction may be brief (e.g., evil maid attack) or persistent. An example of such an attack is a cold boot attack in which an attacker gains access to disk encryption keys after physically accessing the target system. Other examples include peripheral attacks via FireWire/USB Direct Memory Access (DMA).	The vulnerability requires a trusted insider with approved access (physical), with privileged access (admin, configuration management). For example: **On Aircraft:** • Attack requires physical modification of the system, this includes hardware modification, software loading, LRU installation, wiring modifications and maintenance access. **Off Aircraft:** • Attack requires physical access to modify or access the system. This includes physical access to management consoles, software configuration and replacement of physical components.

Modified Attack Complexity (MAC)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to override the base value with one of the other values, and has no impact on the overall CVSS Value.
Low (L)	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success when attacking the vulnerable component.	The vulnerability can be exploited with basic skills; design information and system vulnerabilities are publicly available; known exploit methods are available. An attack would not be readily detected or prevented, such as via logging or auditing of the system. **On Aircraft:** • Product or LRU is located in a publicly available location (Main cabin, seat back, etc.) and would require basic attacker skills to perform an attack. **Off Aircraft:** • Product or LRU is located in a publicly available location (Ticketing Area, Passenger Terminal Area, etc.) and would require basic attacker skills to perform an attack
High (H)	A successful attack depends on conditions beyond the at'acker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected. For example, a successful attack may depend on an	Exploiting the vulnerability requires a skilled hacker; design information is sensitive and protected; the vulnerability is mitigated from known exploitation. For example: **On Aircraft:** • Requires significant skills to exploit the vulnerability

	attacker overcoming any of the following conditions: • The attacker must gather knowledge about the environment in which the vulnerable target/component exists. For example, a requirement to collect details on target configuration settings, sequence numbers, or shared secrets. • The attacker must prepare the target environment to improve exploit reliability. For example, repeated exploitation to win a race condition, or overcoming advanced exploit mitigation techniques. • The attacker must inject themselves into the logical network path between the target and the resource requested by the victim in order to read and/or modify network communications (e.g., a man in the middle attack).	• Aircraft domain understanding, architecture, wiring, ICD and configuration knowledge is needed • Exploit requires development and implantation of malware into a trusted domain to exploit the system (such as via a supply chain compromise). • Attack requires avoidance of detection, such as by system logging or auditing functions • Product or LRU is located in a restricted area (Cockpit, avionics bay, luggage area, etc.) **Off Aircraft:** • Product or LRU is located in a restricted area (Secured Staff Area, etc.)

Modified Privileges Required (MPR)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to override the base value with one of the other values and has no impact on the overall CVSS Value.
None (N)	The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.	An outsider can carry out the attack without any need for privileged access. No separation of privileges exists.
Low (L)	The attacker requires privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with Low privileges has the ability to access only non-sensitive resources.	The vulnerability requires an insider with approved access (physical/logical) to the system with general privileges. For example: **On Aircraft:** • Exploit requires the attacker to have privileges similar to a general user, such as has access to modify aircraft settings such as flight plans **Off Aircraft:** • Exploit can be performed via user data and files
High (H)	The attacker requires privileges that provide significant (e.g., administrative) control over the vulnerable component allowing access to component-wide settings and files.	The vulnerability requires a trusted insider with approved access (physical/logical), with privileged access (admin, configuration management). For example: **On Aircraft:** • Exploit requires the attacker to have authenticated privileges to modify the

		system, this includes software loading, LRU installation, wiring modifications and maintenance access. This includes supply chain access prior to installation on aircraft. **Off Aircraft**: • Exploit requires the attacker to have admin privileges to modify the system. This includes access to management consoles, software configuration and replacement of physical components.

Modified User Interaction (MUI)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to override the base value with one of the other values and has no impact on the overall CVSS Value.
None (N)	The vulnerable system can be exploited without interaction from any user.	No additional guidance
Reqled (R)	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited. For example, a successful exploit may only be possible during the installation of an application by a system administrator.	The vulnerability requires an insider with approved access (Physical/Logical) to the system, with general privileges. For example: **On Aircraft:** • The vulnerability requires a user with general access to modify the system (including software loading, LRU installation, wiring modifications, maintenance access) in order to enable the attack to be exploited. • Includes user ability to change system w/o specific privileges (e.g. exploit involves influencing approved crew to change a cockpit switch configuration) **Off Aircraft:** • No Additional guidance

C.5.3 Scope

The Modified Scope metric is initially set based on the information known during vulnerability triage and refined as necessary during vulnerability assessment.

