European Union Aviation Safety Agency

Notice of Proposed Amendment 2023-102

in accordance with Article 6 of MB Decision 01-2022

Development of acceptable means of compliance and guidance material to support the Part-IS regulatory package implementation

RMT.0720 SUBTASK 2

EXECUTIVE SUMMARY

This Notice of Proposed Amendment (NPA) proposes acceptable means of compliance (AMC) and guidance material (GM) to the Part-IS regulatory package (Regulations (EU) 2022/1645 and 2023/203).

The objective of the proposed AMC and GM is to support and facilitate the application of the new Regulations, thereby maintaining a high level of safety and contributing to the protection of the aviation system against information security (cybersecurity) risks.

REGULATION(S) TO BE AMENDED/ISSUED	ED DECISIONS TO BE ISSUED
N/A	ED Decision 2023/NNN/R — AMC & GM to Part-IS
	ED DECISIONS TO BE AMENDED
	ED Decision 2021/002/R— AMC & GM to Part-ARA
	ED Decision 2022/012/R— AMC & GM to Part-ARO
	ED Decision 2022/016/R— AMC & GM to Part-ADR.AR
	ED Decision 2015/015/R — AMC & GM to Part ATCO.AR
	ED Decision 2022/004/R— AMC & GM to Part-ATM/ANS.AR
	ED Decision 2022/017/R— AMC & GM to Part-CAMO
	ED Decision 2022/011/R— AMC & GM to Part-145
	ED Decision 2022/021/R— AMC & GM to Part 21

AFFECTED STAKEHOLDERS

DOA and POA holders, Part-ORO air operators, AeMCs, FSTD operators, U-space service providers and single common information service providers, apron management service providers, AOC holders (CAT), MOs, CAMOs, training organisations, ATM/ANS providers, aerodrome operators, Member States and national competent authorities (NCAs)

WORKING METHOD(S)		
Development	**Impact assessment(s)**	**Consultation**
By EASA with external support	Light	**NPA — Focused** (EASA Advisory Bodies and FAA, TCA, ANAC Brazil, CAA Israel)

Related documents / information

- ToR RMT.0720, issued on 16.1.2019
- Opinion No 03/2021, issued on 11.6.2021

PLANNING MILESTONES: Refer to the latest edition of EPAS Volume II.

Table of contents

1. About this NPA

1.1. How this regulatory material was developed

This rulemaking activity aims at developing AMC and GM to the Part-IS regulatory package (Regulations (EU) 2022/1645[1] and 2023/203[2]).

This rulemaking activity is included in Volume II of the European Plan for Aviation Safety (EPAS) for 2023–2025[3] under Rulemaking Task (RMT).0720.

EASA developed the regulatory material in question in line with Regulation (EU) 2018/1139[4] (the Basic Regulation) and the Rulemaking Procedure[5], as well as in accordance with the objectives and working methods described in the Terms of Reference (ToR) for this RMT.

In particular, EASA developed the regulatory material in question with the support of the European Strategic Coordination Platform (ESCP). The ESCP has been regularly meeting since September 2021 for the development of AMC and GM to the Part-IS regulatory package. Besides EASA, representatives from the following organisations have participated in this activity:

— **ESCP Members**

- European Commission (DG-MOVE);
- other EU agencies and organisations:
  - European Union Agency for Network Information Security (ENISA);
  - EUROCONTROL;

[1] Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, 26.9.2022, p. 18) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1645).

[2] Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 (OJ L 31, 2.2.2023, p. 1) (https://eur-lex.europa.eu/eli/reg_impl/2023/203).

[3] European Plan for Aviation Safety 2023-2025 | EASA (europa.eu)

[4] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

[5] EASA is bound to follow a structured rulemaking process as required by Article 115(1) of Regulation (EU) 2018/1139. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 01-2022 of 2 May 2022 on the procedure to be applied by EASA for the issuing of opinions, certification specifications and other detailed specifications, acceptable means of compliance and guidance material ('Rulemaking Procedure'), and repealing Management Board Decision No 18-2015 (https://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-01-2022-rulemaking-procedure-repealing-mb).

- European Defence Agency (EDA);

- Six European States' national competent authorities (Finland, France, Italy, Poland, Spain and Switzerland);
- European Civil Aviation Conference (ECAC);
- aviation industry associations:
  - AeroSpace and Defence Industries Association Europe (ASD);
  - Airlines for Europe (A4E);
  - Airports Council International — Europe (ACI);
  - Civil Air Navigation Services Organisation — Europe (CANSO);
  - European Cockpit Association (ECA);
  - European Helicopter Association (EHA);
  - European Regional Airlines Association (ERAA);
  - General Aviation Manufacturers (GAMA);
  - International Air Transport Association — Europe (IATA).

— **ESCP Observers**

- Federal Aviation Administration (FAA), Transport Canada Civil Aviation (TCCA), CAA Israel, Agência Nacional de Aviação Civil (ANAC) Brazil;
- North Atlantic Treaty Organization (NATO);
- Aerospace Industries Association of America (AIA);
- Aviation Information Sharing and Analysis Center (A-ISAC);
- European Business Aviation Association (EBA).

1.2. How to comment on this NPA

The draft regulatory material is hereby submitted for consultation of the EASA Advisory Bodies (MAB and SAB) as well as FAA, TCCA, CAA Israel, ANAC (CAA Brazil) in accordance with the ToR for this RMT.

In order to facilitate your review and to prepare for your commenting activity, EASA will organise a workshop on 16 March 2023 at the EASA premises in Cologne.

Please submit your comments via email to **cybersecurity@easa.europa.eu**.

The deadline for the submission of comments is **21 April 2023**.

1.3. The next steps

Following the consultation of the draft regulatory material, EASA will review all the comments received and will duly consider them in the subsequent phases of this rulemaking activity.

Considering the above, EASA may issue a Decision issuing the AMC and GM.

When issuing the Decision, EASA will also provide feedback to the commenters and information to the public on who engaged in the process and/or provided comments during the consultation of the draft regulatory material, which comments were received, how such engagement and/or consultation was used in rulemaking, and how the comments were considered.

2. In summary — why and what

2.1. Why we need to act — issue/rationale

Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645 lay down rules for the identification and management of information security risks in aviation organisations and aviation competent authorities, including EASA. This NPA proposes possible means of compliance for the application of both the Implementing and the Delegated Commission Regulation, facilitating the harmonisation between Member States.

For the description of the issue that the Part-IS regulatory package addresses, see Opinion No 03/2021 'Management of information security risks'. No further issues have been identified with this NPA.

2.2. Assessment of the issue

For the assessment of the issue that the Part-IS regulatory package addresses, see Opinion No 03/2021 'Management of information security risks'. No further assessments have been developed with this NPA.

2.3. Who is affected by the issue

For the description of the stakeholders affected by the issue, see Opinion No 03/2021 'Management of information security risks'.

2.4. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 1 of the Basic Regulation. The regulatory material presented here is expected to contribute to achieving these overall objectives by addressing the issue described in Section 2.1.

More specifically, with the regulatory material presented here, EASA intends to facilitate the timely and harmonised implementation of the Part-IS regulatory package.

2.5. How we want to achieve it — overview of the amendments

The Part-IS regulatory package introduces mostly performance- and risk-based provisions for the identification and management of information security risks in aviation organisations and aviation competent authorities. Compliance with these provisions could be achieved through different approaches and means; therefore, EASA wants to propose AMC, harmonised with all affected organisations represented in the ESCP, that will serve as a common basis to achieve compliance, thereby supporting the application of the requirements in the Part-IS regulatory package. At the same time, through the GM, EASA would like to provide an insight into how certain requirements should be understood from the Agency's point of view and advice on the practical aspects related to the implementation of the requirements (how to). This is also done by referring to available industry standards that could be used to demonstrate compliance. Moreover, in order to facilitate the timely and harmonised implementation in all Member States, the same AMC and GM material is proposed for both the Implementing and the Delegated Regulation and thus for all organisations within the scope of the Part-IS regulatory package and, to a large extent, for authorities when requirements for authorities and organisations contain similar provisions.

AMC and GM are proposed, in particular, to address the following specific issues:

— **Objective of the rule**

The assessment of the safety impact, taking into account the different perspectives of the organisations/authorities subject to the Regulation, for some of which an information security incident may have an immediate safety impact, while for others it may have a delayed impact. This aspect is addressed in several parts of the AMC and GM material such as the risk assessment, the incident management, and the examples of threat scenarios.

— **Definitions**

Although a number of definitions have been included in the Regulation, specific terms utilised throughout the AMC and GM material have been described.

— **Identification of interfaces with other organisations**

The identification of the interfaces (also called 'functional chains') with other organisations with which the organisation/authority shares information security risks, as well as of commonly shared and understood criteria for performing the risk assessments and for sharing information on residual risks.

— **Identification of threat scenarios and risk assessment**

- The identification of threat scenarios as a way for the organisation/authority to identify information security risks that could have an impact on aviation safety.
- Assessment of the information security risk as a combination of the potential of occurrence of the threat scenario and the severity of its safety consequences, and establishment of risk acceptance criteria.

— **Treatment of unacceptable risks**

A possible way for the development and implementation of measures aimed at treating those risks that cannot be accepted, including considerations about the prioritisation of certain measures and the evaluation of their effectiveness.

— **Proportionality**

To implement an ISMS taking into account aspects such as the inherent risk of the organisation's/authority's activities, as well as the size and the complexity of the organisation/authority.

— **Temporary exemption of certain organisations from the requirement to have an ISMS**

For organisations, how to perform the 'information security risk assessment' required by IS.I.OR.200(e) / IS.D.OR.200(e) in order to demonstrate to the competent authority that the organisation's activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with an impact on safety neither to itself nor to other organisations.

— **Evaluation of staff sufficiency and staff competence**

- A possible way to evaluate the sufficiency of the resources to execute the main tasks stemming from the implementation of the Regulation.
- The design of a tailored competence scheme for the personnel that is involved in Part-IS-related tasks and activities.

3. What are the expected benefits and drawbacks of the regulatory material

No additional impacts have been identified compared to those created by the Regulations and described in Opinion No 03/2021 'Management of information security risks'.

Overall, the provision of AMC and GM is beneficial in supporting the application of the rule.

4. Proposed regulatory material

Based on the above, the following AMC and GM are proposed as Annexes I, II, III to this NPA:

— **Annex I**

This Annex contains AMC and GM to the Articles and to both the authority requirements (IS.AR.XXX) and organisation requirements (IS.I.OR.XXX) of Commission Implementing Regulation (EU) 2023/203.

— **Annex II**

This Annex contains AMC and GM to the Articles and to organisation requirements (IS.D.OR.XXX) (for design and production organisations, aerodrome operators and apron management services providers) of Commission Delegated Regulation (EU) 2022/1645.

— **Annex III**

Amendments to the AMC & GM listed under 'ED DECISIONS TO BE AMENDED' on the cover page of this document.

It is important to note that the AMC and GM to the organisation requirements in Regulations (EU) 2022/1645 and 2023/203 are almost identical.

5. Monitoring and evaluation

The usefulness of the AMC & GM to Commission Regulations (EU) 2022/1645 and 2023/203 will be monitored through standardisation and oversight activities.

Moreover, the AMC & GM will be monitored in the frame of the implementation support task (IST.0001).

6. Proposed actions to support implementation

Under IST.0001 ‘Supporting the implementation of the IS management system (ISMS) by industry and NCAs’ described in Volume II of the EPAS for 2023–2025, EASA will:

— set up dedicated thematic workshops;

— support national competent authorities and organisations in the development of competence building / training for the implementation of the Part-IS regulatory package and the relevant oversight.

— set up a dedicated task force with volunteer NCAs to jointly discuss and address the challenges linked with the Part-IS regulatory package implementation;

— carry out pilot projects with volunteer organisations to implement the Part-IS regulatory package ahead of the applicability date.

7. References

The following (non-exhaustive) list includes regulations/documents that have been considered during the development of this NPA:

— Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014

— Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664

— ISO 27000 Series on ‘information security management systems (ISMS)’ standards

— EUROCAE ED-200 Series on ‘information security in aviation’ standards

Appendix — Quality of the NPA

To continuously improve the quality of its documents, EASA welcomes your feedback on the quality of this document with regard to the following aspects:

Please provide your feedback on the quality of this document as part of the other comments you have on this NPA. We invite you to also provide a brief justification, especially when you disagree or strongly disagree, so that we consider this for improvement. Your comments will be considered for internal quality assurance and management purposes only and will not be published.

1. The regulatory proposal is of technically good/high quality

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

2. The text is clear, readable and understandable

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

3. The regulatory proposal is well substantiated

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

4. The regulatory proposal is fit for purpose (achieving the objectives set)

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

5. The impact assessment (IA), as well as its qualitative and quantitative data, is of high quality

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

6. The regulatory proposal applies the 'better regulation' principles[1]

Please choose one of the options
Fully agree / Agree / Neutral / Disagree / Strongly disagree

7. Any other comments on the quality of this document (please specify)

[1] For information and guidance, see:
- https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how_en
- https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en
- https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

Annex I

AMC & GM to Commission Implementing Regulation (EU) 2023/203

GM1 Article 1 — Subject matter

When taking measures under this Regulation, the affected organisations and competent authorities are encouraged to consider the principle of proportionality to ensure that such measures are appropriate to the nature and risk of their activities.

GM1 Article 3 — Definitions

For the sake of common understanding, the following is a description of the terms used in this document:

Audit	It refers to a systematic, independent, and documented process for obtaining evidence, and evaluating it objectively to determine the extent to which requirements are complied with. *Note: Audits may include inspections.*
Assessment	In the context of management system performance monitoring, continuous improvement and oversight, it refers to a planned and documented activity performed by competent personnel to evaluate and analyse the achieved level of performance and maturity in relation to the organisation's policy and objectives. *Note: An assessment focuses on desirable outcomes and the overall performance, looking at the organisation as a whole. The main objective of the assessment is to identify the strengths and weaknesses to drive continuous improvement.* *Remark: For 'risk assessment', please refer to the definition below.*
Competency	It is a combination of individual skills or standard of performance, practical and theoretical knowledge, attitudes, training, and experience.
Control	It is a measure that maintains and/or modifies risk.
Correction	It is the action taken to eliminate a detected non-compliance.
Corrective action	It is the action taken to eliminate or mitigate the root cause(s) and prevent the recurrence of an existing detected non-compliance or other undesirable conditions or situations.
Deficiency	It is as a deviation from compliance with or a non-fulfilment of any requirement or objectives, either from a regulatory or an organisation's perspective, either completely or partially.
Experience	It is the fact or state of having been affected by or gained knowledge and skills through observation, participation or doing.
Functional chain	The concept of functional chain pursues the objective of supporting the management of risks, through consideration of all the involved functions starting from the aircraft downstream. This shall allow a holistic perspective for identifying and assessing risks, including the involved support functions. An example could be when the cyber risk for FMS data integrity is assessed, the following functions require consideration: MRO (maintenance of the FMS), wireless access to FMS, FMS supply chain for the sourcing of components, other potential wireless data communication means (e.g. with airport, AOC, etc.).
Hazard	It is a condition or an object with the potential to cause or contribute to an aircraft incident or accident.

Human factors	They are concerned with the application of what we know about human beings, their abilities, characteristics and limitations, to the design of equipment they use, environments in which they function, and jobs they perform.
Just culture	It means a culture in which front-line operators or other persons are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but in which gross negligence, wilful violations and destructive acts are not tolerated, as defined in Article 2 of Regulation (EU) No 376/2014.
Knowledge	Content of information needed to perform adequately in the job at an acceptable level, usually obtained through formal education and on-the-job experience. This knowledge is necessary for job performance but is not sufficient on its own.
Management (activity)	In the general organisational context, it refers to the activities aimed at directing, controlling, and continually improving the organisation within appropriate structures. In the context of this Regulation it means, more specifically, the supervision and making of decisions necessary to achieve the organisation's safety and information security objectives.
Management system	It refers to a set of interrelated or interacting system elements to establish policies, objectives and processes to achieve those objectives, where the system elements include the organisational structure, roles and responsibilities, planning and operations.
Qualification	It is the combination of knowledge, aptitude, skill, quality, ability, accomplishment or capacity that makes a person suitable to take on a certain role or to carry out a task or gives the justification to do so.
Professional background	It is the combination of knowledge, experience and current on-the-job training.
Risk assessment	It is an evaluation that is based on engineering and operational judgement and/or analysis methods in order to establish whether the achieved or perceived risk is acceptable or tolerable.
Risk register	It refers to a physical or digital means of documentation used as a risk management tool that acts as a repository for all identified risks and contains additional information about each risk, such as the nature of the risk, mitigation measures, ownership, status, etc.
Safety risk	It refers to the predicted likelihood and severity of the consequences or outcomes of a hazard.

GM1 Article 6 — Competent authority

A competent authority may be a ministry, a national aviation authority, or any aviation body designated by the Member State and located within that Member State. A Member State may designate more than one competent authority to cover different areas of responsibility, as long as the designation decision contains a list of the competencies of each authority and there is only one competent authority responsible for each given area of responsibility. In certain cases, the competent authority may be the Agency.

GM1 IS.AR.200 Information security management system (ISMS)

An **information security management system (ISMS)** is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security aimed to protect the information assets in order to achieve the organisation's operational and safety objectives in a risk-managed, effective and efficient manner.

The ISMS applies an information security requirement analysis and an information security risk management process to decide on, and manage the selection, implementation and operation of controls over all architectural layers (governance, business, application, technology, data), domains (organisational, human, physical, technical) and the perspectives of governance, risk management and compliance (GRC) within the ISMS scope. The risk management process is based on an aviation safety risk assessment and the risk acceptance levels designed to effectively treat and manage risks with a potential impact on aviation safety caused by threats exploiting vulnerabilities of information assets in aeronautical systems, as depicted in Figure 1.

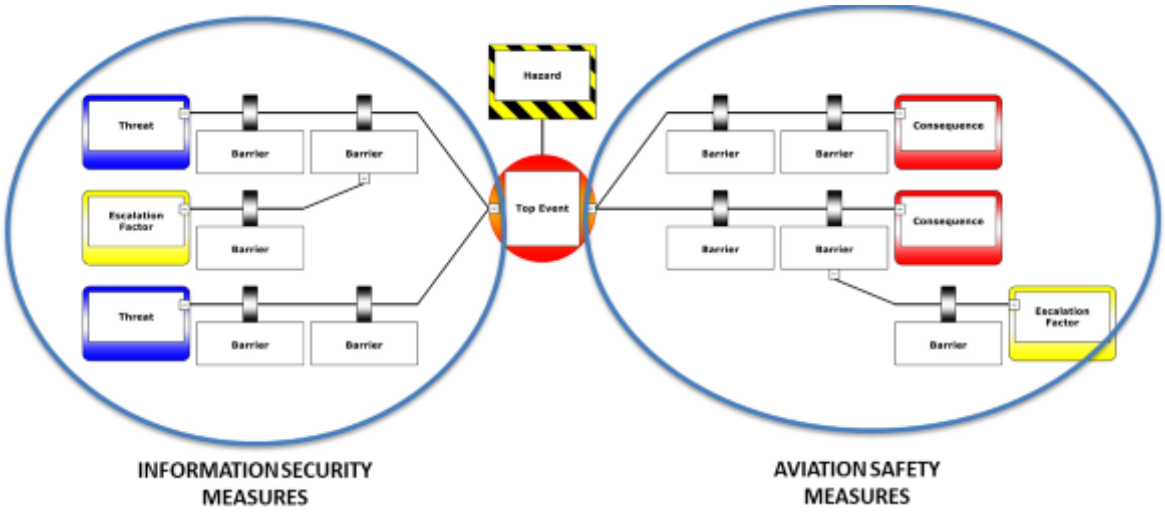

Figure 1: Bow-tie representation of management of aviation safety risks posed by IS threats

The ISMS in this Regulation should bring together the information security and aviation safety competence in most of the processes, including, for instance, identifying critical systems or threats, and assessing potential impacts on and risks to aviation safety.

ISMS implementation and maintenance

An ISMS, as per this Regulation, employs the perspectives of governance, risk and compliance, and an approach that combines the dimensions of safety risk and performance to determine the information security controls that are appropriate for and compliant with the specific context and can effectively provide the required level of protection to achieve the aviation safety objectives:

— **Governance** perspective refers to providing management direction and leadership aimed to achieve the entity's own overarching objectives:

  — leadership and commitment of the senior management defining and ensuring the close involvement of the management and a 'top-down' ISMS implementation

  — information security and safety objectives derived from, aligned and consistent with the entity's business objectives and monitored by, e.g., management reviews

  — information security policies stating the principles and objectives to be achieved

  — roles, responsibilities, competencies and resources required for an effective ISMS

  — effective, target-group-oriented communication to internal & external stakeholders

— **Risk** perspective refers to a key aspect of an ISMS in an aviation safety context according to this Regulation and serves as a basis for transparent decision-making and prioritisation of controls and risk treatment options. It further refers to the assessment, treatment and monitoring of information security risks in support of the management of aviation safety risks for the key processes and information assets upon which they depend. This includes protection requirements, risk exposure, attitude towards risks and risk acceptance criteria, methods and industry standards.

— **Compliance** perspective refers to the compliance with regulatory, legal and contractual (supply chain and operational peers) requirements. This includes:

  — this Regulation,

  — the entity's own policies and standards and may further include international or industry standards adopted by the entity from ISO, EUROCAE, etc.

  The perspective comprises the definition, implementation and maintenance of the required security provisions whose effectiveness and compliance shall be regularly monitored and assured by, e.g., (internal) audits.

Based on these perspectives, we may identify 14 core components or building blocks that have been shown to be relevant for the establishment of an effective ISMS. These ISMS core components can be summarised as follows:

(a) context establishment defining the scope, interfaces, dependencies and requirements of interested parties;

(b) leadership and commitment of the senior management;

(c) information security and safety objectives;

(d) information security policies;

(e) roles, responsibilities, competencies and resources required for an effective ISMS;

(f) communication to internal and external stakeholders, and a sufficient level of security awareness among employees, managers and third parties;

(g) information security risk management including risk assessment and treatment;

(h) information security incident management establishing processes for the handling of information security incidents and vulnerabilities;

(i) performance & effectiveness monitoring, measurement and evaluation;

(j) internal audits and management reviews;

(k) corrections and corrective actions;

(l) continuous improvement;

(m) relationship with suppliers;

(n) documentation and evidence collection.

Additional critical success factors for the implementation and operation of an ISMS include the following:

— The ISMS should be integrated with the entity's processes and overall management structure or even — at least partially, with safeguards for their respective integrity, and as reasonably applicable — with an overarching management system comprising information security, aviation safety and quality management.

— Information security has to be considered at an early stage in the overall design of processes and procedures, of systems and of information security controls, to be seamlessly integrated, for maximum effectiveness, minimal functional interference and optimised cost. None of these benefits can be achieved by integrating it later.

— The risk management process determines appropriate characteristics of preventive controls to reach and maintain acceptable risk levels.

— The incident management process ensures that the organisation detects, reacts and responds to information security incidents in a timely manner. This is achieved by defining responsibilities, procedures, scenarios and response plans in advance to ensure a coordinated, targeted and efficient response.

— Continuous monitoring and reassessment are undertaken and improvements are made in response.

The above-mentioned core components are related to the requirements in this Regulation, for which Figure 2 provides a high-level depiction of the aspects that are more prominent in the implementation phase and those that characterise the operational phase, as well as the review and possible improvement.

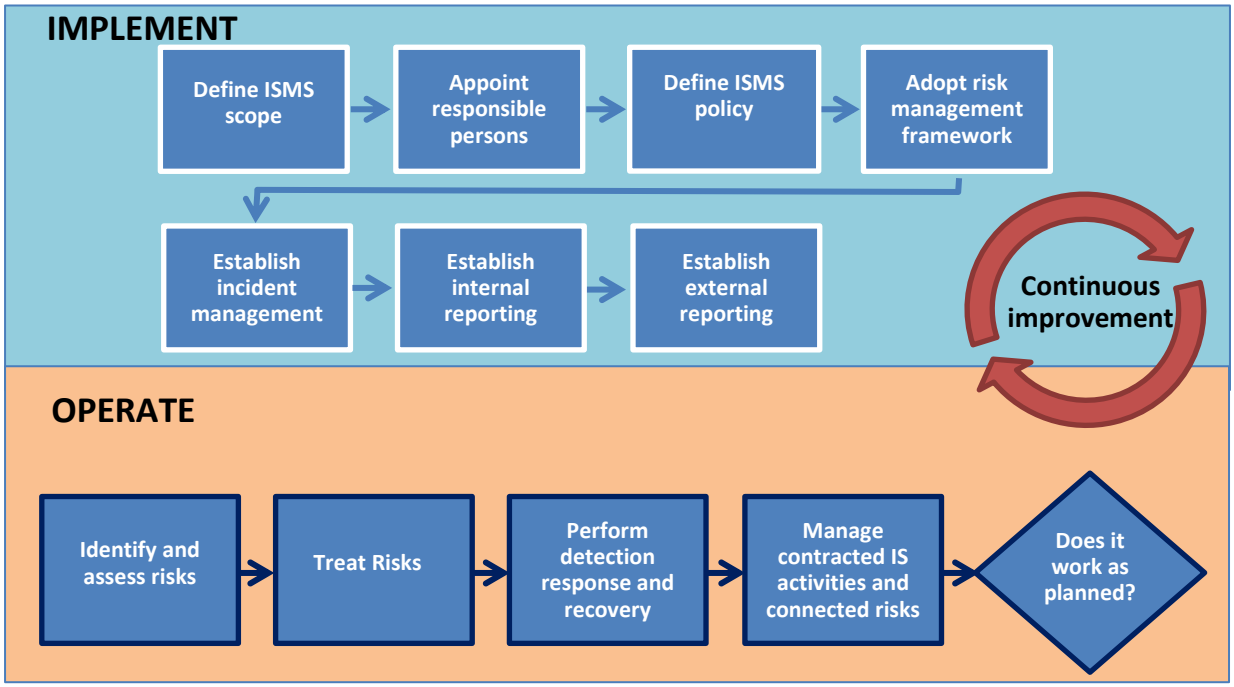

Figure 2: Representation of the Part-IS requirements from an ISMS's life cycle perspective

Plan-Do-Check-Act approach

The Plan-Do-Check-Act (PDCA) refers to a process approach that is often used to establish, implement, operate, monitor, review and improve management systems. Figure 3 depicts the PDCA applied to an ISMS.

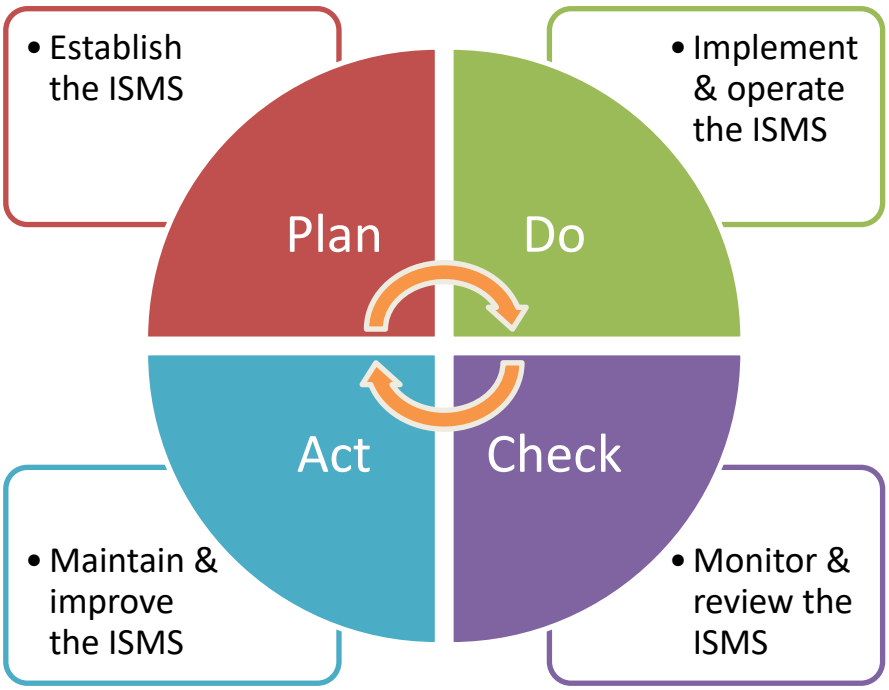

Figure 3: Plan-Do-Check-Act approach applied to ISMS

An alternative cyclical process is Define-Measure-Analyse-Improve-Control (DMAIC, six sigma).

Benefits of an ISMS

The benefits of a management system operating in a dynamic, uncertain or unpredictable risk environment are realised over the long term only when the organisation improves existing controls, processes and solutions based on the assessments of risks, performance and maturity as well as the learnings from incidents, audits, non-conformities and their root causes. A successful adoption and deployment of an ISMS allows an entity to:

— achieve greater assurance to the management and interested parties that its information assets are adequately protected against threats on a continual basis;

— increase its trustworthiness and credibility providing confidence to interested parties that IS risks with an impact on aviation safety are adequately managed;

— increase the resilience of the entity's key processes against unauthorised electronic interactions and maintains the entity's ability to decide and act;

— support the timely detection of control gaps, vulnerabilities or deficiencies aimed to prevent security incidents or at least to minimise their impact;

— detect and timely react to changes in the entity's environment including system architecture and threat landscape or the adoption of new technologies;

— provide a foundation for effective and efficient implementation of a comprehensive security strategy in times of digital transformation, increasing interconnectivity of systems, emerging information security threats and new technologies.

Relation to ISO 27001

The international standard ISO 27001 is a widely adopted standard for ISMS: it specifies generic requirements for establishing, implementing, maintaining and continually improving an ISMS and also includes requirements for the assessment and treatment of IS risks. The requirements are applicable to all entities, regardless of type, size or nature. The conformity of an ISMS with the ISO 27001 standard can be certified by an external qualified auditor on behalf of a reputable certification authority. ISO 27001 is compatible with other management system standards (quality, safety, etc.) that have also adopted the structure and terms defined in Annex SL to ISO/IEC Directives, Part 1, Consolidated ISO Supplement: this compatibility allows an entity to operate a single management system that meets the requirements of multiple management system standards.

The requirements for an ISMS specified by this Regulation are in most parts consistent and aligned with ISO 27001; however, this Regulation introduces provisions specific to the context of aviation safety. If an ISO 27001-based ISMS is already operated by an entity for a different scope and context, it can be adapted and extended to the scope and context of this Regulation in a straightforward manner based on an analysis of the scope and the gaps.

PART-IS versus ISO 27001 cross reference table

For a comparison between the main tasks required under Part-IS and the clauses and relevant controls in ISO 27001, refer to Appendix II.

AMC1 IS.AR.200(a)(1) Information security management system

The competent authority should define and document the scope of the ISMS, by determining activities, processes, supporting systems, and identifying those which may have an impact on aviation safety.

The information security policy should cover at least the following aspects with a potential impact on aviation safety by:

(a) endorsement by the person identified as per IS.AR.225(a) and review at planned intervals or if significant changes occur;

(b) committing to comply with applicable legislation, consider relevant standards and best practices;

(c) setting objectives and performance measures for managing information security;

(d) defining general principles, activities, processes for the competent authority to appropriately secure information and communication technology systems and data;

(e) integrating ISMS requirements into the processes of the competent authority;

(f) committing to continually improve towards higher levels of information security process maturity as per IS.AR.235;

(g) committing to satisfy applicable requirements regarding information security and its proactive

and systematic management and to the provision of appropriate resources for its implementation and operation;

(h) assigning information security as one of the essential responsibilities for all managers;

(i) continuously promoting the information security policy within the competent authority/organisation to all personnel;

(j) encouraging the implementation of a 'just culture' and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents;

(k) communicating the information security policy to all relevant parties, as appropriate.

GM1 IS.AR.200(a)(1) Information security management system (ISMS)

INFORMATION SECURITY POLICY AND OBJECTIVES

The information security policy should suit the entity's purpose and direct its IS activities. Such policy should contain the needs for IS in the entity's context, a high-level statement of direction and intent of the IS activities, the principles and most important strategic and tactical objectives to be achieved by the ISMS, as well as the general IS objectives or a specification of a framework (who, how) for setting IS objectives. The IS policy should also contain a description of the established ISMS including roles, responsibilities and references to topic-specific policies and standards.

The IS objectives should be:

— consistent and aligned with the IS policy and consider the applicable IS requirements, derived from the overarching entity's objectives, and the results from the risk assessment and treatment (which, in turn, supports the implementation of the entity's strategic goals and IS policy);

— regularly reviewed to ensure that they are up to date and still appropriate;

— measurable if practicable (to be able to determine whether or not the objective has been met), aimed to be SMART (specific, measurable, attainable, realistic, timely) and aligned with all affected responsible persons.

When defining IS objectives, e.g., based on the overarching entity's objectives, the IS requirements, or the results of risk assessments, it should be determined how these objectives will be achieved. The degree to which IS objectives are achieved must be measurable. If possible, it should be measured by KPIs which have been defined in advance (refer to resources such as COBIT 5 for Information Security). It is recommended to start with the definition of a limited number of IS objectives which are relevant for the entity, more of a long-term nature and measurable with a reasonable effort relative to the delivered benefits.

AMC1 IS.AR.200(a)(8)&(a)(9) Information security management system (ISMS)

When establishing compliance with the provisions under points IS.AR.200 (a)(8) and (a)(9), the competent authority should:

(a) implement a function to periodically monitor compliance of the management system with the relevant requirements and adequacy of the procedures including the establishment of an internal audit process and an information security risk management process. Compliance

monitoring should include a feedback system of audit findings to the person of the competent authority as identified in IS.AR.225(a) to ensure implementation of corrective actions as necessary;

(b) implement and maintain suitably robust information security controls for the protection of information, ensuring the principle of need-to-know. It should protect the source of information in accordance with the relevant provisions established in Regulation (EU) 2018/1139. It should also comply with Regulation (EU) No 376/2014.

AMC1 IS.AR.200(a)(11) Information security management system (ISMS)

When establishing compliance with the provisions under point IS.AR.200(a)(11), the competent authority should implement and maintain a process to share applicable and relevant information for performing information security risk assessments, with other competent authorities, the Agency and other affected organisations within the scope of this Regulation, as soon as it becomes aware of such information. The competent authority should define and document which kind of information needs to be shared and with whom.

GM1 IS.AR.200(a)(8) Information security management system (ISMS)

COMPLIANCE MONITORING

For the purpose of compliance monitoring, internal audits should be conducted at planned intervals to provide assurance on the status of the ISMS to the management and to provide information on the following:

— conformity of the ISMS to the requirements of this Regulation and the competent authority's own requirements either stated in the IS policy, procedures and contracts or derived from information security objectives or outcomes of the risk treatment process;

— effective implementation and maintenance of the ISMS.

Internal audits should follow an independent, evidence-based approach and set up an audit programme taking into consideration the importance of the processes concerned and definitions of the audit criteria and scopes. Documented information should be retained evidencing the audit results, their reporting to the relevant management and the audit programme.

AMC1 IS.AR.200(c) Information security management system (ISMS)

When establishing compliance with the provisions under point IS.AR.200(c), the competent authority should:

(a) provide an outline of the structure of the specific security resources (internal and external), including their roles and responsibilities that will be used to manage and maintain the assets and resources included within the scope and approved by the person identified as per IS.AR.225(a) and review at planned intervals or if significant changes occur;

(b) identify and categorise all relevant contracted organisations or qualified entities used to implement the ISMS. The competent authority should define and document procedures for the management of interfaces and coordination between the competent authority and other national authorities, contracted organisations or qualified entities;

(c) identify and define all key processes and procedures, and internal and external reporting schemes that will be used to maintain compliance with the objectives over the life cycle of the ISMS. The competent authority may adjust existing processes or procedures for compliance;

(d) identify and document any other information that will be used to maintain compliance with the objectives;

(e) when creating and updating documented information, ensure appropriate identification and description (e.g. a title, date, author, or reference number) as well as a review and an approval for suitability and adequacy;

(f) control documented information required by the ISMS to ensure that:

(1) it is available and suitable for use, where and when it is needed;

(2) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

GM1 IS.AR.200(c) Information security management system (ISMS)

The amount of documented information that should be developed to maintain compliance with the objectives of this Regulation may vary between competent authorities due to various factors, such as size and complexity, or the need for harmonisation with other management processes already in place. As general guidance, taking into account the documents required to comply with point IS.AR.200(a) and the record-keeping requirements referred to in IS.AR.230, the following is a non-exhaustive list of information that should be documented:

(a) information security policy that should include the authority's security objectives — see IS.AR.200(a)(1);

(b) responsibilities and accountabilities for roles relevant to information security;

(c) scope of the ISMS and the interfaces with, and dependencies on, other parties — see IS.AR.200(a)(2) and the information security requirements referred to in point IS.AR.205;

(d) information security risk management process;

(e) archive of risks with results of the information security risk assessment and treatment measures (often referred to as 'risk register' or 'risk ledger') — see IS.AR.230;

(f) evidence of the competencies necessary for the personnel performing the activities required under this Regulation;

(g) evidence of the current competencies of the personnel performing the activities required under this regulation;

(h) (key) performance indicators derived from evidence of the monitoring and measurement of the ISMS processes.

GM1 IS.AR.200(d) Information security management system (ISMS)

PROPORTIONALITY IN ISMS IMPLEMENTATION

When implementing the processes and procedures, as well as establishing the roles and responsibilities required under point IS.AR.200(d), the competent authority should primarily consider the risks that it may be posing to other organisations, as well as its own risk exposure. Other aspects that may be relevant include the authority's needs and objectives, security requirements, its own processes, and the size, complexity and structure of the authority, all of which may change over time.

INTEGRATION OF ISMS UNDER THIS REGULATION WITH EXISTING MANAGEMENT SYSTEMS

A competent authority may take advantage of existing management systems when implementing an ISMS by integrating it with those existing systems.

By integrating the ISMS with existing management systems, the competent authority may reduce the effort and costs required to implement and maintain the ISMS, while also ensuring consistency and alignment with the authority's overall management approach. Below is a non-exhaustive list of potential synergies that can be exploited when integrating the ISMS with an existing management system:

— Leverage existing policies and procedures: an authority may use its existing policies and procedures as a foundation for its ISMS. This may help to ensure consistency and minimise the need for additional documentation.