Modified Scope (MS)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to override the base value with one of the other values and has no impact on the overall CVSS Value.
langed (C)	An exploited vulnerability can affect resources beyond the security scope managed by the security authority of the vulnerable component. In this case, the vulnerable component and the impacted component are different and managed by different security authorities.	Exploit of the vulnerable component can result in a system vulnerability; leveraging the vulnerability permits compromise of other systems. For example: **On Aircraft:** • The vulnerable component is a Security Measure (SAL 1/2/3) • Exploit of the vulnerable component impacts the delivery of critical data to other aircraft systems • Exploit of the vulnerable component causes an impact to the integrity or availability of other critical aircraft components **Off Aircraft:** • No additional guidance.

C.5.4 Modified Base Impact Metrics

The Modified Base Impact Metrics are initially set based on the information known during vulnerability triage and the DAL/SAL of the asset, however this may be refined as necessary during vulnerability assessment.

Modified Confidentiality Impact (MC)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score
High (H)	There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact. For example, an attacker steals the a'ministrator's password, or private encryption keys of a web server.	See "None (N)"
Low (L)	There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is limited. The information disclosure does not cause a direct, serious loss to the impacted component.	See "None (N)"

None (N)	There is no loss of confidentiality within the impacted component.	Safety Regulatory guidance would be to set to none. Other regulators may require this be higher.

Modified Integrity Impact (MI)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score
High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.	**On Aircraft:** • DAL A or B • SAL 2 or 3 **Off Aircraft:** Product directly affects the safety of an aircraft (i.e.: ATM, Aircraft Maintenance, etc.)
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is limited. The data modification does not have a direct, serious impact on the impacted component.	**On Aircraft:** • DAL C or D • SAL 1 **Off Aircraft:** Product indirectly affects the safety of an aircraft (PDLs, EFBs, etc.)
None (N)	There is no loss of integrity within the impacted component.	**On Aircraft:** • DAL E • SAL 0 **Off Aircraft:** Product does not affect the safety of an aircraft

Modified Availability (MA)

Metric Value	Baseline Description	Aviation Description
Not Defined (X)	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score	Assigning this value indicates there is insufficient information to choose one of the other values, and has no impact on the overall Environmental Score
High (H)	There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained (while the attacker continues to deliver the attack) or persistent (the condition persists even after the attack has completed). Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted component (e.g., the attacker cannot disrupt existing connections, but can prevent new connections; the attacker can repeatedly exploit a vulnerability that, in each instance of a successful attack, leaks a only small amount of memory, but after repeated exploitation causes a service to become completely unavailable).	**On Aircraft:** • DAL A or B • SAL 2 or 3 **Off Aircraft:** Product directly affects the safety of an aircraft (i.e.: ATM, Aircraft Maintenance, etc.)

Low (L)	Performance is reduced or there are interruptions in resource availability. Even if repeated exploitation of the vulnerability is possible, the attacker does not have the ability to completely deny service to legitimate users. The resources in the impacted component are either partially available all of the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.	**On Aircraft:** • DAL C or D • SAL 1 **Off Aircraft:** Product indirectly affects the safety of an aircraft (PDLs, EFBs, etc.)
None (N)	There is no loss of availability within the impacted component.	**On Aircraft:** • DAL E • SAL 0 **Off Aircraft:** Product does not affect the safety of an aircraft

_____

APPENDIX D

GLOSSARY OF TERMS

Term	Definition
Activity	Tasks that provide a means of meeting the objectives. [Source: ED-202]
Airborne Software	Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)) and Hardware Controlled Software (HCS) [Source: ARINC 667-1]
Aircraft	An aircraft is a machine that is able to fly by gaining support from the air, or, in general, the atmosphere of a planet. It counters the force of gravity by using either static lift or by using the dynamic lift of an airfoil, or in a few cases the downward thrust from jet engines. [Source: Wikipedia]
Aircraft component	An aircraft component is a component approved for installation on a type-certificated aircraft.
Aircraft Information Security Center	The Aircraft Information Security Center should act as the operator's point of contact for aircraft information security issues from within and outside the operator's organization.
Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function. [Source: ARP 4754A]
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
Assumptions	Statements, principles, and/or premises offered without proof. [Source: ARP 4754A]
Attack	An assault on system that derives from an act that is an attempt to violate the security policy of a system. This includes intentional and unintentional acts. [Source: adapted from IETF RFC 2828 "attack"]
Availability	Ensuring authorized users have access to information and associated assets when required. [Source: ER-013A, RTCA Paper No. 120-21/PMC-2151, ISO17799]
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [Source: ER-013A, RTCA Paper No. 120-21/PMC-2151, ISO27000, 2012]
Data Distribution	The ground-based process of moving airborne software and data from a source location to a destination location and the process of storing software and data at each location. Examples of source and destination locations are software vaults, airborne software servers, Aircraft on-board mass storage, and OEM software distribution systems. [Source: ED-204]
Data Loading	The process of moving airborne software and data from a storage source into the active executable memory of aircraft systems. Examples of storage sources are aircraft on-board mass storage, Portable Data Loader (PDL) mass storage or media, Aircraft Data Loader (ADL) mass storage or media, and software vault servers. [Source: ED-204]