— Align ISMS with other management systems: an authority may align the ISMS with other management systems, such as safety management systems (SMS), to ensure that the ISMS is consistent with the organisation's overall management approach.

— Use existing risk management processes: an authority may use their existing risk management processes to identify and assess the security risks to their sensitive information.

— Reuse existing controls: an authority may reuse existing controls, such as access controls or incident management process, to implement the security controls required by the ISMS.

— Continuous improvement process: an authority may use the continuous improvement process of existing management systems to improve the ISMS over time.

AMC1 IS.AR.205(a) Information security risk assessment

The competent authority, when conducting an information security risk assessment, should ensure that all aviation safety-relevant assets (e.g. physical, human, information) are identified and included in the ISMS scope as per IS.AR.200 and relevant AMC. Additionally, the competent authority should provide the justification for those assets that are included and those that are excluded from the scope based on the outcome of its risk assessment. The competent authority should identify the criteria to be used.

The competent authority should identify all the elements of its own organisation which are within the scope of its ISMS and which could be exposed to information security risks and should include at least those listed in IS.AR.205(a).

GM1 IS.AR.205(a) Information security risk assessment

For competent authorities no specific security framework, such as ISO, NIST, or others, is explicitly mentioned for the development of their risk assessment. Each framework offers different benefits and none of these frameworks is perfect for an individual competent authority and should be customised and tailored to meet the overall needs of a competent authority as well as the specific needs related to the aviation assets to be included within the scope of the ISMS.

Competent authorities whose security frameworks have achieved industry certifications can provide this information as supporting artefacts; however, these organisations should show the applicability of the industry certification to the scope of this Regulation.

To help guide aviation entities, aviation-specific guidance defined in the most current version of the EUROCAE ED-201x document 'Risk Management' chapter and in the ED-204x, ED-205x and ED-206x documents supporting chapters for 'Risk Management' appropriate for the unique operating environment, may be considered.

Regardless of the framework used, the competent authority should demonstrate a clear and comprehensive understanding of all relevant data flows and information exchanges. The competent authority should provide corresponding documentation on resources and dependencies related to computing, networking, supply chain and contracted services which have the potential to affect the information security and safety of the functions, services or capabilities within the scope of the risk assessment.

The following non-exhaustive list provides examples of items that should also be included in the aforementioned documentation. The level of detail should be commensurate with the expected level of risk. The purpose is to establish an understanding of all relevant assets, resources and dependencies that are directly a part of the functions, services and capabilities through the following information:

(a) Identification of inputs and outputs of the risk assessment:

- internal;
- external;
- internal leased or managed services, supply chain or other dependency;
- external leased or managed services, supply chain or other dependency;

(b) Identification of all relevant resources (i.e. hardware, software, network and computing resources) used to create, transmit, store or receive the inputs and outputs;

(c) Identification and definition of the physical operating environments and locations for all relevant resources;

(d) For each asset included within the scope, identification and association of the specific methods or resources that will be used by the organisation to manage, operate and maintain each asset over the life cycle of each asset including:

- internal resources;
- contracted resources;
- supply chain;

— managed service provider.

The competent authority should also demonstrate a clear and comprehensive understanding of the resources that are used by the organisation to ensure effective operations, management and oversight (internal and external).

AMC1 IS.AR.205(b) Information security risk assessment

To establish compliance with IS.AR.205(b), the competent authority should, based on the exchange of data and information and the assets used for this, identify within the scope of the information security risk assessment, the interfaces it has with other parties, such as service providers, supply chains and other third parties, and which could result in a situation where information security risks either:

— pose a threat to other parties; and/or

— pose a threat to the competent authority,

as a result of mutual exposure to those risks.

GM1 IS.AR.205(b) Information security risk assessment

Competent authorities may follow any security framework such as ISO, NIST, or other when developing their risk assessment. The method needs to allow for the consideration of risk sharing between interconnected parties. As an example, EUROCAE ED-201A, Figure 4-1 'Risk Assessment and Sharing Stages' represents a risk assessment process which can support competent authorities in identifying, assessing and agreeing on shared risks with others.

Competent authorities should follow the guidance defined in chapters 'Risk Management' and 'The concept of functional chains' of EUROCAE ED-201A. Additional guidance from supporting chapters regarding 'Risk Management' that is appropriate for the unique operating environment can be found in the ED-204x, ED-205x and ED-206x documents.

Risk information sharing

Risk information sharing means that interfacing parties should inform each other about the potential exposure to information security risks by following, for instance, the approach detailed in ED-201A Appendix B.1, B.2 and B.3. The purpose of this exchange of information is to enable the parties to establish a matching mapping for those services which are identified under IS.AR.205(a), including all flows of information and data in order to:

(a) illustrate (e.g. through a functional diagram) the relationships of logical and physical paths connecting the different involved part;

(b) clearly identify all assets and resources that will be used in the exchange;

(c) identify and categorise all functions, activities and processes, including their respective information and data, which will be created, transmitted, received and stored, and associate those with the responsible party which provides or performs those functions, activities and processes;

(d) determine for these paths, constituting the so-called functional chains, the role of the interfacing party as a producer, processor, dispatcher, or consumer of the involved information or data;

(e) determine whether one interfacing party acts as an originator or receiver of a flow across such path.

GM2 IS.AR.205(b) Information security risk assessment

EXAMPLES OF AVIATION SERVICES

Examples of aviation services are provided in Appendix III.

AMC1 IS.AR.205(c) Information security risk assessment

The competent authority should use a risk management framework that includes a methodology for assigning risks with a risk level and establishing criteria for determining risk acceptance or further treatment.

The competent authority should provide documented evidence of risks which have a potential impact on aviation safety including the level of risks. The competent authority should relate each risk to the relevant elements and interfaces identified under IS.AR.205 (a) and (b), and document whether the risk is acceptable or requires further treatment.

The competent authority should provide the assurance that the risk assessment process is performed with the necessary rigour and discipline by documenting the process and its robustness. By doing so, the competent authority should consider:

(a) reproducibility of the assessment's inputs and results;

(b) repeatability of the assessment over time in a way that the results of the different prior assessments can be compared to determine the changes;

(c) the gathering of inputs that are relevant and up to date, in particular:

— the information that allows the determination of the safety consequences;

— the information that allows the determination of the potential of occurrence of the threat scenario.

GM1 IS.AR.205(c) Information security risk assessment

RISK ASSESSMENT

The risk classification levels for potential of occurrence of the threat scenario and severity of the safety consequences listed below may be applied, however this does not prevent the competent authority from developing additional intermediate categories if it deems this necessary for risk assessments. The competent authority should specify and document the applied, entity-specific, classification levels with an accurate qualitative definition and a quantitative definition in terms of a range, or interval of real numbers in order to enable a sufficiently calibrated, consistent estimation, evaluation and communication within the entity, or at the interfaces. The potential of occurrence of the threat scenario may be expressed as an interval of likelihoods including the duration of the observation. Supporting documentation and methods can be found in EUROCAE ED-203A Chapter 3.6 which references the evaluation of the potential of occurrence of the threat scenario in the Security Risk Assessment of EUROCAE ED-202A.

In order to facilitate the mutual comparability of risks assessment methodologies between interfacing

organisations, the competent authority may associate the assessment of the potential of occurrence of the threat scenario with one of the following categories:

— High potential of occurrence: the threat scenario is likely to occur. The attack related to the threat scenario is feasible and similar threat scenarios have occurred many times in the past.

— Medium potential of occurrence: the threat scenario is unlikely to occur. The attack related to the threat scenario is possible and a similar threat scenario may have occurred in the past.

— Low potential of occurrence: the threat scenario is very unlikely to occur. The materialisation of the threat scenario is theoretically possible; however, it is not known to have occurred.

The evaluation of the potential of occurrence of the threat scenario can be based on the following aspects:

Protection (as defined in EUROCAE ED-203A)

— Security measures and architecture that deny access to assets: the degree to which an asset is open to access from compromised systems.

— Access to security measures: the degree to which a security measure prevents access/attack to itself from compromised systems.

— Failure of mechanism: the degree to which the known implementation of a security measure will fail to prevent an attack.

— Detection methods or procedures to recognise the attack and appropriately respond to reduce the potential of occurrence of the threat scenario.

Exposure reduction (as defined in EUROCAE ED-203A)

— Conditions under which an external access connection can be used by a user or attacker

— Limits on the functionality of an external access connection

— Organisational policies that control the time-to-feasibility for developing attack tools specific to the product

— Vulnerability management including intelligence, scanning, treatment and retesting aimed to discover, detect and treat newly reported or detected vulnerabilities in a fast, risk-prioritised manner with high assurance in order to reduce the attack surface

Attack attempt (as defined in EUROCAE ED-203A)

— The capability of the attackers which is determined by the resources and expertise required for their attack

  The capability of the attackers can be assessed through several ways, for instance:

  — information from CERTs/CSIRTs, ISACs;

  — analyses of past activities, tactics, techniques and procedures (TTPs) and success rate of attacks.

For the same reason, the competent authority may associate the outcome of the evaluation of the severity of the safety consequences with one of the following categories:

— High severity: those immediate or delayed scenarios that can cause or contribute to an accident

where an accident means an occurrence associated with the operation of an aircraft in which:

— a person is fatally or seriously injured,

— the aircraft sustains damage or structural failure,

— the aircraft is missing or completely inaccessible;

— Moderate severity: those immediate or delayed scenarios that can cause or contribute to safety incidents where an incident means any occurrence other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operations;

— Low severity: those immediate or delayed scenarios that can cause or contribute to negligible safety consequences.

Additional information can also be found in Regulation (EU) 2015/1018 on mandatory reporting of occurrences. Further examples for aviation domains can be found in EUROCAE ED-201A – Appendix B – Tables B-5, B-6 and B-7.

Risk acceptance criteria

Risk acceptance criteria are critical and should be developed, specified and documented. The criteria may define multiple thresholds, with a desired target risk level, but including also provision for the person identified in IS.AR.225(a) to accept risks above this level under defined circumstances and conditions.

In order to facilitate the mutual comparability of risk assessments between interfacing entities, the competent authority should classify the risks in the following categories:

— unacceptable risk;

— conditionally acceptable risk;

— acceptable risk.

For what concerns the conditional acceptance of risks, the criteria for acceptance should take into account how long a risk is expected to exist (temporary or short-term activity or exposure), or may include requirements for the commitment of future treatments to reduce the risk at an acceptable level within a defined time duration, and show how the risk will be managed over time through the authority's risk governance processes.

Moreover, risks should be conditionally accepted only under the condition that the competent authority demonstrates the presence of a comprehensive risk management structure that includes risk assessment, risk treatment and risk monitoring processes for operations. This is typically achieved when the competent authority reaches a higher level of maturity that is representative of functionality and repeatability of cybersecurity risk management — see GM1 IS.AR.235(a).

The following Figure 1 depicts a risk acceptance matrix based on the aforementioned categories that can be used by interfacing organisations for mutual comparability.

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Figure 1: Risk acceptance matrix

* The potential of occurrence of the threat scenario is reassessed in a timely manner (refer to IS.AR.205(d)) and monitored to ensure that it remains low and that if the risk materialises, it is early detected and dealt with.

A comprehensive risk management structure typically entails the following aspects and processes:

— a repeatable and reproduceable risk assessment. If the risk factors are considered fairly uncertain and within some wide value range or not sufficiently precise, further iterations of the risk assessment are performed involving additionally gathered or detailed information and a more in-depth assessment in order to reduce uncertainty and increase precision;

— a thorough review of those risks proposed to be conditionally acceptable that is performed by the person identified in IS.AR.225(a) who may impose additional conditions for the risk retention;

— strict monitoring of the key risk indicators that includes a defined, reliable detection of the potentially evolving risk materialisation;

— an incident response scheme is in place with reactive measures that are triggered by detection mechanisms in order to immediately contain the consequences, in particular, for risk scenarios involving a high severity level.

Note: A risk assessment processes can be classified as ‘repeatable’ when under the same conditions an entity or a person delivers the same result. Conditions can include:

— use of the same information security risk assessment framework or methodology;

— use of the same inputs, assumptions, security context and threat environment, considering the time period, where long breaks can significantly affect the repeatability;

— use of the same observing entity/person.

Similarly, a risk assessment processes can be classified as ‘reproduceable’ when another entity or another person given the same inputs, assumptions, security context and threat environment can reproduce the assessment in its entirety.

Threat scenario identification

A threat scenario is one of the possible ways a threat could materialise. Typically, a threat scenario describes a potential attack targeting one or more vulnerabilities of assets, as well as processes.

The purpose of the threat scenario identification under this Regulation is to develop a list of scenarios that may lead to an information security threat having an impact on aviation safety.

A threat scenario, in general, is characterised by the following:

— a threat source of the information security attack;

— an attack vector and a path through the organisation up to the asset;

— the security controls that would mitigate the attack;

— the consequence of the attack including the affected safety aspects.

Threat scenario identification guidance can be found in ED-202A Chapter 3.4. This is not the only source where guidance can be found, and the competent authority may refer to different guidance more appropriate for their application.

Additional methods to identify relevant threat scenarios

When conducting this analysis, both security and safety aspects should be coordinated throughout the process to ensure mutual understanding of the threat preventive measures and mitigations being applied. In the following Figure 2 the interactions between information security and aviation safety are depicted through a 'bow-tie' diagram that highlights the links between risk controls and the underlying management system.

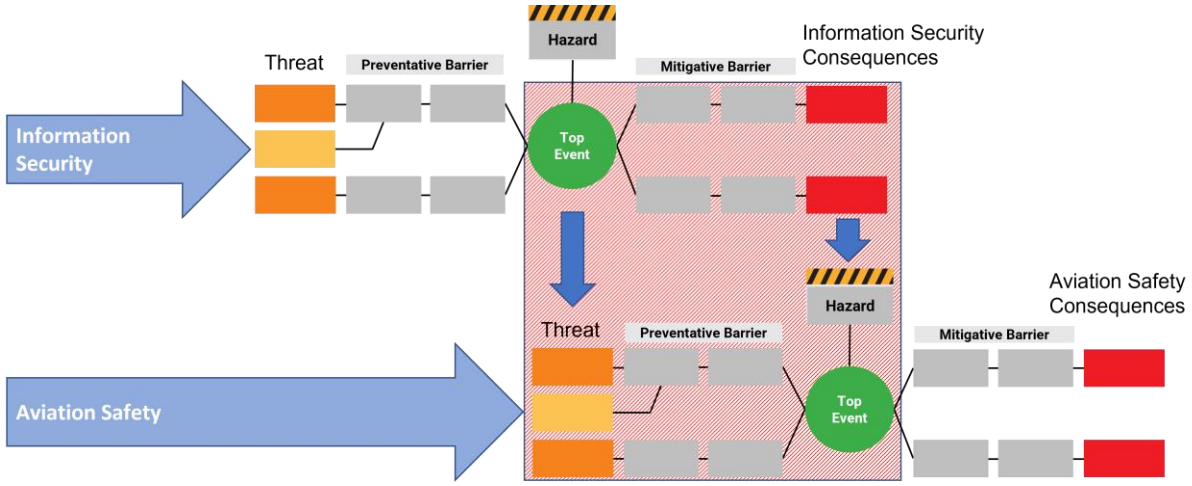

Figure 2: Interactions between information security and aviation safety risk management areas

Examples of threat scenarios

Threat catalogues may provide guidance and elements for the elaboration of threat scenarios that are relevant for the organisation. References can be found in ARINC 811 – Att. 3 – Tables 3-6 to 3-8 for the threat catalogue examples and other threat catalogue examples as they are provided by EU institutions. However, this is not an exhaustive list of examples; the identification of threat scenarios should therefore not be limited to those examples only. In addition, other relevant resources containing information on information security threats and the information security threat landscape should be consulted to support the risk assessment process with relevant inputs.

A set of examples of threat scenarios can be found in Appendix I.

AMC1 IS.AR.205(d) Information security risk assessment

The competent authority should take into account the following criteria when establishing compliance with the objectives contained in point IS.AR.205(d):

(a) The risk assessment performed under points IS.AR.205 (a), (b) and (c) should be reviewed at regular intervals, the periodicity being determined by the authority performing the assessment considering the criticality of the assets within the scope of the risk assessment, levels of post-assessment risk of the assets within the scope of the risk assessment and any customer or regulatory requirements. A higher criticality or level of risk will require more frequent review.

(b) The periodicity of risk assessment reviews should be documented by the competent authority and include the justification, date of approval and information about the risk owner.

GM1 IS.AR.205(d) Information security risk assessment

Risks are not static and will not stay the same forever. Risk assessments can be undertaken on different levels where one pursues a high-level risk assessment and another one a more granular approach to support the identification of changes and the need a for more detailed risk assessment. Risk assessments should be subject to regular reviews to:

(a) allow for continuous improvement of the quality of risk assessment;

(b) ensure efficiency and effectiveness of risk controls and mitigations in both their design and operation;

(c) review plans and actions for risk treatment;

(d) update any changes which may require revision of risk treatments and priorities;

(e) maintain an overview of the complete risk picture; and

(f) identify any emerging risks.

The objective of a risk assessment review is to re-evaluate the risks, their likelihood and impact. One possible approach is to tier risk assessments with a higher-level risk assessment which is used to identify changes. In a next step, the higher-level risk assessment could allow the identification of the detailed risks that should be reviewed.

Risk assessment reviews should involve the risk owners, project teams and other stakeholders as applicable.

GM2 IS.AR.205(d) Information security risk assessment

Risk assessments should be reviewed regularly and may be reviewed more or less frequently depending on whether the assets within the scope of the risk assessment are of sufficient criticality or complexity, the levels of post-assessment risk warrant more frequent analysis, or to adhere to any regulatory or customer requirements. The criticality of assets can be determined through an assessment of the impacts of a loss of the assets i.e. an impact assessment.

The periodicity of risk assessment reviews should be documented by the authority in security manuals, processes or procedures and should align with wider change management activities and management reviews of information security. Further guidance on criteria and frequency of risk assessment review can be found in EUROCAE ED-201A Chapter 4, as well as ED-205A Chapter 3.2 (for ATMS/ANS).

Risk assessments should also be reviewed when:

(a) there is a change in the elements subject to information security risks as identified in IS.AR.205(a); changes may be identified through management reviews or change control processes. Change in the elements will include:

— additions to or removals from elements within the scope of the risk assessment (as identified in IS.AR.205(a));

— changes to design or configuration of elements within the scope of the risk assessment (as identified in IS.AR.205(a)) that have the potential to alter the risk assessment outcomes; or

— changes to values, which would potentially trigger changes to impact levels, of elements within the scope of the risk assessment (as identified in IS.AR.205(a));

(b) there is a change in the interfaces between the authority and other parties with which the authority shares information security risks or relies upon to mitigate information security risks (e.g. supply chains, service providers, cloud providers and customers), as identified in IS.AR.205(b), or between the system within the scope of the risk assessment and any other interconnected systems, or in the risks notified to the authority by other parties, as identified in IS.AR.205(b), or owners or managers of the other systems including:

— establishment of new interfaces;

— removal of existing interfaces;

— changes to existing interfaces that would have the potential to alter the risk assessment outcomes.