Design Approval Holder	A design approval holder is the holder of a type certificate, a Parts Manufacturer Approval or a Technical Standard Order authorization or the licensee of a Type Certificate. ***NOTE:*** *References to a type certificate includes supplemental type certificates unless noted otherwise.* All design approval holders must: • Report failures, malfunctions, and defects • Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner • Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order Authorization Holders and Type Certificate Holders [Source: FAA]
Enrollment dossier	The enrollment dossier summarizes all relevant information to maintain security for that asset in its ISMS context.
External Agreement	Assumptions and requirements for the purpose of coordinating roles and responsibilities between dependent systems and external actors. [Source: ED-202]
Field Loadable Software (FLS)	FAA 8110.49 defines Field Loadable Software as follows: Software that can be loaded without removal of the equipment from the installation. FLS can also refer to either executable code or data (see EUROCAE ED-12B / RTCA DO-178B). FLS might also include software loaded into a line replaceable unit at a repair station or shop. [Source: ARINC 667-1]
Ground Support Equipment (GSE)	Refers to Ground Support Equipment that digitally connects to the aircraft at any time during ground or maintenance operations [Source: ED-204]
Information	Information is the (subjective) interpretation of data. [Source: Gollmann, 2005]
Information security	'Information security' means the preservation of confidentiality, integrity and availability of information. [Source: Part IS]
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ***NOTE:*** *The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.* [Source: ISO 27001]
Information Security Event	'Information security event' means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security. [Source: Part IS]
Information Security Incident	'Information security incident' means a single or a series of unwanted or unexpected events having an actual adverse effect on information security. [Source: Part IS]
Integrity	The property of protecting the accuracy and completeness of assets. [Source: ER-013A, RTCA Paper No. 120-21/PMC-2151, ISO27000, 2012]
Level of Protection	Indicator representing the degree of an asset's defense against an attack.

Level of Threat	A qualitative evaluation of the possibility that a Threat Condition might occur. [Source: ED-202A]
Media	Devices or material, which acts as a means of transferring or storage of software (e.g., programmable read-only memory, magnetic tapes or discs). [Source: ARINC 667-1]
Operational Environment	The set of defined concepts of operations, regulations, plans, policies, and procedures of the external organizations and systems that interact with the dependent systems of the aircraft, together with any regulations and policies which apply internally to the aircraft systems themselves. [Source: ED-202]
Operational Security Measures	Security measures that are applied during the operation of the aircraft
Security Event	See Information Security Event definition
Security event screening	The first analysis of events in order to identify suspicious events for further analysis. The purpose of security event screening is to reduce the amount of data to analyze and it is not conclusive with respect to declaring an incident or vulnerability.
Security Incident	See Information Security Incident definition
Security log	A file that is maintained by a system that contains operational security related data.
Security log data	Security related data is the data captured within log files to support the identification and assessment of security events. It includes both security related activities, such as authentications and firewall rejections, and contextual data, such as aircraft and system configuration. The data includes both normal activities and indications of abnormal behavior. It may reside in standard log files or dedicated security log files.
Security Measure	Used to mitigate or control a threat condition. Security measures may be features, functions or procedures, both on-board or off-board. Security measures can be physical, logical or organizational. Similar to security control [Source: ED-202A / DO-326A]
Suspicious security event	A security event identified by event screening for further analysis. Typically, an event that is unexpected or anomalous with an unknown root cause. Suspicious security events may still be legitimate, e.g., caused by maintenance actions or human error, and further analysis is needed in order to verify a security incident or vulnerability.
Vulnerability Management	Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems however it can also extend to organizational behavior and strategic decision-making processes. Refer also to ISO 27001 / 27002.
Threat	‘Threat’ means a potential violation of information security which exists when there is an entity, circumstance, action or event that could cause harm. [Source: Part IS]