Note: Some organisational or system interconnections may be with entities that are not within the scope of this Regulation as defined in Article 2 and therefore are not subject to the requirements of Part-IS. Where this is the case, these entities should be informed of their responsibility to report such changes as listed above, through contractual arrangement and reporting requirements between the affected entities on a case-by-case basis and where applicable;

(c) there is a change in the information or knowledge used for the identification, analysis and classification of risks including:

— changes to threats and their values or addition of new threats that have not previously been assessed;

— changes to vulnerabilities or addition of new vulnerabilities that have not previously been assessed;

— changes in impacts or consequences of assessed threats or vulnerabilities;

— changes in aggregation of risks that may result in unacceptable levels of risks;

— changes or improvements in the risk management process, risk assessment approach and related activities;

— changes or improvements in the treatments of risks;

— changes in the criteria used to determine acceptance and treatments of risks;

(d) there are lessons learned from the analysis of information security incidents including:

— understanding of why and how incidents have occurred; and

— reviewing all types of incidents including those due to external factors, technical reasons, human factors or processes. For human factors a distinction can be made between malign and benign actions.

Evidence of risk assessment review should be documented and should include:

— evidence of approval of the review by the designated risk owner; and

— the rationale behind or basis for the risk owner's approval of the review.

Such evidence may comprise, but is not limited to:

— reports which constitute a form of documentation to track information security risks potentially impacting an authority;

— the documentation of the information security risk assessment;

— exerts from a business or security risk register.

Note: In some cases the information contained in the risk report, security cases or risk register may be sensitive to the authority and may need to be redacted in agreement with the Agency, or a method may need to be established for the Agency to view such content on the authority's systems.

GM1 IS.AR.210 Information security risk treatment

The risk management options referred to in IS.AR.210(a) may be used in combination; however, there is no obligation for the competent authority to do so.

The application of risk treatment options under points IS.AR.210 (a)(1) and (a)(2) lead to the introduction of security measures, often referred to as security controls.

GM2 IS.AR.210 Information security risk treatment

For each identified risk, the competent authority should define the specific risk treatments, methods or resources that will be used over the life cycle of each asset to:

— manage risk reduction;

— monitor and maintain each asset;

— update and fulfil activities for configuration management;

— manage supply chain;

— manage contracted services or service provider.

The review of risk treatment measures should include life cycle considerations which are introduced by equipment, procedures and personnel.

A risk treatment plan as an outcome of the risk management process should include a prioritisation of risks, the corresponding information on the objectives and means for risk treatment to reach an acceptable level of risk, as well as agreed timelines specifying when responsible personnel should have implemented the risk treatment measures. The timelines for the implementation of a risk treatment measure should be agreed by the personnel responsible for the implementation and shall be communicated to and accepted by the person identified in IS.AR.225(a) /IS.I.OR.240(a) or delegated person(s).

Any subsequent implementation delay, together with its cause, reason, rationale or necessity, should be documented in the risk treatment plan. The delay should also be communicated to the Agency in case the materialisation of risk would lead to an unsafe condition. The delay is also subject to the acceptance by the person identified in IS.AR.225(a). The identified person may condition such acceptance on the implementation or availability of compensating controls or reactive measures to monitor, early detect and timely respond to the materialisation of the risk in treatment. In order to timely respond, the incident response team may be informed to trigger their preparedness.

The risk treatment plan can act as a means of communication with the Agency to demonstrate effective treatment of unacceptable risks. Similarly, this plan can be utilised to communicate to interfacing organisations how shared risks are controlled.

In accordance with IS.AR.205(d), a regular or conditional review of the risk assessment is necessary, and this includes the review of the risk treatment measures developed under IS.AR.210(a) to identify whether they are still effective or they require adaptations.

In addition, the competent authority should also consider the potential impact on the effectiveness of risk treatment measures where a shared information security risk may arise as a result of the interaction between interfacing entities (see IS.AR.220 and relevant AMC).

AMC1 IS.AR.210(a) Information security risk treatment

The competent authority should take into account the following criteria when establishing compliance with point IS.AR.210(a):

(a) the measures developed under point IS.AR.210(a)(1) should be implemented according to a risk treatment plan with defined, risk-based priorities, objectives and agreed timelines and owners;

(b) identification and association of the life cycle considerations to ensure continuous effectiveness of the security measures including exchange of data with other entities;

(c) the authority should review and update the risk assessment, according to IS.AR.205(d), to evaluate whether the measures developed under point IS.AR.210(a) do not introduce new unacceptable risks or modify existing risks into a way that they become unacceptable.

Risk treatment should be documented in the risk registry even if the risk has been avoided.

GM1 IS.AR.215 Information security incidents – detection, response and recovery

Without prejudice to the definition of 'information security event' in Article 3, those events that indicate the potential materialisation of unacceptable risks include both occurrences (i.e. anything that causes harm or have the potential to cause harm) and discovery of vulnerabilities. In fact, information security risks are associated with the potential that threats will exploit vulnerabilities, therefore the discovery of an exploitable vulnerability is an information security event.

In light of this, in the context of this Regulation:

— detection activities required under IS.AR.215(a) include vulnerability discovery;

— response activities required under IS.AR.215(b) include vulnerability management.

AMC1 IS.AR.215(a) Information security incidents – detection, response and recovery

DETECTION

When complying with the requirement in IS.AR.215(a), the competent authority should define and implement a strategy to detect information security events having an impact on safety.

This should be done in a way to ensure that at least the detection strategy is able to cover all known information security threats to their assets that may materialise in a safety hazard having an unacceptable consequence.

DETECTION STRATEGY

In order to determine the scope of the event detection, the competent authority should:

(a) identify a list of threat scenarios from the risks identified under IS.AR.205;

(b) identify, as a minimum, those assets that contribute to the scenario(s) that may materialise in an unsafe condition. For this identification of the assets, the measures introduced under IS.AR.210 should also be considered.

Note: The contribution of an asset to the threat scenario and the materialisation of an unsafe condition should be assessed by considering the whole functional chain. In some cases, the asset may be at the end of a functional chain and if it is compromised, the effect on safety is direct and may be immediate; conversely if the asset is far from the end of functional chain and it is compromised, the effect should propagate and may be delayed.

GM1 IS.AR.215(a) Information security incidents – detection, response and recovery

DETECTION STRATEGY

When developing the detection strategy, for those items within the scope of event detection, the competent authority should define the conditions that trigger a process that, for example, would require personnel intervention and further analysis. These conditions on the items may be defined using elements from:

(a) expected functional baseline: engage in the identification of deviations from the expected functional operation of the system (excluding security functions/controls);

(b) expected security baseline: engage in the identification of deviations from the expected information security operation of security controls.

These conditions should consider both abnormal behaviour and substantial deviations from the baselines and relevant correlation of multiple independent events.

Further guidance on the objectives for the establishment of a detection strategy can be consulted in EUROCAE ED-206 – Chapter 4.

AMC1 IS.AR.215(b) Information security incidents – detection, response and recovery

(a) INCIDENTS

The competent authority should take into account the following aspects when establishing compliance with the objectives contained in point IS.AR.215(b) relative to incidents:

(1) Preparation of procedures and delineation of roles and responsibilities to manage timely, effective, and orderly response to any relevant security incidents.

(2) The response procedure should:

(i) consider the warnings, unitary or combined, from IS.AR.215(a)(2), and assess their potential impacts on aviation safety;

(ii) establish, in accordance with IS.AR.215(b)(2), a containment strategy for each asset category in relation with the potential worst-case effect and the mission constraints, and provide criteria indicating when the attack is contained;

(iii) define, in accordance with IS.AR.215(b)(3), the acceptable impact on safety and security of each asset in scope when they fail due to the materialisation of a threat scenario.

(3) The response time should be commensurate with the impact level assessed in (2)(iii).

(4) The response measures implemented under IS.AR.215(b) should be based on the response procedure referred to in the above point (a)(2) and it should, in particular, consider the following:

(i) the maximum acceptable safety level degradation of the items within the scope of the threat scenario;

(ii) the actions, such as resistance, containment, deception and control of the possible ways systems can fail, which will contribute to achieving the acceptable safety level degradation identified in point (i) while minimising impact on operations;

(iii) the resources required to implement the actions specified in point (ii).

(b) VULNERABILITIES

The competent authority should take into account the following aspects when establishing compliance with the objectives contained in point IS.AR.215(b) relative to vulnerabilities:

(1) Establishment of a vulnerability management plan defining procedures, roles and responsibilities to manage quick, effective, and orderly response to any detected relevant vulnerabilities.

(2) The response measures implemented under point IS.AR.215(b) should be based on the maximum acceptable risk of the items within the scope of the vulnerability, considering the worst-case scenario of the vulnerability being exploited.

(3) The response time should be commensurate with the pre-triage done on the warnings and with the assessment of the potential impact of the vulnerability, if it is exploited.

GM1 IS.AR.215(b) Information security incidents – detection, response and recovery

An attack is considered contained (i.e. it is not spreading any further) when the boundaries of the incident have been identified and the threat does not propagate beyond these boundaries. Further guidance can be found in EUROCAE ED-206 – Chapter 5.

Guidance about vulnerability strategy can be found in EUROCAE ED-206 – Chapter 3.4.2.

AMC1 IS.AR.215(c) Information security incidents – detection, response and recovery

When complying with the requirement in IS.AR.215(c), the competent authority should develop an incident recovery procedure including at least the following:

(a) a list of those assets that enable safe operations, as well as the dependencies among them, this constituting the scope of the recovery;

(b) a description of the process with the necessary priority actions to be executed for a return to a safe and secure state for the assets within the scope of the recovery;

(c) the resources required to execute the actions defined in point (b) to ensure that these resources are readily available after an incident has occurred;

(d) the objectives for recovery time that should be set in relation to the safety criticality of the assets within the scope of the recovery.

GM1 IS.AR.215(b)&(c) Information security incidents – detection, response and recovery

RECOVERY OBJECTIVES AND TIMING

This Regulation focuses on incidents that have an impact on safety and requires response and recovery measures to be in place to ensure that operational safety remains above a minimum acceptable level.

The level of operations and safety may be interrelated, so in some cases when the level of operations is compromised by an information security incident and drops, the level of safety does the same. This is, for instance, the case of air traffic control; if air traffic services are reduced or became unreliable, the safety of flights is reduced too.

However, in other cases the relation between the level of operations and safety may be the inverse, or they may be decoupled, so when an incident occurs and the operations drop, the level of safety is

preserved. One example is the compromise of software loading process on board the aircraft. In this case a detected incident followed by the decision to interrupt the software loading operations would preserve the existing level of safety.

The following Figure 1 depicts a conceptual framework that may be considered for the definition of the response and recovery objectives, including the recovery time. It represents, in the worst-case scenario, how the expected level of operational safety (safety level) for a process or an activity may vary over time when a security incident occurs. In this scenario, the safety level first is reduced by the incident and then it degrades as long as the time passes. The figure also shows the expected effect that mitigations and controls should have, respectively: in containing the operational safety drop as soon as an incident occurs, and in improving the recovery, i.e. the return to the expected safety level.

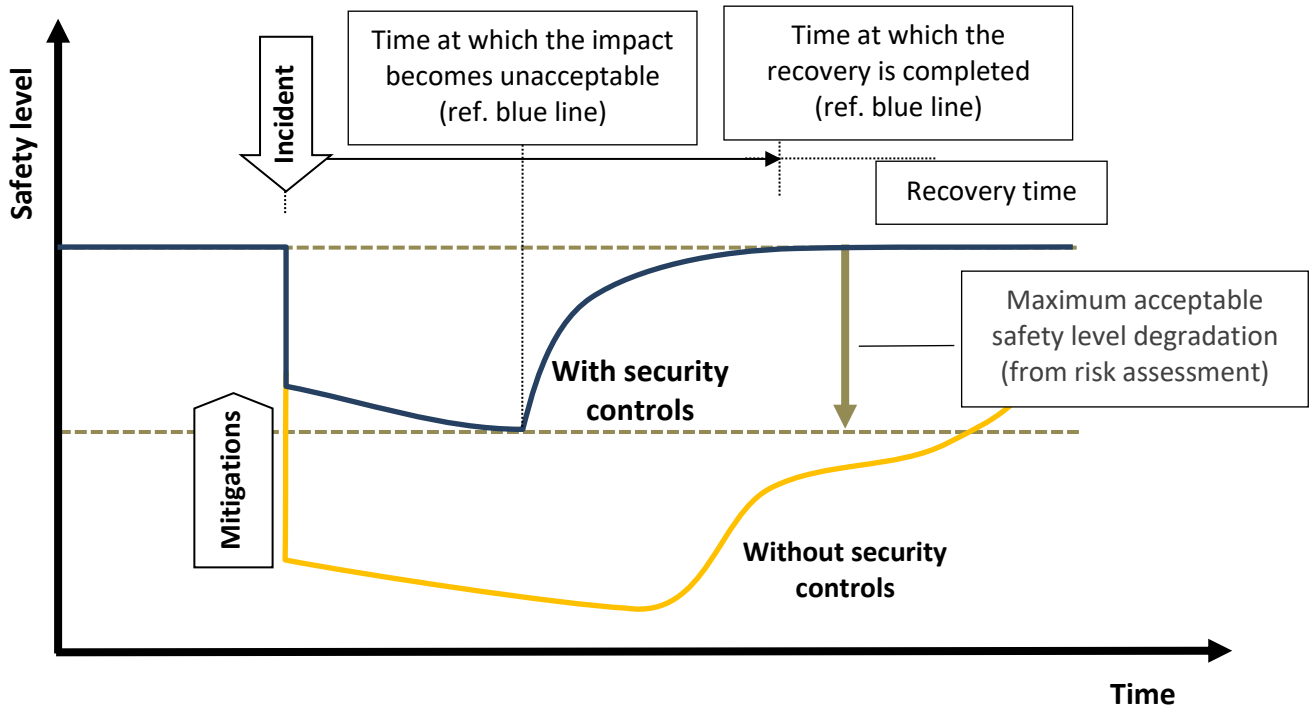

Figure 1: Conceptual framework for the definition of the response and recovery objectives

As mentioned, there might be different relations between the level of operations and safety that would lead to a different representation of the above figure. In certain cases, an incident may have a delayed effect on the safety level (e.g. a compromised development environment) as depicted in Figure 2, or it may have no impact if properly controlled, as in the case of the compromised software loading process mentioned before that is depicted in Figure 3.

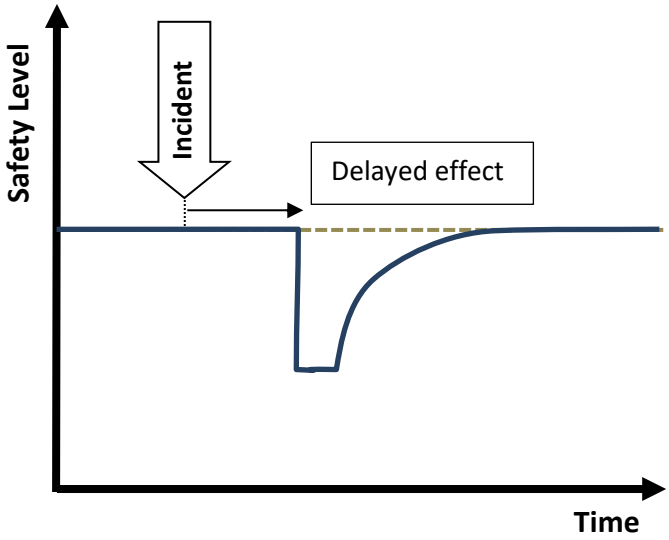

Figure 2: Incident with a delayed effect on safety

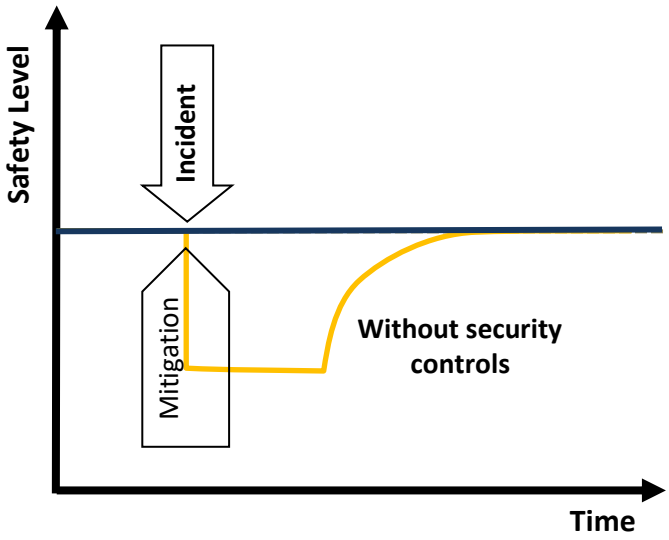

Figure 3: Incident with a fully mitigated effect on safety

Moreover, it should be noticed that there might be different ways the same incident can be dealt with since there are several factors that may affect safety.

In practical terms, the objectives for recovery time under AMC to IS.AR.215(c) may be expressed as a list of resources and services to be restored by order of priority, within the scope of the recovery. Guidance about objectives for recovery time can be found in EUROCAE ED-206 – Chapter 7.3.5.

GM1 IS.AR.215(c) Information security incidents – detection, response and recovery

A recovery procedure or recovery plan should describe incident recovery actions and the internal or external resources that are involved (e.g. staff, IT, buildings, providers, BCM). Guidance about incident recovery plan can be found in ED 206 – Chapter 7 – Recover.

The resources required to apply the recovery measures should be available in order to implement recovery actions in a timely manner after an incident has occurred. Those resources may be internally available or provided by contracted organisations as foreseen by IS.AR.220. The contracting of recovery activities should be established before an incident occurs (proactive) and the contract should include provisions for the contracted party to react in a timely manner.

The return to a safe and secure state may initially require emergency measures, which are actions that are initiated based on the best information available at the time, before a complete understanding of the situation is achieved and these measures can potentially degrade the level of service or functionalities. The return to a safe and secure state should be evaluated against the initial risk assessment and may only temporarily differ from the normal operational conditions. However, any increase of residual risk and the duration of this risk increase, i.e. due to the implementation of emergency measures, should be documented and accepted at the right level of accountability.

The recovery activities mentioned herein may also be the outcome of the response to incidents for which the authority has received information that requires the implementation of adequate measures in order to react to security incidents or vulnerabilities with a potential impact on aviation safety.

In such context the authority may not have a process or a recovery plan covering the specific

occurrence. Therefore, the definition from the authority of a specific recovery plan and its approval by the competent agency is usually required.

GM1 IS.AR.220 Contracting of information security management activities

The objectives of point IS.AR.220 are:

(a) to protect critical and sensitive information and assets when being handled by contracted organisations (including organisations in the supply chain) either at their facilities or organisation facilities, or when being transmitted between the organisation and contracted organisations, or being remotely accessed by contracted organisations.

(b) to prevent information security risks from being introduced through products and services developed or provided by the contracted organisations to the organisation, in the frame of the provision of information security management activities.

(c) to ensure that information security risks are managed throughout all the stages of the relation with the contracted organisations.

GM2 IS.AR.220 Contracting of information security management activities

The contracting of information security management activities is a means to allocate tasks from the contracting organisation to third parties (contracted organisations). The contracting organisation remains accountable for compliance with this Regulation.