Threat Condition	A condition having an 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 unauthorized electronic interaction, involving cyber threats, considering flight phase and relevant adverse operational or environmental conditions. [Source: ED-203A / DO-356A]
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [Source: ED-202]

APPENDIX E

ACRONYMS

Acronym	Definition
AMOC	Alternative Method of Compliance
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATM	Air Traffic Management
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, and Availability
CNS	Communications, Navigation, and Surveillance
COTS	Commercial Off-The-Shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAH	Design Approval Holder
EASA	European Aviation Safety Agency
EFB	Electronic Flight Bag
FAA	Federal Aviation Administration
FLS	Field Loadable Software
GNSS	Global Navigation Satellite System
GSE	Ground Support Equipment
ICAO	International Civil Aviation Organization
ISAC	Information Sharing and Analysis Center
ISEM	Information Security Event Management
ISMS	Information Security Management System
IT	Information Technology
IUEI	Intentional Unauthorized Electronic Interaction
LoP	Level of Protection
MRO	Maintenance, Repair and Overhaul
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
QRH	Quick Reference Handbook
SMS	Safety Management System
STC	Supplemental Type Certificate
TC	Type Certificate
UAS	Unmanned Aerial Systems
USB	Universal Serial Bus
UTM	Unmanned Traffic Management

VDP	Vulnerability Disclosure Policy

APPENDIX F

REFERENCES

NOTE: *The reader of this document should use the applicable revisions of the documents indicated below.*

Reference	Document
ARINC 667-1	Guidance for the Management of Field Loadable Software
ARINC 811	Commercial Aircraft Information Security Concepts of Operation and Process Framework
ARINC 827	Electronic Distribution of Software By Crate (EDS Crate)
EUROCAE ED-202A RTCA DO-326A	Airworthiness Security Process Specification
EUROCAE ED-203A RTCA DO-356A	Airworthiness Security Methods and Considerations
EUROCAE ED-204A RTCA DO-355A	Information Security Guidance for Continuing Airworthiness
EUROCAE ED-201A RTCA DO-391	Aeronautical Information System Security (AISS) Framework Guidance
EU 748/2012	Part 21, Section A AMC 25.1309 AMC 20-8
14 CFR	Ch 1 Ch. 21.3 AC 21-45 para.5.B Part 121.375 Part 135.415
FAA AC90-113	AC 90-113B - Instrument Flight Procedure Validation (IFPV) of Performance Based Navigation (PBN) Instrument Flight Procedures (IFP)
FAA AC 119-1	Aircraft Network Security Program (ANSP)
ICAO Annex 2	Rules of the Air
ICAO Annex 17	Safeguarding International Civil Aviation Against Acts of Unlawful Interference
NIST SP 800-61	Computer Security Incident Handling Guide
ISO / IEC 27001:2018	Information technology – Security techniques – Information security management systems – Requirements
ISO / IEC 27035:2016	Information Security Incident Management
ISO / IEC 29147:2018	Information technology — Security techniques — Vulnerability disclosure
49 CFR Section 1544	Aircraft Operator Security: Air Carriers and Commercial Operators

APPENDIX G

WG-72 and SC-216 MEMBERSHIP

Chairpersons:

EUROCAE WG-72	Cyrille Rosay	EASA
WG-72 SG-3	Alain Combes	AIRBUS
RTCA SC-216	David Pierce	GE Aviation

Secretaries:

WG-72	Clive Goodchild	BAE Systems
WG-72 SG-3	Frédérique Dauvillaire	Thales Group
SC-216	Sam Masri	Honeywell International, Inc.

Technical Programme Manager

EUROCAE	Anna Guégan

Program Director

RTCA	Karan Hofmann

Document Editors:

WG-72 SG-3	Armelle Gauthe	AIRBUS
WG-72 SG-3	Cristian Bertoldi	AIRBUS
WG-72 SG-3	Felix Meier-Hedde	AIRBUS
SC-216	Ted Patmore	DELTA

US Government Authorized Representative:

RTCA SC-216:	Varun Khanna	Federal Aviation Administration (FAA)

First Name	Last Name	Organisation Name
Pierre	Abdoulhadi	DGAC/DTA/STAC
Bree	Abernathy	Rolls-Royce
Imran	Akhter	NATS
David	Alexander	SAE International
Ken	Alexander	Federal Aviation Administration (FAA)
Michel	Allouche	Michel Allouche
Hannes	Alparslan	European Defence Agency (EDA)
Yohannes	Amare	The Boeing Company
Rosemberg	Andre da Silva	Agência Nacional de Aviação Civil (ANAC-Brazil)
John	Angermayer	The MITRE Corporation
Rafael	Apaza	NASA
Eric	Asselin	Collins Aerospace
Bruno	Ayral	Thales LAS France SAS
Jacques	Baldeck	DASSAULT AVIATION

Sebastien	Barbereau	EUROCONTROL
Maarten	Barendregt	Embraer
Marc	Beaudoin	Department of National Defence (Canada)
Ginette	Bebung	Searidge Technologies
Karim	Benmeziane	Bureau de Normalisation de l'Aéronautique et de l'Espace
Damien	Bertero	Airbus Operations SAS
Benoit	Berthe	ATR
Cristian	Bertoldi	Airbus Operations SAS
Raphael	Blaize	APSYS
Nuria	Blanco	European Commission
György	Blazsovszky	HungaroControl
Timo	Blunck	EUROCONTROL
Andy	Boff	Egis Aviation UK
Jean Philippe	Bonhomme	Nextidee
Beau	Branback	Astronautics Corporation of America
Liz	Brandli	Federal Aviation Administration (FAA)
Jonathan	Branker	Federal Aviation Administration (FAA)
Dr. Agustin	Bravo Del Alamo	Airbus Defence & Space (Spain)
Philippe	Brochain	QFE
Brian	Brown	Federal Express Corporation (A4A)
Angelo	Bruno	LEONARDO SpA
Linda	Brussaard	EASA
William	Bryant	Modern Technology Solutions, Inc.
Jeffrey	Burkey	Federal Aviation Administration (FAA)
Martin	Call	The Boeing Company
Pasquale Junior	Capasso	Università Telematica Giustino Fortunato
Tamara	Casey	Aura Network Systems
Pascal	Chamma	NAVCANADA
Ming	Chen	SZ DJI Technology Co., Ltd.
David	Chen	Federal Aviation Administration (FAA)
Aurel	Chiriac	ROHDE SCHWARZ TOPEX
Renuka	Chitikesi	Honeywell International, Inc.
Stephane	Chopart	Airbus Helicopters
Philip	Church	Egis Aviation UK
Matthew	Clark	Air Line Pilots Association
Andrew	Cocking	NATS
Alain	Combes	Airbus Operations SAS
Ernest	Condon	National Institute for Aviation Research (NIAR) at Wichita State University
Tim	Cooper	IATA
John	Corcoran	Saab
Antonio	Correas	Skymantics
Jakub	Cunat	Egis Aviation UK
Rosemberg	da Silva	ANAC - SAE

Matthew	Dahl	Astronautics Corporation of America
Thomas	Dance	BAE Systems (Operations) Limited
Frederique	Dauvillaire	Thales Group
Aharon	David	A.D.Ventures Software ltd.
Claudio	de Castro	Lilium GmbH
Poliana	de Moraes	EMBRAER
Raymond	DeCerchio	Federal Aviation Administration (FAA)
Stéphane	Deharvengt	DSNA
Philippe	Dejean	SAFRAN
Christine	DeJong Bernat	GAMA
Bertrand	DELERIS	Airbus Operations SAS
Jose	Delgado Tejedor	Indra Sistemas
Ulrich	Dersch	Lucerne University of Applied Sciences and Arts
Gilles	Descargues	Thales Group
Francesco	Di Maio	ENAV SpA
Jakub	Dluhoš	Honeywell International
Ricardo	dos Santos	Embraer
Andrew	Drake	NetJets Inc.
Paul	Dunlap	Airbus
NICOLAS	Durabdeau	EASA
Scott	Edwards	Piper Aircraft
Alexander	Engel	EUROCAE
Kurt	Eschbacher	University of Salzburg
Zhe	Fan	COMAC BASTRI
Manuel	Fernández Montes	Clue Technologies SL
Christian	Fiore	The MITRE Corporation
Ruben	Flohr	SESAR Joint Undertaking
John	Flores	Federal Aviation Administration (FAA)
HOSEMANS	Françoise	Airbus Operations SAS
Vasileios	Friligkos	EUROCONTROL
Anne	FRISCH	DGAC/DTA/STAC
Patricia	Fuilla-Weishaupt	Airbus Operations SAS
Rossella	Gagliardi	LEONARDO SpA
Stephen	Gahn	Rolls-Royce
Marc	Gallant	L3Harris
RAOUFOU	Ganiou	Transport Canada
Eduardo	Garcia	CANSO
Marty	Gasiorowski	Worldwide Certification Services
Manon	Gaudet	IATA
Armelle	Gauthe	Airbus Operations SAS
Birgit	Goelz	DFS Deutsche Flugsicherung GmbH
Cesar	Gomez	Federal Aviation Administration (FAA)
Will	Gonzalez	Federal Aviation Administration (FAA)