GM3 IS.AR.220 Contracting of information security management activities

EXAMPLES

Examples of security management activities required under IS.AR.200 that can be contracted.

IS.AR.200 activity	Contracted activity
a-1: establishes a policy on information security describing the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;	Security policy drafting and consultancy
a-2: identifies and reviews information security risks in accordance with point IS.AR.205;	Identify activities, facilities and resources. Identify interfaces with other organisations which could be exposed to information security risks. Perform risk analysis or part of it, e.g. identify and classify information security risks.

IS.AR.200 activity	Contracted activity
a-3: defines and implements information security risk treatment measures in accordance with point IS.AR.210;	Define, develop and implement measures. Verify the initial and the continued effectiveness of the implemented measures (e.g. Red-Team/Blue-Team exercises, penetration testing, vulnerability scanning, etc.). Communicate to the involved stakeholders the outcome of the risk assessment and their responsibilities as part of the risk treatment process.
a-4: defines and implements, in accordance with point IS.AR.215, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety and responds to, and recovers from, those information security incidents;	Define, develop and implement measures to detect events. Define, develop and implement measures to respond to any event conditions. Define, develop and implement measures aimed at recovering from information security incidents.
a-5: complies with the requirements contained in point IS.AR.2220 when contracting any part of the activities described in point IS.AR.200 to other organizations;	
a-6: complies with the personnel requirements contained in point IS.AR.225;	Contracted organisation to ensure that sufficient personnel is on duty to perform the activities related to this Regulation Define, develop and deliver adequate training to achieve the competencies required by the staff. Perform pre-employment checks.
a-7: complies with the record-keeping requirements contained in point IS.AR.230.	Define, develop and implement secured archiving. Provision of secure data centre (as a service) Provision of records updates
a-8: monitors compliance of its own organisation with the requirements of this Regulation and provides feedback on findings to the person referred to in point IS.AR.225(a) to ensure effective implementation of corrective actions.	Compliance monitoring including the execution of independent audits
a-9: protects the confidentiality of any information that the competent authority may have related to organisations subject to its oversight and the information received through the organisation's external reporting schemes established in accordance with point IS.I.OR.230 and point IS.D.OR.230 of Part-IS.	Define, develop and implement solutions to protect the confidentiality of any information.

IS.AR.200 activity	Contracted activity
a-10: notifies the Agency of changes that affect the capacity of the competent authority to perform its tasks and discharge its responsibilities as defined in this Regulation.	
a-11: defines and implements procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other competent authorities and agencies, as well as organisations subject to this Regulation, to conduct effective security risk assessments relating to their activities.	
b: In order to continuously meet the objectives described in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.AR.235.	Execute independent effectiveness and maturity assessments. Define, develop and implement the necessary improvement measures.
c: The competent authority shall document all key processes, procedures, roles and responsibilities required to comply with point IS.AR.200(a) and establish a process for amending this documentation.	Production of documentation to detail all key processes, procedures, roles and responsibilities required to comply with point IS.AR.200(a) (e.g. information security policies, general description of the staff, procedures to specify compliance). Define, develop and implement processes for approving amendments and changes.

AMC1 IS.AR.220 Contracting of information security management activities

(a) OVERSIGHT OF THE CONTRACTED ORGANISATION

In order to demonstrate proper oversight of the contracted organisation, the competent authority should have:

(1) a process to ensure compliance with the provisions regarding contracted activities contained in this Regulation;

(2) a structured process to follow the expected execution of the contract that includes:

(i) definition and agreement of the scope of the activities;

(ii) definition and review of key performance indicators;

(iii) reaction to deviation from contractual obligations;

(iv) performance of audits, according to predefined scope and objectives, with the aim of evaluating operational and associated assurance activities.

(b) MANAGEMENT OF THE RISKS ASSOCIATED WITH THE CONTRACTED ACTIVITIES

In order to demonstrate proper management of the risks associated with the contracted activities, the organisation should meet the following criteria:

(1) A prior assessment of the suppliers is conducted before outsourcing any security management activities. The assessment should evaluate suppliers' competencies, sustainability as well as qualifications in relation to the activities to be contracted.

(2) There is an assessment of the risks associated with the provision of the contracted activities that has been agreed between the organisation under Part-IS and the contracted organisation.

(3) The organisation establishes and maintains an information security focal point with the contracted organisation.

GM1 IS.AR.220 Contracting of information security management activities

RISK ASSESSMENT ASSOCIATED WITH THE PROVISION OF THE CONTRACTED ACTIVITIES

The risk assessment should take into account the maturity level of the contracted organisation, and should consider the following:

(a) Identification and assessment of critical and sensitive information and assets that may be shared with, or provided by, external suppliers;

(b) Identification of the information security requirements of the authority that are applicable to the contracted organisation;

(c) Evaluation, by means of a supplier assessment, of the ability of the contracted organisation (both existing and new contracted organisations) to meet the information security requirements of the authority;

(d) Assessment of risks that may be introduced by the contracted organisation.

This agreed risk assessment should also include the roles and responsibilities of the parties (i.e. contracting and contracted organisation).

GM2 IS.AR.220 Contracting of information security management activities

AUDIT OF CONTRACTED ORGANISATIONS

The following aspects should be considered by the authority when auditing a supplier contracted to perform security management activities:

— the scope of the audit as well as the objective should be limited to processes, resources and data used for the execution of Part-IS contracted activities;

— compliance and/or implementation audits should be done at the authority's discretion;

— findings identified during an audit shall be addressed through a remediation plan with a time frame to be validated by the authority.

GM1 IS.AR.225 Personnel requirements

The objectives of the requirements contained in point IS.AR.225 are:

(a) to ensure that an effective organisational structure is in place in order to comply with the requirements of this Regulation;

(b) to provide trust to other organisations with whom they share risks.

AMC1 IS.AR.225(a) Personnel requirements

The person referred to in point IS.AR.255(a) is normally intended to be a manager in the authority who, by virtue of his or her position, has overall (including financial) responsibility for information security. This person is not necessarily required to be knowledgeable on technical matters; however, he or she should be aware of the overarching objectives of this Regulation and its implications for the authority. The authority should make sure that this person has direct access to the Director General (or equivalent) and has the necessary funding allocation for the activities under this Regulation.

GM1 IS.AR.225(a) Personnel requirements

The person referred to in point IS.AR.255 (a) should be capable of managing the authority's cybersecurity strategy and its implementation to ensure the achievement of the objectives described in Article 1. According to the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022, this person may be described for instance as: (Chief) Information Security Officer, Cybersecurity Programme Director or Information Security Manager.

AMC1 IS.AR.225(b) Personnel requirements

PERSONNEL SUFFICIENCY

To determine the sufficiency of the personnel, the following elements should be taken into consideration:

— the organisational structures, policies, processes and procedures subject to information security management;

— the amount of coordination required with other organisations, contractors and suppliers;

— the level of risk associated with the activities performed by the authority.

GM1 IS.AR.225(b) Personnel requirements

PERSONNEL SUFFICIENCY

For the purpose of this Regulation, personnel refers to the combination of the personnel directly employed by the authority, as well as the personnel contracted as specified in IS.AR.220.

The activities reported in Annex II 'Main tasks stemming from the implementation of the Part-IS Regulation' should be considered when establishing the organisational structure necessary to comply with the requirements of this Regulation.

AMC1 IS.AR.225(c) Personnel requirements

NECESSARY COMPETENCE

To determine the competence needed by the personnel performing the activities, the following elements should be taken into consideration:

— work roles and the associated tasks;

— required knowledge, skills and abilities.

As part of the process to ensure that personnel maintain the necessary competence, the Member

State, or the competent authority on its behalf, should:

— assess the personnel qualifications and experience with respect to the required competence for the assigned work roles to identify gaps;

— align the personnel qualifications and experience to the expected competence by either organising adequate learning programmes for existing personnel members, recruiting new resources, or a combination thereof.

GM1 IS.AR.225(c) Personnel requirements

TRAINING PROGRAMME

A training programme should start from the identification of the competence required by the personnel for each role, followed by the identification of the gaps between the existing competence and the required one.

In order to develop the list of competencies, an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the NICE (National Initiative for Cybersecurity Education) based on the NIST Cybersecurity Framework (NIST CF).

The competencies listed in Appendix II stemming from the NIST CF that are mapped to the main tasks of this Regulation may be used to establish a baseline to identify the aforementioned competence gaps.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the authority's needs considering the size, scope, required competencies, and complexity of the organisation.
Finally, as information security/cybersecurity evolves due to the rise of new threats, the authority should periodically review the adequacy of the training programme.

AMC1 IS.AR.225(d) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Regarding any assigned role and task, the authority should specify all information security responsibilities an employee has in a clear and transparent manner.

As part of this, the employee should acknowledge, in a traceable and verifiable manner, understanding of the instructions received as well as the expected roles and responsibilities.

GM1 IS.AR.225(d) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Acknowledgement of receipt such as a valid electronic or wet signature, confirmation email, etc., is a traceable proof of acceptance.

AMC1 IS.AR.225(e) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

(a) The establishment of a person's identity should be determined on the basis of documentary evidence.

(b) Regarding the establishment of trustworthiness, a standard level of vetting, which includes the verification of:

(1) employment, education and any gaps during at least the preceding 5 years;

(2) criminal records in all states of residence during at least the preceding 5 years,

should always be completed, taking also into account the relevant national laws and regulations.

(c) In case the information system and data to be accessed have been associated with a high severity of the safety consequences in accordance with AMC IS.AR.205(b)(3), an enhanced level of vetting should be performed for persons having administrator rights, or unsupervised and unlimited access, or having been otherwise identified in the risk assessment in accordance with IS.AR.205.

(d) An enhanced level of vetting should include the verification, to be completed in accordance with relevant national laws and regulation, of:

(1) employment, education and any gaps during at least the preceding 5 years.

(2) criminal records in all states of residence during at least the preceding 5 years;

(3) intelligence and any other relevant information (e.g. available to the national competent authorities) that is considered to be relevant for the suitability of a person to work in a function which requires an enhanced level of vetting.

GM1 IS.AR.225(e) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

Enhanced level of vetting may be used when already existing controls or mitigation measures for risk treatment identified during the risk analysis relies on organisational/operational procedures. Thus, enhanced level of vetting is needed for personnel who operates such measures. For instance, correct configuration and administration of information technologies, database operations, security monitoring, etc.

Intelligence and any other relevant information should be gathered by screening and analysing public sources such as social media and websites.

Standard and enhanced background check, as defined in Regulation (EU) 2015/1998, are suitable for the standard and enhanced level of vetting respectively. However, it should be noted that the standard and enhanced levels of vetting referred to in AMC1 IS.AR.225(e) do not constitute compliance with the provisions on background checks as defined in Regulation (EU) 2015/1998.

GM1 IS.AR.230 Record-keeping

Records are required to document results achieved or to provide evidence of activities performed. Records become factual when recorded and cannot be modified. Therefore, they are not subject to version control. Even when a new record is produced covering the same issue, the previous record remains valid.

AMC1 IS.AR.230(a)(1)(iv)&(a)(4) Record-keeping

When complying with the requirements under points (a)(1)(iv) and (a)(4), the competent authority should establish a data retention policy defining procedures to:

(a) manage relevant security data files;

(b) establish the periodical assessment of their content; and

(c) define the criteria to allow deletion of events when the objective of requirement (a)(4) is no longer met.

GM1 IS.AR.230(a)(1)(iv)&(a)(4) Record-keeping

The objective of the requirement (a)(1)(iv) is to ensure detection of possible indication of compromise or vulnerabilities which are not obvious by normal operation (e.g. previously unknown situations), while the objective of (a)(4) is to allow the necessary flexibility to control the volume of the stored security events.

Records of information security events include those events identified within the scope of the detection activities under IS.AR.215(a), as well as other security data produced by assets that have been identified under IS.AR.205.

A data retention policy clarifies what information should be stored or archived and for how long. Some guidance about data retention can be found in EUROCAE standard ED-206 Chapter 2.6.

Once a data set completes its retention period, it can be deleted or moved as permanent historical data to a secondary or tertiary storage.

AMC1 IS.AR.230(c)&(d) Record-keeping

When complying with the requirements under points (c) and (d) for all the records required by points IS.AR.230 (a) and (b), the competent authority should consider the following:

(a) Records should be kept in paper form or in electronic format or a combination of both media. The records should remain accessible whenever needed within a reasonable time and usable throughout the required retention period. The retention period starts when the record has been created.

(b) Records data integrity and availability should be protected in consistency with protection of corresponding operational data, and as such, should be within the scope of the ISMS.

(c) Backup/archiving systems should be protected against unauthorised access (i.e. data leakage attempts against personal data/modification of records) and thus should have security measures implemented in consistency with the level of cyber risk associated with them.

(d) Once records shall not be retained anymore, the destruction of records and decommissioning of assets used for their storage should be implemented appropriately.

GM1 IS.AR.230(c)&(d) Record-keeping

RECORDS ACCESSIBILITY THROUGHOUT THE RETENTION PERIOD

It is recommended to follow best practices for data retention and backup strategies, such as using automated backup tools, segregation, or geographical separation of backup storage location(s), and to consider offline backups to prevent ransomware risks. These criteria should be considered also when record-keeping is contracted to service providers with distributed resources.

Special attention should be paid to significant hardware and software changes, ensuring that stored digital records remain accessible and readable (e.g. file system, application file format, forward compatible database versions, etc.). Paper-based information needs to be archived in an adequate environment, in which records are protected against long-term degradation factors (e.g. heat, light, humidity).

RECORDS DATA INTEGRITY AND PROTECTION FROM UNAUTHORISED ACCESS

A commonly used method to achieve authenticity and integrity protection is the use of digital signatures at document level. Digital signatures can be added to the document's file (e.g. PDF) to ensure that a record has not been modified by someone other than its author (integrity) and that the author is who is expected to be (authenticity).

Moreover, to prevent unauthorised access, a record can be protected with a password at file level. Commercial applications feature built-in basic password protection functions for their file formats. Access protection can also be achieved by protecting the environment where the individual records are stored (e.g. access protection on databases, file shares, directories, etc.).

AMC1 IS.AR.235 Continuous improvement

The continuous improvement process (CIP) as required by IS.AR.200(b) should aim to continuously improve the effectiveness, suitability and adequacy of the ISMS. This should be achieved by a proactive and systematic assessment of the ISMS and all of its elements including its maturity. The assessment should take into account the outcomes and conclusions of other information security and assurance processes including audits, management reviews, evaluation of performance, effectiveness and maturity, as well as the outcomes of the derived corrective actions and corrections.

The steps to be performed should be at least the following:

(a) Identification of improvement opportunities based on the outcomes of the assessment of the ISMS with respect to its suitability, effectiveness, adequacy and, if deemed necessary, efficiency, as well as any other suggestion for improvement. The assessment should consider performance indicators which reflect its processes and elements and the defined objectives for effectiveness and maturity;

(b) Evaluation of the identified opportunities regarding cost-benefit, absence or reduction of undesired effects and achievement of the targeted objectives and intended outcomes;

(c) Proposal on the evaluated improvement opportunities to the management and recommendation of actions to support their review and decision-making;

(d) According to the decision taken under point (c) above, planning, development and implementation of actions and changes to the ISMS, its processes or elements to achieve the improvements;

(e) Evaluation of the effectiveness of the implemented actions and ISMS changes as well as, as applicable, verification that the root cause of identified deficiencies has been eliminated;

(f) Documentation of the management decisions as well as the planned and implemented actions and ISMS changes, their results and effectiveness.

The management should assess and review the outcomes of the CIP at planned intervals to ensure the continuing effectiveness, adequacy and suitability of the ISMS, to decide on the prioritisation of the implementation of actions and changes, as well as to revise or set new objectives, or targets for continuous improvement.

GM1 IS.AR.235 Continuous improvement

Point IS.I.AR.235 covers assurance processes for the ISMS in a manner that can be considered equivalent to the safety assurance in ICAO Doc 9859 'Safety Management Manual (SMM)', which includes performance monitoring and measurement, management of change and continuous improvement of the SMS.

In this Regulation:

— IS.AR.235(a) addresses, using adequate performance indicators, the effectiveness and maturity assessment of the ISMS;

— IS.AR.235(b) addresses the improvement measures, i.e. corrections and corrective actions, for the deficiencies detected in IS.AR.235(a) and the continuous improvement process.

Similar provisions for continuous improvement are foreseen in other information management systems such as ISO 27001 (see Appendix II to this document).

The context and risk environment of competent authorities are never static and therefore require a dynamic adaptation, evolution and change of the entity's objectives, architectures, organisational structures and processes to maintain the information security risks at an acceptable level. Consequently, the ISMS should be considered as an evolving and learning part/element of the entity which needs to be continuously monitored and improved to ensure alignment with the entity's safety objectives and effectiveness.

The CIP aims to continuously improve the effectiveness, suitability, adequacy and, if deemed necessary, the efficiency of the ISMS. An entity may integrate the Part-IS CIP in some other already operated CIP and may apply methods such as Plan-Do-Check-Act (PDCA) Cycle or Define-Measure-Analyse-Improve-Control (DMAIC) (see also GM1 IS.AR.200).

The CIP is based on a proactive and systematic assessment of the ISMS and all its elements including the information security processes and controls driven by the ISMS. The assessment should be carried out against organisational targets for desired levels of performance, effectiveness, and maturity. These targets, besides ensuring the achievement of compliance with the requirements under this Regulation, may also aim to include objectives established by the entity's policy or standards and by management decisions.

The above-mentioned assessment is based on the outcome of performance evaluations, audits, risk and incident processes, as well as already applied corrective actions and corrections. Some factors that should be considered when performing the assessment are the following:

— **Adequacy** refers to whether the system uses industry standards for information security in a sufficient manner with regard to compliance with the requirements of this Regulation.

— **Effectiveness of the ISMS** and the effective implementation of processes and controls driven by the ISMS is assessed by analysing whether:

  — The information security risks are managed to achieve the safety objectives;

  — the intended outcomes of the ISMS are achieved, and the requirements or objectives are met;

  — all types of deficiencies, including failures, are managed to fulfil or correctly implement a requirement or control.

— **Efficiency** of the ISMS refers to the implementation of streamlined processes; however, efficiency improvements should not adversely impact effectiveness.

Identification of improvement opportunities

Improvement opportunities may be identified from the results of the CIP assessment or may be introduced as suggestions from other sources. The identification often involves deviations or corrective actions as well as ineffective processes or controls which are not remediated.

Suggestions for improvements stem from sources including:

— Risk management: the results of regularly conducted risk analyses and the subsequent risk treatment are a primary factor in improving the ISMS whereby the risk treatment process involves monitoring of the implemented security measures and evaluating their effectiveness.

— Performance & effectiveness evaluation: conclusions from (key) performance indicators, their measurement, analysis and continued monitoring as well as the result of the assessment of the effectiveness including the outcomes of the subsequently applied corrections and corrective actions

— Evaluation of maturity including the results of the subsequent corrections and corrective actions

— Lessons learned from security incident detection, handling and response process and a potential treatment of a root cause

— Results of (internal) audits may be used to verify whether the ISMS and controls within the audit scope meet the entity's requirements and to determine where there are potential areas for improvements.