Xylene	Gonzalez-Pelayo	Air Line Pilots Association (ALPA)
Clive	Goodchild	BAE Systems (Operations) Limited
Michael	Goodfellow	ICAO
Christopher	Grant	United Technologies Corporation
Judicael	Gros-Desirs	Airbus Operations SAS
Anna	Guegan	EUROCAE
Mark	Gulick	GE Aviation Systems UK
Adrian	Hada	ROHDE SCHWARZ TOPEX
Edward	Hahn	Air Line Pilots Association (ALPA)
Ladislas	Hajnal	ENAC
Erwan	Hamon	Thales LAS France SAS
Jerry	Hancock	INMARSAT
Andreas	Hartl	Telcoadvice consulting services
Christian	Haury	Safran Electronics & Defense
Jens	Hennig	General Aviation Manufacturers Association
Martin	Henzl	Honeywell International
Andrei	Herta	R.A. ROMATSA
Nils	Heuermann	ANSYS
Frédéric	Heurtaux	SAFRAN
Arthur	Hinson	Lockheed Martin Corporation
Karan	Hofmann	RTCA, Inc.
Steven	Hofmann	CCxH, LLC
Michael	Hooper	Iridium Satellite LLC
Marek	Hrubesz	Department of National Defence of Canada
Yaying	Hu	COMAC BASTRI
Roger	Huerlimann	skyguide
Simone	Irti	Thales Group
Graham	Ison	Thales Group
Owen	Jing	Department of National Defence of Canada
Nikita	Johnson	Rolls-Royce
Daniel	Johnson	Honeywell International, Inc.
David	Jones	Astronautics Corporation of America
Theodore	Kalthoff	National Institute for Aviation Research (NIAR) at Wichita State University
Angeliki	Karakoliou	EASA
Hagop	Kazarian	Bombardier Aerospace
Mark	Kelley	AVISTA, Inc
Mehmet	Keyvan	Keyvan Havacilik A.S.
Karim	Khalil	Naviair
Varun	Khanna	Federal Aviation Administration (FAA)
InKyum	Kim	Korea Institute of Aviation Safety Technology
Rainer	Koelle	EUROCONTROL
Andrew	Kornecki	Embry-Riddle Aeronautical University
Miroslav	Krupa	Honeywell International

Jeroen	Kruse	European Cockpit Association (ECA)
Robert	Kuchera	BAE Systems, Inc.
Hans	Kuil	TKH Airport Solutions bv
Renuka	Kurucheti	Honeywell International
Marcus	Labay	Federal Aviation Administration (FAA)
Maurice	LaBonde	Airbus Defence & Space (Spain)
Christopher	Lacey	Airbus Operations SAS
Kristof	Lamont	EUROCONTROL
Adrien	Lapointe	Department of National Defence (Canada)
Richard	Laxton	Vertical Aerospace
Laurent	Leonardon	Collins Aerospace
Jerome	Lephay	Collins Aerospace
JUNDA	LI	Honeywell International
Qi	Li	Department of National Defence (Canada)
Zhao	Liang	Aviation Data Communication Corporation
Juan	Lopez Campos	Indra Sistemas
Félix	Lopez Perez	Hensoldt Sensors GmbH
Marc	Lord	Department of National Defence (Canada)
Luis Manuel	Lozano Ruiz	INECO
Bret	Lynch	Pratt & Whitney
Laurent	Macquet	DSNA
Roman	Madarasz	Frequentis AG
Reza	Madjidi	ConsuNova, Inc.
Tatiana	Maillard	Thales Group
Vaughn	Maiolla	ICAO
Carlos	Marban	DTN
Cyril	Marchand	Thales Group
Kyle	Martin	GAMA
Davide	Martini	EASA
Stephan	Marwedel	Airbus Operations SAS
Sergiu	Marzac	THE BOEING COMPANY
Sam	Masri	Honeywell International
Patrick	McGrath	Irish Aviation Authority
Andrew	McLaughlin	Honeywell International, Inc.
Peter	McNeely	Astronautics Corporation of America
Patrick	McTernen	American Airlines
Kevin	Meier	Cessna Aircraft Company
Felix	Meier Hedde	Airbus Operations SAS
Vincent	Melchor	SAFRAN
Tom	Merrill	Air Line Pilots Association (ALPA)
Stephane	Miglio	Airbus
Hed	Milay	Elbit Systems LTD
Jennifer	Miosi	United Airlines, Inc.
Manfred	Mohr	IATA

Eric	Mok	Universal Avionics Systems Corporation
Dinkar	Mokadam	Association of Flight Attendants - CWA
Rens	Molenaar	Civil Aviation Authority of NZ
Thomas	Monot	Safran Electronics & Defense
Peter	Mooney	Menapia Ltd
Poliana	Moraes	Embraer
Jean-Paul	Moreaux	European Aviation Safety Agency (EASA)
Cecile	Morlec	Airbus
Catherine	Morlet	European Space Agency
Patrick	Morrissey	Collins Aerospace
Joe	Morrissey	The MITRE Corporation
Christian	Motte	AES Aerospace Embedded Solutions GmbH
Marie Chantal	Mouret	Airbus Helicopters
Johnny	Mowry	Textron Aviation
Michal	Mrazek	Honeywell International
Gil	Mulin	Airbus Operations SAS
David	Munoz	Thales Group
Miguel	Muñoz MArtinez	STARTICAL
Alistair	Munro	Alistair MUNRO
Paul	Nelson	NASA
Gerry	Ngu	EASA
Daniel	Nguyen	The Boeing Company
Ravi	Nori	Teledyne Controls LLC
Siobvan	Nyikos	The Boeing Company
Billy	Ogunsola	CAA/SRG
Mika	Okuda	NEC corp.
Michael	Olive	Honeywell International, Inc.
Martin	Pacher	European Cockpit Association (ECA)
Thomas	Parmer	Federal Aviation Administration (FAA)
Jean Michel	Pater	AIR CARAIBES S.A
Ted	Patmore	Delta Air Lines, Inc.
Adam	Patrick	Rolls-Royce
Daniel Patrick	Pereira	Airbus Defence & Space (Spain)
Félix	Pérez	Indra Sistemas
Ric	Peri	Aircraft Electronics Association, Inc.
Mark	Perini	Honeywell International
Mark	Perini	Honeywell International, Inc.
Tom	Phan	Federal Aviation Administration (FAA)
David	Pierce	GE Aviation
Laurent	Plateaux	DGAC/DTA/STAC
Juan	Ponce	Airbus Defence & Space (Spain)
Marc	Poncon	Airbus Helicopters
Jason	Posniak	United Technologies Corporation
Caroline	Prado	The Boeing Company

Stefano	Prola	International Air Transport Association (IATA)
Serkan	Pusat	Keyvan Havacilik A.S.
Mariusz	Pyzynski	IATA
Amanda	Quilici	Elbit Systems
Jeanne	Rabaute	Airbus
Nayyar	Rao	Honeywell International, Inc.
Paul	Ravenhill	Think Research Ltd
Patrick	Redon	Thales LAS France SAS
Kanwal	Reen	Collins Aerospace
Aaron	Renshaw	American Airlines, Inc.
Sebastian	Reschenhofer	EUROCAE
Marty	Reynolds	A4A
Steven	Rines	SAFRAN ENGINEERING
Judith	Ritchie	SAE International
Philippe	Robert	PMV Engineering
Lionel	Robin	SAFRAN
Makrem	Romdhane	INEO ENERGY & SYSTEMS
Marc	Ronell	Federal Aviation Administration (FAA)
Cyrille	Rosay	European Aviation Safety Agency (EASA)
Mickael	Sabelle	Collins Aerospace
Shohreh	Safarian	Federal Aviation Administration (FAA)
Romuald	Salgues	Airbus Operations SAS
Bradley	Sams	Delta System Solutions GmbH
Raul	Sanchez Ramirez	EASA
Jose	Sanchez Redondo	Indra Sistemas
Elda	Scalera	ESG Elektroniksystem- und Logistik-GmbH
Derek	Schatz	THE BOEING COMPANY
Stephan	Schlisske	Rolls-Royce
Michael	Schraub	DFS Deutsche Flugsicherung GmbH
Uwe	Schwark	Airbus
Stefan	Schwindt	GE Aviation Systems UK
Robert	Segers	Federal Aviation Administration (FAA)
Lilian	Segonds	Airbus Operations SAS
Remzi	Seker	Embry-Riddle Aeronautical University
Rebecca	Selzer	United Airlines, Inc.
Valerio	Senni	Collins Aerospace
Joan	Serra	GAMA
Michael	Severson	Bell Helicopter Textron, Inc
Charles	Sheehe	NASA
Matt	Shreeve	Helios - UK
Li	Shunbin	ZTE CORPORATION
Marta	Skomin	Triumph Engine Control Systems
IJsbert	Smant	DTN
Terry	Smart	NAVCANADA