— Review and evaluation by management, review of the current action plan, setting or revision of the objectives or decision on improvement opportunities and actions

— Entity's suggestion programme (suggestions for improvement), reviews, surveys or assessments with employees or feedback from suppliers or interfacing parties

Any outcome of this process should be documented. The resulting actions may be integrated into an overarching action plan which is centrally consolidated and periodically reviewed according to the

relevant policies. The resulting action plan may be further divided into a tactical, short-/mid-term action plan and a strategic, long-term action plan.

AMC1 IS.AR.235(a) Continuous improvement

(a) **ISMS EFFECTIVENESS EVALUATION**

When complying with IS.AR.235(a), the competent authority should have a process in place to monitor, measure, evaluate and review the effectiveness of its ISMS that defines:

(1) who monitors, measures, analyses and evaluates the results and takes accountable decisions;

(2) when the above steps should be performed;

(3) which methods for monitoring, measurement, analysis and evaluation are applied to ensure comparable and reproducible results.

The frequency of the assessments should be commensurate with the level of risk established under IS.AR.205.

The process to monitor, measure, evaluate and review the effectiveness of its ISMS referred to under AMC1 IS.AR.235(a) should include as a minimum:

(1) the gathering and retention of metrics of the activities, and additional information that could be useful for monitoring purposes;

(2) the analysis of the metrics in order to identify trends and deviations from predefined performance targets.

(b) **ISMS maturity evaluation**

The competent authority should assess the maturity of its ISMS using a suitable maturity model in order to identify areas for improvement to the ISMS. To do so, the competent authority should:

(1) define or adopt a maturity model which represents a set of important and relevant processes and capabilities that are expected to be implemented and maintained;

(2) for each assessed process or capability, ensure that the model defines criteria for the specific aspects, characteristics and effectiveness to be assessed and evaluated to determine a maturity level;

(3) define for each assessed process or capability its desired target maturity level.

(c) For each assessed security process or capability contained in the maturity model, the competent authority should:

(1) evaluate and justify the current maturity level;

(2) identify any area for improvement it should make to reach the targeted maturity level;

(3) collect and record the evidence regarding strengths and weaknesses of the implemented ISMS and its evaluated maturity.

GM1 IS.AR.235(a) Continuous improvement

(a) As general guidance, the elements of the ISMS that should be monitored, measured and evaluated should be, as a minimum:

(1) the risk assessment and treatment process (including risks at the interfaces with other entities);

(2) the management of non-conformities and corrective actions;

(3) the incident and vulnerability management;

(4) the personnel competence management.

(b) Existing maturity models for ISMS maturity evaluation

As general guidance, for the definition or the adoption of a maturity model (MM), the following existing models may be considered:

— Cybersecurity Capability Maturity Model (C2M2), version 1.1: this model was published by the US Department of Energy in 2014. It introduces the notion of Maturity Indicator Levels (MIL) ranging from 0 to 3, and addresses not only performance levels but also performance practices (under Approach Objectives and approach progression) as well as assurance practices (under Management Objectives and institutionalization progression).

— Systems Security Engineering – Capability Maturity Model (SSE-CMM): published by ISO as ISO 21827 in 2008. It focuses on engineering practices, much less on operational practices that are split in 11 'Security Base Practices', and 11 'Project and Organizational Base Practices'. It introduces the notion of five Capability Levels, from 'Performed Informally' to 'Continuously Improving'.

— NIST Cybersecurity Framework (NIST CF), version 1.1: published by NIST in April 2018. Although it is not proposed as a MM, the framework defines four 'Implementation Tiers', from 'Partial' to 'Adaptive', which are a qualitative measure of organisational cybersecurity risk management practices. It focuses on the functionality and repeatability of cybersecurity risk management.

— ATM Cybersecurity Maturity Model, edition 1: published in February 2019 by the EUROCONTROL NM for organisations in the ATM domain. Whilst not being designed for wider application, it can be adapted as necessary. It defines five maturity levels, ranging from 'Non-existent' to 'Adaptive' inspired by the 'Tier' terminology from the NIST CSF. In fact, the model is founded on NIST CSF, together with some elements of ISO 27001.

The following Table 1 maps the MM mentioned above to a hypothetical five-level MM.

Mapping with a five-level MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial	MIL 0	Non-Existent	Performed Informally	
Defined	MIL 1 (Initial)	Partial	Planned & Tracked	Partial
Implemented	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved		Adaptive	Continuously Improving	Adaptive

Table 1: Mapping matrix of an existing MM to a hypothetical five-level MM

AMC1 IS.AR.235(b) Continuous improvement

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

Based on an evaluation of the impact and extent of the deficiency and the potential consequences on the ISMS, the process should include as criteria for compliance:

(a) deciding on corrections and their implementation without undue delay in order to limit the impact of the deficiency and deal with its consequences as well as, as applicable, to control or eliminate it;

(b) deciding on the need for, and the implementation of, corrective actions to eliminate the cause and contributing factors of the deficiency based on a root cause analysis and an evaluation of actions remediating the cause aimed at being proportionate to the consequences and impact of the deficiency;

(c) verifying the implemented actions:

— to be effective and to result in acceptable residual risks;

— not to have unintended side effects leading to other deficiencies, new risks, or an ISMS not aligned with the applicable requirements; as well as

— for corrective actions, to effectively remediate or eliminate the root cause.

(d) reporting to and reviewing the identified deficiencies, action plan and results of the action taken with the person identified in IS.AR.225(a) and, as necessary, with other involved or affected roles and parties;

(e) documenting as evidence the detected deficiencies, the planned and implemented corrections and/or corrective actions with deadlines and responsible persons, the management feedback, the outcomes of the process step under point (c) above and, if necessary, the change decisions made for the ISMS itself.

GM1 IS.AR.235(b) Continuous improvement

The 'necessary improvement measures' referred to in IS.AR.235(b) refer to correction or corrective actions to eliminate deficiencies, or actions aimed at improving the effectiveness as well as the maturity of the ISMS.

A process satisfying the criteria defined in AMC1 IS.AR.235 should include the following aspects:

(a) identifying the extent, impact, context and triggers of the deficiency, evaluating it according to some established criteria, analysing potential consequences on the ISMS including a potential existence in other areas;

(b) deciding on corrections and their implementation to immediately limit the impact and manage the consequences of the deficiency as well as, as applicable, to control or eliminate it;

(c) deciding on corrective actions required to eliminate the (root) cause(s) of the deficiency that are proportionate to the consequences;

(d) reassessing the elements of the ISMS which may be affected by the implemented actions to ensure that no further risk is introduced;

(e) verifying the implemented actions referred to in AMC1 IS.AR.235(b);

(f) reporting to and reviewing the outcomes of the process steps with the management;

(g) documenting and evidencing the result of the process steps above.

GM IS.I.OR.200 Information security management system (ISMS)

An **information security management system (ISMS)** is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security aimed to protect the information assets in order to achieve the organisation's operational and safety objectives in a risk-managed, effective and efficient manner.

The ISMS applies an information security requirement analysis and an information security risk management process to decide on, and manage the selection, implementation and operation of controls over all architectural layers (governance, business, application, technology, data), (organisational, human, physical, technical) and the perspectives of governance, risk management and compliance (GRC) within the ISMS scope. The risk management process is based on an aviation safety risk assessment and the risk acceptance levels designed to effectively treat and manage risks with a potential impact on aviation safety caused by threats exploiting vulnerabilities of information assets in aeronautical systems, as depicted in Figure 1.

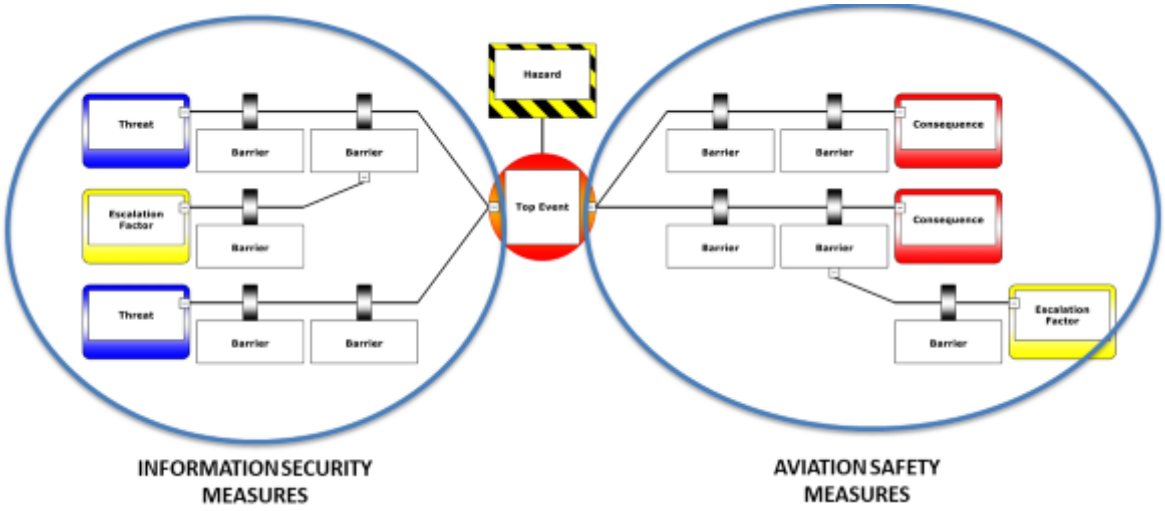

Figure 1: Bow-tie representation of management of aviation safety risks posed by IS threats

The ISMS in this Regulation should bring together the information security and aviation safety competencies in most of the processes, including, for instance, identifying critical systems, or threats, and assessing potential impacts on and risks to aviation safety.

ISMS implementation and maintenance

An ISMS as per this Regulation employs the perspectives of governance, risk and compliance, and an approach that combines the dimensions of safety risk and performance to determine the information security controls that are appropriate for and compliant with the specific context and can effectively provide the required level of protection to achieve the aviation safety objectives:

— **Governance** perspective refers to providing management direction and leadership aimed to achieve the entity's own overarching objectives:
  — leadership and commitment of the senior management defining and ensuring the close involvement of the management and a 'top-down' ISMS implementation
  — information security and safety objectives derived from, aligned and consistent with the entity's business objectives and monitored by, e.g. management reviews
  — information security policies stating the principles and objectives to be achieved
  — roles, responsibilities, competencies and resources required for an effective ISMS
  — effective, target-group-oriented communication to internal & external stakeholders
— **Risk** perspective refers to a key aspect of an ISMS in an aviation safety context according to this Regulation and serves as a basis for transparent decision-making and prioritisation of controls and risk treatment options. It further refers to the assessment, treatment and monitoring of information security risks in support of the management of aviation safety risks for the key processes and information assets upon which they depend. This includes protection requirements, risk exposure, attitude towards risks and risk acceptance criteria, methods and industry standards.
— **Compliance** perspective refers to the compliance with regulatory, legal and contractual (supply chain and operational peers) requirements. This includes:
  — this Regulation,

— the entity's own policies and standards and may further include international or industry standards adopted by the entity from ISO, EUROCAE, etc.

The perspective comprises the definition, implementation and maintenance of the required security provisions whose effectiveness and compliance shall be regularly monitored and assured by, e.g. (internal) audits.

Based on these perspectives we may identify 14 core components or building blocks that have been shown to be relevant and necessary for the establishment of an effective ISMS. These ISMS core components can be summarised as follows:

(a) context establishment defining the scope, interfaces, dependencies and requirements of interested parties;

(b) leadership and commitment of the senior management;

(c) information security and safety objectives;

(d) information security policies;

(e) roles, responsibilities, competencies and resources required for an effective ISMS;

(f) communication to internal and external stakeholders and a sufficient level of security awareness among employees, managers and third parties;

(g) information security risk management including risk assessment and treatment;

(h) information security incident management establishing processes for the handling of information security incidents and vulnerabilities;

(i) performance & effectiveness monitoring, measurement and evaluation;

(j) internal audits and management reviews;

(k) corrections and corrective actions;

(l) continuous improvement;

(m) relationship with suppliers;

(n) documentation and evidence collection.

Additional critical success factors for the implementation and operation of an ISMS include the following:

— The ISMS should be integrated with the entity's processes and overall management structure or even — at least partially, with safeguards for their respective integrity, and as reasonably applicable — with an overarching management system comprising information security, aviation safety and quality management.

— Information security has to be considered at an early stage in the overall design of processes and procedures, of systems and of information security controls, to be seamlessly integrated, for maximum effectiveness, minimal functional interference and optimised cost. None of these benefits can be achieved by integrating it on later.

— The risk management process determines appropriate characteristics of preventive controls to reach and maintain acceptable risk levels.

— The incident management process ensures that the organisation detects, reacts and responds to information security incidents in a timely manner. This is achieved by defining responsibilities, procedures, scenarios and response plans in advance to ensure a coordinated, targeted and efficient response.

— Continuous monitoring and reassessment are undertaken and improvements are made in response.

The above-mentioned core components are related to the requirements in this Regulation, for which Figure 2 provides an high-level depiction of the aspects that are more prominent in the implementation phase and those that characterise the operational phase, as well as the review and possible improvement.

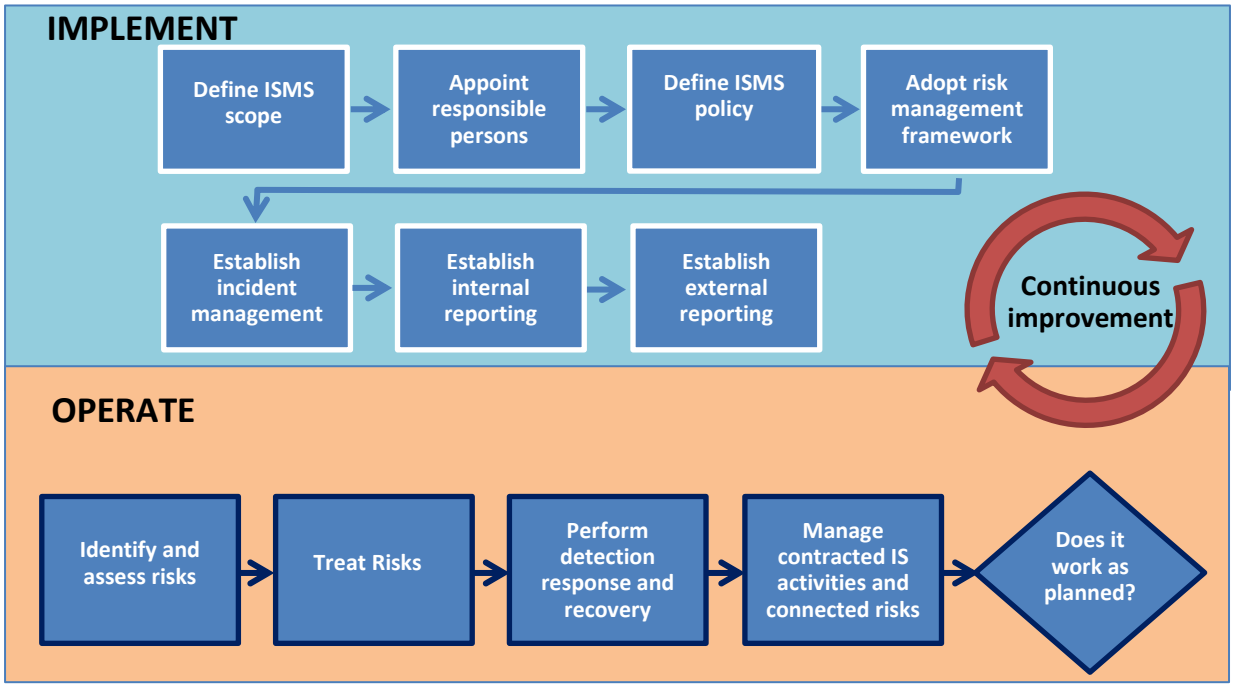

Figure 2: Representation of the Part-IS requirements from an ISMS's life cycle perspective

Plan-Do-Check-Act approach

The Plan-Do-Check-Act (PDCA) refers to a process approach that is often used to establish, implement, operate, monitor, review and improve management systems. Figure 3 depicts the PDCA applied to an ISMS.

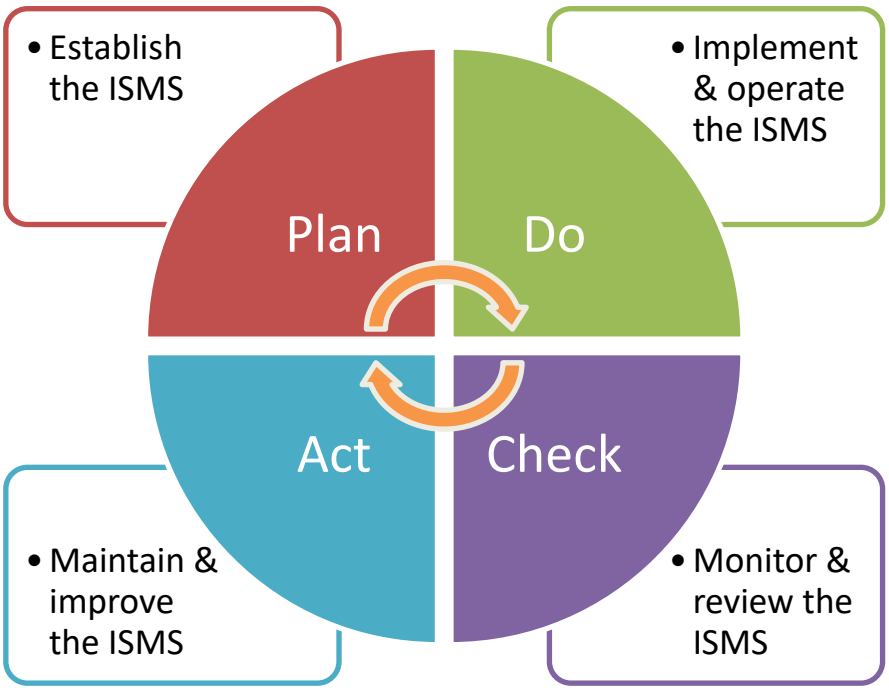

Figure 3: Plan-Do-Check-Act approach applied to ISMS

An alternative cyclical process is Define-Measure-Analyse-Improve-Control (DMAIC, six sigma).

Benefits of an ISMS

The benefits of a management system operating in a dynamic, uncertain or unpredictable risk environment are realised over the long term only when the organisation improves existing controls, processes and solutions based on the assessments of risks, performance and maturity as well as the learnings from incidents, audits, non-conformities and their root causes. A successful adoption and deployment of an ISMS allows an entity to:

— achieve greater assurance to the management and interested parties that its information assets are adequately protected against threats on a continual basis;

— increase its trustworthiness and credibility providing confidence to interested parties that IS risks with an impact on aviation safety are adequately managed;

— increase the resilience of the entity's key processes against unauthorised electronic interactions and maintains the entity's ability to decide and act;

— support the timely detection of control gaps, vulnerabilities or deficiencies aimed to prevent security incidents or at least to minimise their impact;

— detect and timely react on changes in the entity's environment including system architecture and threat landscape or the adoption of new technologies;

— provide a foundation for effective and efficient implementation of a comprehensive security strategy in times of digital transformation, increasing interconnectivity of systems, emerging information security threats and new technologies.

Relation to ISO 27001

The international standard ISO 27001 is a widely adopted standard for ISMS: it specifies generic requirements for establishing, implementing, maintaining and continually improving an ISMS and also includes requirements for the assessment and treatment of IS risks. The requirements are applicable to all entities, regardless of type, size or nature. The conformity of an ISMS with the ISO 27001 standard can be certified by an external qualified auditor on behalf of a reputable certification authority. ISO 27001 is compatible with other management system standards (quality, safety, etc.) that have also adopted the structure and terms defined in Annex SL to ISO/IEC Directives, Part 1, Consolidated ISO Supplement: this compatibility allows an entity to operate a single management system that meets the requirements of multiple management system standards.

The requirements for an ISMS specified by this Regulation are in most parts consistent and aligned with ISO 27001; however, this Regulation introduces provisions specific for the context of aviation safety. If an ISO 27001-based ISMS is already operated by an entity for a different scope and context, it can be adapted and extended to the scope and context of this Regulation in a straightforward manner based on an analysis of the scope and the gaps.

PART-IS versus ISO 27001 cross reference table

For a comparison between the main tasks required under Part-IS and the clauses and relevant controls in ISO 27001, refer to Appendix II.

AMC1 IS.I.OR.200(a)(1) Information security management system (ISMS)

The organisation should define and document the scope of the ISMS, by determining activities, processes, supporting systems, and identifying those which may have an impact on aviation safety.

The information security policy should cover at least the following aspects with a potential impact on aviation safety by:

(a) endorsement by the accountable manager or, in the case of design organisations, the head of the design organisation and review at planned intervals or if significant changes occur;

(b) committing to comply with applicable legislation, consider relevant standards and best practices;

(c) setting objectives and performance measures for managing information security;

(d) defining general principles, activities, processes for the organisation to appropriately secure information and communication technology systems and data;

(e) integrating ISMS requirements into the processes of the organisation;

(f) committing to continually improve towards higher levels of information security process maturity as per IS.I.OR.260;

(g) committing to satisfy applicable requirements regarding information security and its proactive and systematic management and to the provision of appropriate resources for its

implementation and operation;

(h) assigning information security as one of the essential responsibilities for all managers

(i) continuously promoting the information security policy within the competent authority/organisation to all personnel;

(j) encouraging the implementation of a 'just culture' and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents;

(k) communicating the information security policy to all relevant parties, as appropriate.

GM1 IS.I.OR.200(a)(1) Information security management system (ISMS)

INFORMATION SECURITY POLICY AND OBJECTIVES

The information security policy should suit to the entity's purpose and direct its IS activities. Such policy should contain the needs for IS in the entity's context, a high-level statement of direction and intent of the IS activities, the principles and most important strategic and tactical objectives to be achieved by the ISMS, as well as the general IS objectives or a specification of a framework (who, how) for setting IS objectives. The IS policy should also contain a description of the established ISMS including roles, responsibilities and references to topic-specific policies and standards.

The IS objectives should be:

— consistent and aligned with the IS policy and consider the applicable IS requirements, derived from the overarching entity's objectives, and the results from the risk assessment and treatment (which, in turn, supports the implementation of the entity's strategic goals and IS policy);

— regularly reviewed to ensure that they are up to date and still appropriate;

— measurable if practicable (to be able to determine whether or not the objective has been met), aimed to be SMART (specific, measurable, attainable, realistic, timely) and aligned with all affected responsible persons.

When defining IS objectives, e.g., based on the overarching entity's objectives, the IS requirements, or the results of risk assessments, it should be determined how these objectives will be achieved. The degree to which IS objectives are achieved must be measurable. If possible, it should be measured by KPIs which have been defined in advance (refer to resources such as COBIT 5 for Information Security). It is recommended to start with the definition of a limited number of IS objectives which are relevant for the entity, more of a long-term nature and measurable with a reasonable effort relative to the delivered benefits.

GM1 IS.I.OR.200(a)(12) Information security management system (ISMS)

COMPLIANCE MONITORING

For the purpose of compliance monitoring, internal audits should be conducted at planned intervals to provide assurance on the status of the ISMS to the management and to provide information on the following:

— conformity of the ISMS to the requirements of this Regulation and the organisation's own requirements either stated in the IS policy, procedures and contracts or derived from information security objectives or outcomes of the risk treatment process;

— effective implementation and maintenance of the ISMS.

Internal audits should follow an independent, evidence-based approach and set up an audit programme taking into consideration the importance of the processes concerned and definitions of the audit criteria and scopes. Documented information should be retained evidencing the audit results, their reporting to the relevant management and the audit programme.

AMC1 IS.I.OR.200(a)(12)&(a)(13) Information security management system (ISMS)

When establishing compliance with the provisions under points IS.I.OR.200 (a)(12) and (a)(13), the organisation should:

(a) implement a function to periodically monitor compliance of the management system with the relevant requirements and adequacy of the procedures including the establishment of an internal audit process and an information security risk management process. When the organisation has already established a compliance monitoring function under the implementing regulation for its domain, such function should include the monitoring of the management system with the relevant requirements within the scope of its activities. Compliance monitoring should include a feedback system of audit findings to the accountable manager or, in the case of design organisations, the head of the design organisation or delegated persons to ensure implementation of corrective actions as necessary;

(b) implement and maintain suitably robust information security controls for the protection of information, ensuring the principle of need-to-know. It should protect the source of information in accordance with the relevant provisions established in Regulation (EU) 2018/1139. It should also comply with Regulation (EU) No 376/2014.

AMC1 IS.I.OR.200(c) Information security management system (ISMS)

When establishing compliance with the provisions under point IS.I.OR.200(c), the organisation should:

(a) provide an outline of the structure of the specific security resources (internal and external), including their roles and responsibilities that will be used to manage and maintain the assets and resources included within the scope and approved by the accountable manager or, in the case of design organisations, by the head of the design organisation and review at planned intervals or if significant changes occur;

(b) identify and categorise all relevant contracted organisations used to implement the ISMS. The organisation should define and document procedures for the management of interfaces and coordination between the organisation and other organisations, including contracted organisations;

(c) identify and define all key processes and procedures, and internal and external reporting schemes that will be used to maintain compliance with the objectives over the life cycle of the ISMS. The organisation may adjust existing processes or procedures for compliance;

(d) identify and document any other information that will be used to maintain compliance with the objectives;

(e) when creating and updating documented information, ensure appropriate identification and description (e.g. a title, date, author, or reference number) as well as a review and an approval for suitability and adequacy;

(f) control documented information required by the ISMS to ensure that:

(1) it is available and suitable for use, where and when it is needed;

(2) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

GM1 IS.I.OR.200(c) Information security management system (ISMS)

The amount of information that should be documented to maintain compliance with the objectives of this Regulation may vary between organisations due to various factors, such as size and complexity, or the need for harmonisation with other management processes already in place. As general guidance, taking into account the documents required to comply with point IS.I.OR.200(a), the record-keeping requirements referred to in IS.I.OR.245 and the information security management manual requirements referred to in IS.I.OR.250, the following is a non-exhaustive list of information that should be documented:

(a) information security policy that should include the organisation's security objectives — see IS.I.OR.200(a)(1);

(b) responsibilities and accountabilities for roles relevant to information security;

(c) scope of the ISMS and the interfaces with, and dependencies on, other parties — see IS.I.OR.200(a)(2) and the information security requirements referred to in point IS.I.OR.205;

(d) information security risk management process;

(e) archive of risks with results of the information security risk assessment and treatment measures (often referred to as 'risk register' or 'risk ledger') — see IS.I.OR.245;

(f) evidence of the competencies necessary for the personnel performing the activities required under this Regulation;

(g) evidence of the current competencies of the personnel performing the activities required under this Regulation;

(h) (key) performance indicators derived from evidence of the monitoring and measurement of the ISMS processes.

GM1 IS.I.OR.200(d) Information security management system (ISMS)

PROPORTIONALITY IN ISMS IMPLEMENTATION

When implementing the processes and procedures, as well as establishing the roles and responsibilities required under point IS.I.OR.200(d), the organisation should primarily consider the risks that it may be posing to other organisations, as well as its own risk exposure. Other aspects that may be relevant include the organisation's needs and objectives, information security requirements,

its own processes and the size, complexity and structure of the organisation, all of which may change over time.

SMALL ORGANISATIONS IMPLEMENTING THE ISMS

Small organisations should consider seeking third-party service providers that can provide additional personnel and expertise to support the ISMS, and to this end consider the provision of IS.I.OR.235 and the related AMC. Outsourcing specific ISMS functions, such as security monitoring or incident response to a third-party service provider can help ensure that the organisation has access to the necessary personnel and expertise. Similarly, small organisations may want to be supported by a third party in performing the risk assessment.

Regarding the establishment of the appropriate personnel to implement and comply with the provisions of this Regulation, small organisations should always refer to AMC1 IS.I.OR.240(f) and GM1 IS.I.OR.240(f), however by considering that multiple responsibilities may be assigned to one person, while always ensuring the compliance monitoring independence.

As an introduction to the nature of information security risks and their management by small businesses, organisations may use, as initial guidance, the NIST Interagency Report (NISTIR) 'Small Business Information Security: The Fundamentals'.

INTEGRATION OF ISMS UNDER THIS REGULATION WITH EXISTING MANAGEMENT SYSTEMS

An organisation may take advantage of existing management systems when implementing an ISMS by integrating it with those existing systems.

By integrating the ISMS with existing management systems, the organisation may reduce the effort and costs required to implement and maintain the ISMS, while also ensuring consistency and alignment with the organisation's overall management approach. Below is a non-exhaustive list of potential synergies that can be exploited when integrating the ISMS with an existing management system:

— Leverage existing policies and procedures: an organisation may use its existing policies and procedures as a foundation for its ISMS. This may help to ensure consistency and minimise the need for additional documentation.

— Align ISMS with other management systems: an organisation may align the ISMS with other management systems, such as safety management systems (SMS), to ensure that the ISMS is consistent with the organisation's overall management approach.

— Use existing risk management processes: an organisation may use their existing risk management processes to identify and assess the security risks to their sensitive information.

— Reuse existing controls: an organisation may reuse existing controls, such as access controls or incident management process, to implement the security controls required by the ISMS.

— Continuous improvement process: an organisation may use the continuous improvement process of existing management systems to improve the ISMS over time.

AMC1 IS.I.OR.200(e) Information security management system (ISMS)

EXEMPTIONS

Organisations should follow the directions provided in AMC1 IS.I.OR.205(a) and AMC1 IS.I.OR.205(b) to perform a documented information security risk assessment to seek the approval from the competent authority of an exemption under point IS.I.OR.200(e). In order to justify the grounds for an exemption, the risk assessment is expected to provide explanations for the exclusion of all assets from the scope of the ISMS.

Organisations that would like to have the risk assessment performed by a third party should consider the provision of IS.I.OR.235 and the related AMC.

GM1 IS.I.OR.200(e) Information security management system (ISMS)

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for exemption by the competent authority following the procedure outlined in AMC1 IS.I.OR.200(e). It is up to the authority to determine whether this assessment is deemed satisfactory for an exemption to be granted.

Some examples of organisations that may consider asking for an exemption might include:

— A DOA or POA organisation that designs or produces only components or parts that are not involved in ensuring the structural integrity of the aircraft (e.g. carpets, interiors), nor any aircraft navigation or control functionality.

— An air operator that performs commercial (non-transport) specialised operations (SPO) with non-complex aircraft if the nature of the operations justifies the grounds for an exemption.

— An air operator that operates ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 with the exception of e.g. one aircraft in predefined operational conditions or under certain operational limitations e.g. taking off and landing in the same aerodrome or operating site, operating in VFR, etc.

The aforementioned examples are not exhaustive and are only indicative of potential scenarios that might provide an initial basis for the preparation of an information security risk assessment that justifies the exclusion of all assets of an organisation from the scope of the ISMS.

AMC1 IS.I.OR.205(a) Information security risk assessment

The organisation, when conducting an information security risk assessment, should ensure that all aviation safety-relevant assets (e.g. physical, human, information) are identified and included in the ISMS scope as per IS.I.OR.200 and relevant AMC. Additionally, organisation should provide the justification for those assets that are included and those that are excluded from the scope based on the outcome of its risk assessment. The organisation should identify the criteria to be used.

The organisation should identify all the elements of its own organisation which are within the scope of its ISMS and which could be exposed to information security risks, and should include at least those listed in IS.I.OR.205(a).

GM1 IS.I.OR.205(a) Information security risk assessment

For aviation, there are specific regulations and standards that govern the aircraft operating environment. Aircraft operators, aircraft manufacturers and suppliers whose equipment will be within the aircraft domain should continue to follow that same structure. For organisations managing their ground environment, no specific security framework, such as ISO, NIST or others, is explicitly mentioned for the development of their risk assessment. Each framework offers different benefits and none of these frameworks is perfect for an individual organisation and should be customised and tailored to meet the overall needs of an organisation, as well as the specific needs related to the aviation assets to be included within the scope of the ISMS.

Organisations whose security frameworks have achieved industry certifications can provide this information as supporting artefacts; however, these organisations should show the applicability of the industry certification to the scope of this Regulation.

To help guide organisations, aviation-specific guidance defined in the most current version of the EUROCAE ED-201x document 'Risk Management' chapter and in the ED-204x, ED-205x and ED-206x document supporting chapters for 'Risk Management' appropriate for their unique operating environment, may be considered.

Regardless of the framework used, the organisation should demonstrate a clear and comprehensive understanding of all relevant data flows and information exchanges. The organisation should provide corresponding documentation on resources and dependencies related to computing, networking, supply chain and contracted services which have the potential to affect the information security and safety of the functions, services or capabilities within the scope of the risk assessment.

The following non-exhaustive list provides examples of items that should also be included in the aforementioned documentation. The level of detail should be commensurate with the expected level of risk. The purpose is to establish an understanding of all relevant assets, resources and dependencies that are directly a part of the functions, services and capabilities through the following information:

(a) Identification of inputs and outputs of the risk assessment:

- internal;
- external;
- internal leased or managed services, supply chain or other dependency;
- external leased or managed services, supply chain or other dependency;

(b) Identification of all relevant resources (i.e. hardware, software, network and computing resources) used to create, transmit, store or receive the inputs and outputs;

(c) Identification and definition of the physical operating environments and locations for all relevant resources;

(d) For each asset included within the scope, identification and association of the specific methods or resources that will be used by the organisation to manage, operate and maintain each asset over the life cycle of each asset including:

- internal resources;
- contracted resources;

— supply chain;

— managed service provider.

The organisation should also demonstrate a clear and comprehensive understanding of the resources that are used by the organisation to ensure effective operations, management and oversight (internal and external).

AMC1 IS.I.OR.205(b) Information security risk assessment

To establish compliance with IS.I.OR.205(b), the organisation should, based on the exchange of data and information and the assets used for this, identify within the scope of the information security risk assessment, the interfaces it has with other parties such as service providers, supply chains and other third parties, and which could result in a situation where information security risks either:

— pose a threat to other parties; and/or

— pose a threat to the organisation,

as a result of mutual exposure to those risks amongst the involved parties.

GM1 IS.I.OR.205(b) Information security risk assessment

Organisations may follow any security framework such as ISO, NIST or other when developing their risk assessment. The method needs to allow for the consideration of risk sharing between interconnected organisations. As an example, EUROCAE ED-201A, Figure 4-1 'Risk Assessment and Sharing Stages' represents a risk assessment process which can support organisations in identifying, assessing and agreeing on shared risks with others.

Organisations should follow the guidance defined in chapters 'Risk Management' and 'The concept of functional chains' of EUROCAE ED-201A. Additional guidance from supporting chapters regarding 'Risk Management' that is appropriate for their unique operating environment can be found in the ED-204x, ED-205x and ED-206x documents.

Risk information sharing

Risk information sharing means that interfacing organisations should inform each other about the potential exposure to information security risks by following, for instance, the approach detailed in ED-201A Appendix B.1, B.2 and B.3. The purpose of this exchange of information is to enable the organisations to establish a matching mapping for those services which are identified under IS.I.OR.205(a), including all flows of information and data in order to:

(a) illustrate (e.g. through a functional diagram) the relationships of logical and physical paths connecting the different parts involved;

(b) clearly identify all assets and resources that will be used in the exchange;

(c) identify and categorise all functions, activities and processes, including their respective information and data, which will be created, transmitted, received and stored, and associate those with the responsible party which provides or performs those functions, activities and processes;

(d) determine for these paths, constituting the so-called functional chains, the role of the interfacing party as a producer, processor, dispatcher or consumer of the information or data involved;

(e) determine whether one interfacing party acts as an originator or receiver of a flow across such path.

GM2 IS.I.OR.205(b) Information security risk assessment

EXAMPLES OF AVIATION SERVICES

Examples of aviation services are provided in Appendix III.

AMC1 IS.I.OR.205(c) Information security risk assessment

The organisation should use a risk management framework that includes a methodology for assigning risks with a risk level and establishing criteria for determining risk acceptance or further treatment.

The organisation should provide documented evidence of risks which have a potential impact on aviation safety including the level of risks. The organisation should relate each risk to the relevant elements and interfaces identified under IS.I.OR.205 (a) and (b), and document whether the risk is acceptable or requires further treatment.

The organisation should provide the assurance that the risk assessment process is performed with the necessary rigour and discipline by documenting the process and its robustness. By doing so, the organisation should consider:

(a) reproducibility of the assessment's inputs and results;

(b) repeatability of the assessment over time in a way that the results of the different prior assessments can be compared to determine the changes;

(c) the gathering of inputs that are relevant and up to date, in particular:

— the information that allows the determination of the safety consequences;

— the information that allows the determination of the potential of occurrence of the threat scenario.

GM1 IS.I.OR.205(c) Information security risk assessment

RISK ASSESSMENT

The risk classification levels for the potential of occurrence of the threat scenario and severity of the safety consequences listed below may be applied, however this does not prevent the organisation from developing additional intermediate categories if it deems this necessary for risk assessments. The organisation should specify and document the applied, entity-specific, classification levels with an accurate qualitative definition and a quantitative definition in terms of a range or interval of real numbers in order to enable a sufficiently calibrated, consistent estimation, evaluation and communication within the entity or at the interfaces. The potential of occurrence of the threat scenario may be expressed as an interval of likelihoods including the duration of the observation. Supporting documentation and methods can be found in EUROCAE ED-203A Chapter 3.6 which

references the evaluation of the potential of occurrence of the threat scenario in the Security Risk Assessment of EUROCAE ED-202A.

In order to facilitate the mutual comparability of risk assessment methodologies between interfacing organisations, the organisation may associate the assessment of the potential of occurrence of the threat scenario with one of the following categories:

— High potential of occurrence: the threat scenario is likely to occur. The attack related to the threat scenario is feasible and similar threat scenarios have occurred many times in the past.

— Medium potential of occurrence: the threat scenario is unlikely to occur. The attack related to the threat scenario is possible and a similar threat scenario may have occurred in the past.

— Low potential of occurrence: the threat scenario is very unlikely to occur. The materialisation of the threat scenario is theoretically possible; however, it is not known to have occurred.

The evaluation of the potential of occurrence of the threat scenario can be based on the following aspects:

Protection (as defined in EUROCAE ED-203A)

— Security measures and architecture that deny access to assets: the degree to which an asset is open to access from compromised systems.