Kris	Smith	Triumph Engine Control Systems
Nicholas	Smith	L3Harris
Patrick	Souchu	DSNA
Leslie	Stair	Crane Aerospace & Electronics
Dan	Stanescu	ROHDE SCHWARZ TOPEX
Garv	Stephenson	Wisk
Seth	Stewart	ENSCO Avionics Inc.
Stefan	Strasser	skyguide
David	Stubbersfield	Skyports
Engin	Sülün	ONUR A.S.
Nicolas	Syssoïeff	Airbus Operations SAS
Adam	Tanverdi	Aura Network Systems
Gilles	Tehel	Airbus Operations SAS
Kimberly	Ten Pas Bell	Federal Aviation Administration
Carlos	Tendero Caulín	Airbus Defence & Space (Spain)
Kimberly	Tenpasbell	Federal Aviation Administration (FAA)
Hugo	Teso	Emirates
Christian	Tettamanti	ACI EUROPE
Lirong	Tian	Aeronautics Computing Technique Research Institute (ACTRI)
Anstey	Tim	THE BOEING COMPANY
Filippo	Tomasello	EuroUSC
Dennis	Tracz	Air Canada
Christophe	Travers	DASSAULT AVIATION
Francois	Triboulet	EASA
Todd	Trncak	American Airlines, Inc.
Mitchell	Trope	Garmin Ltd.
William	Trussell	IFR Development, LLC
Peter	Tsagaris	Transport Canada
George	Tudor	ROHDE SCHWARZ TOPEX
Benjamin	Uceta Gomez	ENAIRE
Yildiz	Uludag	Tubitak Bilgem
Michael	Vanguardia	THE BOEING COMPANY
John	vanHoudt	Federal Aviation Administration (FAA)
Bela	Varkonyi	Frequentis AG
Alexandra	Vasile	Think Research Ltd
Eric	Vautier	ACI EUROPE
Virupaksha	Veranna	Amazilia Aerospace GmbH
Isidore	Venetos	Federal Aviation Administration (FAA)
Herman	Verhoef	IATA
Brian	Verna	Federal Aviation Administration
Ivan	Vincze	HungaroControl
Giulio	Vivaldi	LEONARDO SpA
Anna	von Groote	EUROCAE

Tong	Vu	Federal Aviation Administration (FAA)
Mohammed	Waheed	Aviage Systems
Adrian	Waller	Thales Group
Zhipeng	Wang	Aviation Data Communication Corporation (ADCC)
Philip	Watson	Panasonic Avionics Corporation
Roberto	Weger	SITTI
Matthieu	Willm	DASSAULT AVIATION
Philip	Windust	Federal Aviation Administration (FAA)
Matt	Winslow	Gulfstream Aerospace Corporation
Marcie	Wise	Delta Air Lines, Inc.
Thomas	Wittmann	ESG Elektroniksystem- und Logistik-GmbH
Richard	Wong	Teledyne Controls LLC
Cameron	Wright	Southwest Airlines
Leon	Yang	SZ DJI Technology Co., Ltd.
Donghwan	Yoon	Korea Institute of Aviation Safety Technology
Bryan	Zelley	The MITRE Corporation
Dongsong	Zeng	The MITRE Corporation
Changxiao	Zhao	Civil Aviation University of China

IMPROVEMENT SUGGESTION FORM

Name: _____ Company: _____

Address: _____

City: _____ State, Province: _____

Postal Code, Country: _____ Date: _____

Phone: _____ Fax: _____

Email: _____

Document : ED- / DO- _____ Sec: _____ Page: _____ Line: _____

[ ] Documentation error (Format, punctuation, spelling)
[ ] Content error
[ ] Enhancement or refinement

Rationale (Describe the error or justification for enhancement): _____

_____

_____

Proposed change (Attach marked-up text or proposed rewrite): _____

_____

_____

_____

Please provide any general comments for improvement of this document: _____

_____

_____

_____

Return completed form to:

EUROCAE
Attention: Secretariat General
9 – 23 rue Paul Lafargue
93200 Saint-Denis
France
Email: eurocae@eurocae.net