— Access to security measures: the degree to which a security measure prevents access/attack to itself from compromised systems.

— Failure of mechanism: the degree to which the known implementation of a security measure will fail to prevent an attack.

— Detection methods or procedures to recognise the attack and appropriately respond to reduce the potential of occurrence of the threat scenario.

Exposure reduction (as defined in EUROCAE ED-203A)

— Conditions under which an external access connection can be used by a user or attacker

— Limits on the functionality of an external access connection

— Organisational policies that control the time-to-feasibility for developing attack tools specific to the product

— Vulnerability management including intelligence, scanning, treatment and retesting aimed to discover, detect and treat newly reported or detected vulnerabilities in a fast, risk-prioritised manner with high assurance in order to reduce the attack surface

Attack attempt (as defined in EUROCAE ED-203A)

— The capability of the attackers which is determined by the resources and expertise required for their attack

  The capability of the attackers can be assessed through several ways, for instance:

  — information from CERTs/CSIRTs, ISACs;

  — analyses of past activities, techniques and procedures (TTPs) and success rate of attacks.

  For the same reason the organisation may associate the outcome of the evaluation of the

severity of the safety consequences with one of the following categories:

— High severity: those immediate or delayed scenarios that can cause or contribute to an accident where an accident means an occurrence associated with the operation of an aircraft in which:

  — a person is fatally or seriously injured;

  — the aircraft sustains damage or structural failure;

  — the aircraft is missing or completely inaccessible;

— Moderate severity: those immediate or delayed scenarios that can cause or contribute to safety incidents where an incident means any occurrence other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operations;

— Low severity: those immediate or delayed scenarios that can cause or contribute to negligible safety consequences.

Additional information can also be found in Regulation (EU) 2015/1018 on mandatory reporting of occurrences. Further examples for aviation domains can be found in EUROCAE ED-201A – Appendix B — Tables B-5, B-6 and B-7.

Risk acceptance criteria

Risk acceptance criteria are critical and should be developed, specified and documented. The criteria may define multiple thresholds, with a desired target risk level, but including also provision for the accountable manager or, in the case of design organisations, the head of the design organisation or delegated persons to accept risks above this level under defined circumstances and conditions.

In order to facilitate the mutual comparability of risk assessments between interfacing entities, the organisation should classify the risks in the following categories:

— unacceptable risk;

— conditionally acceptable risk;

— acceptable risk.

For what concerns the conditional acceptance of risks, the criteria for acceptance should take into account how long a risk is expected to exist (temporary or short-term activity or exposure), or may include requirements for the commitment of future treatments to reduce the risk at an acceptable level within a defined time duration and show how the risk will be managed over time through the organisation’s risk governance processes.

Moreover, risks should be conditionally accepted only under the condition that the organisation demonstrates the presence of a comprehensive risk management structure that includes risk assessment, risk treatment and risk monitoring processes for operations. This is typically achieved when the organisation reaches a higher level of maturity that is representative of functionality and repeatability of cybersecurity risk management — see GM1 IS.I.OR.260(a).

The following Figure 1 depicts a risk acceptance matrix based on the aforementioned categories that can be used by interfacing organisations for mutual comparability.

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Figure 1: Risk acceptance matrix

* The potential of occurrence of the threat scenario is reassessed in a timely manner (refer to IS.I.OR.205(d)) and monitored to ensure that it remains low and that if the risk materialises, it is early detected and dealt with.

A comprehensive risk management structure typically entails the following aspects and processes:

— a repeatable and reproduceable risk assessment. If the risk factors are considered fairly uncertain and within some wide value range or not sufficiently precise, further iterations of the risk assessment are performed involving additionally gathered or detailed information and a more in-depth assessment in order to reduce uncertainty and increase precision;

— a thorough review of those risks proposed to be conditionally acceptable that is performed by the accountable manager or, in the case of design organisations, the head of the design organisation or delegated person(s) who may impose additional conditions for the risk retention;

— strict monitoring of the key risk indicators that includes a defined, reliable detection of the potentially evolving risk materialisation;

— an incident response scheme is in place with reactive measures that are triggered by detection mechanisms in order to immediately contain the consequences, in particular, for risk scenarios involving a high severity level.

Note: A risk assessment process can be classified as ‘repeatable’ when under the same conditions an entity or a person delivers the same result. Conditions can include:

— use of the same information security risk assessment framework or methodology;

— use of the same inputs, assumptions, security context and threat environment, considering the time period, where long breaks can significantly affect the repeatability;

— use of the same observing entity/person.

Similarly, a risk assessment processes can be classified as ‘reproduceable’ when another entity or another person given the same inputs, assumptions, security context and threat environment can reproduce the assessment in its entirety.

Threat scenario identification

A threat scenario is one of the possible ways a threat could materialise. Typically, a threat scenario describes a potential attack targeting one or more vulnerabilities of assets, as well as processes.

The purpose of the threat scenario identification under this Regulation is to develop a list of scenarios that may lead to an information security threat having an impact on aviation safety.

A threat scenario, in general, is characterised by the following:

— a threat source of the information security attack;

— an attack vector and a path through the organisation up to the asset;

— the security controls that would mitigate the attack;

— the consequence of the attack including the affected safety aspects.

Threat scenario identification guidance can be found in ED-202A Chapter 3.4. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

Additional methods to identify relevant threat scenarios

When conducting this analysis, both security and safety aspects should be coordinated throughout the process to ensure mutual understanding of the threat preventive measures and mitigations being applied. In the following Figure 2 the interactions between information security and aviation safety are depicted through a 'bow-tie' diagram that highlights the links between risk controls and the underlying management system.

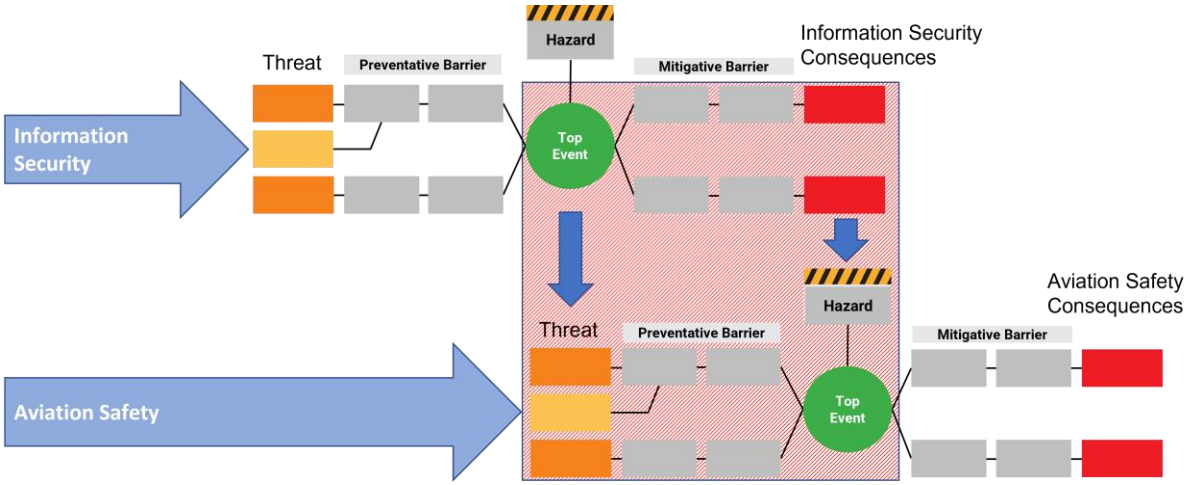

Figure 2: Interactions between information security and aviation safety risk management areas

Examples of threat scenarios

Threat catalogues may provide guidance and elements for the elaboration of threat scenarios that are relevant for the organisation. References can be found in ARINC 811 – Att. 3 – Tables 3-6 to 3-8 for the threat catalogues examples and other threat catalogue examples as they are provided by EU institutions. However, this is not an exhaustive list of examples and the identification of threat scenarios should therefore not be limited to those examples only. In addition, other relevant resources

containing information on information security threats and the information security threat landscape should be consulted to support the risk assessment process with relevant inputs.

A set of examples of threat scenarios can be found in Appendix I.

AMC1 IS.I.OR.205(d) Information security risk assessment

The organisation should take into account the following criteria when establishing compliance with the objectives contained in point IS.I.OR.205 (d):

(a) The risk assessment performed under points IS.I.OR.205 (a), (b) and (c) should be reviewed at regular intervals, the periodicity being determined by the organisation performing the assessment considering the criticality of the assets within the scope of the risk assessment, levels of post-assessment risk of the assets within the scope of the risk assessment and any customer or regulatory requirements. A higher criticality or level of risk will require more frequent review.

(b) The periodicity of risk assessment reviews should be documented by the organisation and include the justification, date of approval and information about the risk owner.

GM1 IS.I.OR.205(d) Information security risk assessment

Risks are not static and will not stay the same forever. Risk assessments can be undertaken on different levels where one pursues a high-level risk assessment and another one a more granular approach to support the identification of changes and the need for a more detailed risk assessment. Risk assessments should be subject to regular reviews to:

(a) allow for continuous improvement of the quality of risk assessment;

(b) ensure efficiency and effectiveness of risk controls and mitigations in both their design and operation;

(c) review plans and actions for risk treatment;

(d) update any changes which may require revision of risk treatments and priorities;

(e) maintain an overview of the complete risk picture; and

(f) identify any emerging risks.

The objective of a risk assessment review is to re-evaluate the risks, their likelihood and impact. One possible approach is to tier risk assessments with a higher-level risk assessment which is used to identify changes. In a next step, higher-level risk assessment could allow the identification of the detailed risks that should be reviewed.

Risk assessment reviews should involve the risk owners, project teams and other stakeholders as applicable.

GM2 IS.I.OR.205(d) Information security risk assessment

Risk assessments should be reviewed regularly and may be reviewed more or less frequently depending on whether the assets within the scope of the risk assessment are of sufficient criticality or complexity, the levels of post-assessment risk warrant more frequent analysis, or to adhere to any regulatory or customer requirements. The criticality of assets can be determined through an assessment of the impacts of a loss of the assets i.e. an impact assessment.

The periodicity of risk assessment reviews should be documented by the organisation in security manuals, processes or procedures and should align with wider change management activities and management reviews of information security. Further guidance on criteria and frequency of risk assessment review can be found in EUROCAE ED-201A Chapter 4, as well as ED-205A Chapter 3.2 (for ATMS/ANS).

Risk assessments should also be reviewed when:

(a) there is a change in the elements subject to information security risks as identified in IS.I.OR.205(a); changes may be identified through management reviews or change control processes. Change in the elements will include:

- additions to or removals from elements within the scope of the risk assessment (as identified in IS.I.OR.205(a));
- changes to design or configuration of elements within the scope of the risk assessment (as identified in IS.I.OR.205(a)) that have the potential to alter the risk assessment outcomes; or
- changes to values, which would potentially trigger changes to impact levels, of elements within the scope of the risk assessment (as identified in IS.I.OR.205(a));

(b) there is a change in the interfaces between the organisation and other organisations with which the organisation shares information security risks or relies upon to mitigate information security risks (e.g. supply chains, service providers, cloud providers and customers), as identified in IS.I.OR.205(b), or between the system within the scope of the risk assessment and any other interconnected systems, or in the risks notified to the organisation by other organisations, as identified in IS.I.OR.205(b), or owners or managers of the other systems including:

- establishment of new interfaces;
- removal of existing interfaces;
- changes to existing interfaces that would have the potential to alter the risk assessment outcomes.

Note: Some organisational or system interconnections may be with organisations that are not within the scope of this Regulation as defined in Article 2 and therefore are not subject to the requirements of Part-IS. Where this is the case, these organisations should be informed of their responsibility to report such changes as listed above through contractual arrangement and reporting requirements between the affected organisations on a case-by-case basis and where applicable;

(c) there is a change in the information or knowledge used for the identification, analysis and classification of risks including:

— changes to threats and their values or addition of new threats that have not previously been assessed;

— changes to vulnerabilities or addition of new vulnerabilities that have not previously been assessed;

— changes in impacts or consequences of assessed threats or vulnerabilities;

— changes in aggregation of risks that may result in unacceptable levels of risks;

— changes or improvements in the risk management process, risk assessment approach and related activities;

— changes or improvements in the treatments of risks;

— changes in the criteria used to determine acceptance and treatments of risks;

(d) there are lessons learned from the analysis of information security incidents including:

— understanding of why and how incidents have occurred; and

— reviewing all types of incidents including those due to external factors, technical reasons, human factors or processes. For human factors a distinction can be made between malign and benign actions.

Evidence of risk assessment review should be documented and should include:

— evidence of approval of the review by the designated risk owner; and

— the rationale behind or basis for the risk owner's approval of the review.

Such evidence may comprise, but is not limited to:

— reports which constitute a form of documentation to track information security risks potentially impacting an organisation;

— the documentation of the information security risk assessment;

— exerts from a business or security risk register.

Note: In some cases the information contained in the risk report, security cases or risk register may be sensitive to the organisation and may need to be redacted in agreement with the authority, or a method may need to be established for the authority to view such content on the organisation's systems.

AMC1 IS.I.OR.205(e) Information security risk assessment

SAFETY SUPPORT ASSESSMENT

Non-ATS providers should conduct a safety support assessment as it is described in Regulation (EU) 2017/373 to assess the information security risk on their assets in regard to the service specification, e.g. integrity and availability, and to identify the residual risk. The residual risk should be used to assess the potential impact on services and products that a non-ATS provider offers to an ATS provider.

The non-ATS provider should share the information on residual risk and the impact on the services provided with the ATS provider in an appropriate form so that the ATS provider can use this as an input for its security risk assessment and, more importantly, to evaluate the potential impacts of these residual risks on safety.

GM1 IS.I.OR.205(e) Information security risk assessment

SAFETY SUPPORT ASSESSMENT

The table below shows the non-ATS providers which shall comply with Subpart C of Annex III to Regulation (EU) 2017/373. These are the organisations having to conduct the safety support assessment in order to provide the required information to ATS providers.

The information on the impact on products and services could be shared between non-ATS providers and ATS providers through agreed means, e.g. service level agreement, external agreement (in line with EUROCAE ED-201A), etc.

Shared information should enable ATS providers to perform an accurate assessment of the residual risk for their services. For instance, if the non-ATS providers identified a risk which could affect the availability of data provided to an ATS provider, the impact on the availability should be described in a way that allows the ATS provider to assess whether the resulting latency or delay in data transmissions could have a safety impact. This is relevant because only the ATS provider through its assessment can either accept or decline a residual risk.

	Annex III (Part-ATM/ANS.OR)				Annex IV (Part-ATS)	Annex V (Part-MET)	Annex VI (Part-AIS)	Annex VII (Part-DAT)	Annex VIII (Part-CNS)	Annex IX (Part-ATFM)	Annex X (Part-ASM)	Annex XI (Part-FPD)	Annex XII (Part-NM)	Annex XIII (Part-PERS)
	Subpart A	Subpart B	Subpart C	Subpart D										
Air traffic services providers (see Note 1)	X	X		X	X									
Meteorological services providers	X	X	X	X		X								
Aeronautical information services providers	X	X	X	X			X							
Data services providers	X	X	X					X						
Communication, navigation and surveillance service providers	X	X	X	X					X					
Air traffic flow management service providers	X	X	X	X						X				
Airspace management service providers	X	X	X								X			
Flight procedure design services providers	X	X	X									X		
Network Manager	X	X	X	X									X	
service providers (see Note 2)														X

Table: Non-ATS providers which shall comply with Subpart C of Annex III to Regulation (EU) 2017/373

GM1 IS.I.OR.210 Information security risk treatment

The risk management options referred to in IS.I.OR.210(a) may be used in combination; however, there is no obligation for the organisation to do so.

The application of risk treatment options under points IS.I.OR.210 (a)(1) and (a)(2) lead to the introduction of security measures, often referred to as security controls.

GM2 IS.I.OR.210 Information security risk treatment

For each identified risk, the organisation should define the specific risk treatments, methods or resources that will be used over the life cycle of each asset to:

— manage risk reduction;

— monitor and maintain each asset;

— update and fulfil activities for configuration management;

— manage supply chain;

— manage contracted services or service provider.

The review of risk treatment measures should include life cycle considerations which are introduced by equipment, procedures and personnel.

A risk treatment plan as an outcome of the risk management process should include a prioritisation of risks, the corresponding information on the objectives and means for risk treatment to reach an acceptable level of risk, as well as agreed timelines specifying when responsible personnel should have implemented the risk treatment measures. The timelines for the implementation of a risk treatment measure should be agreed by the personnel responsible for the implementation and shall be communicated to and accepted by the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s).

Any subsequent implementation delay, together with its cause, reason, rationale or necessity, should be documented in the risk treatment plan. The delay should also be communicated to the competent authority in case the materialisation of risk would lead to an unsafe condition. The delay is also subject to the acceptance by the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s). This person may condition such acceptance on the implementation or availability of compensating controls or reactive measures to monitor, early detect and timely respond to the materialisation of the risk in treatment. In order to timely respond, the incident response team may be informed to trigger their preparedness.

The risk treatment plan can act as a means of communication with the competent authority to demonstrate effective treatment of unacceptable risks. Similarly, this plan can be utilised to communicate to interfacing organisations how shared risks are controlled.

In accordance with IS.I.OR.205(d), a regular or conditional review of the risk assessment is necessary, and this includes the review of the risk treatment measures developed under IS.I.OR.210(a) to identify whether they are still effective or they require adaptations.

In addition, the organisation should also consider the potential impact on the effectiveness of risk treatment measures where a shared information security risk may arise as a result of the interaction between interfacing entities (see IS.I.OR.235 and related AMC).

AMC1 IS.I.OR.210(a) Information security risk treatment

The organisation should take into account the following criteria when establishing compliance with point IS.I.OR.210(a):

(a) the measures developed under point IS.I.OR.210(a)(1) should be implemented according to a

risk treatment plan with defined, risk-based priorities, objectives and agreed timelines and owners;

(b) identification and association of the life cycle considerations to ensure continuous effectiveness of the security measures including exchange of data with other entities;

(c) the organisation should review and update the risk assessment, according to IS.I.OR.205(d), to evaluate whether the measures developed under point IS.I.OR.210(a) do not introduce new unacceptable risks or modify existing risks in a way that they become unacceptable.

Risk treatment should be documented in the risk registry even if the risk has been avoided.

AMC1 IS.I.OR.215(a)&(b) Information security internal reporting scheme

Organisations will have the means to detect security incidents and vulnerabilities in accordance with IS.I.OR.220. Organisations should have a mechanism to collect notifications of events by personnel and by sources outside the company including suppliers, partners, customers and security researchers. The mechanism for collecting information by personnel and external sources should be easily accessible and communicated.

The organisation should collect all events gathered through the detection means for internal analysis. Each event should be analysed to identify whether it is indicative of suspicious behaviour and if yes, what potential or actual impact on aviation safety has occurred. Events should be considered in combination with other events to provide correlation to identify incidents.

The organisation should develop a vulnerability management strategy in order to ensure that a proper evaluation of all known, relevant information relating to the information security vulnerabilities is carried out when new vulnerabilities are identified. This strategy should consider the outcome of the risk assessment to determine whether further analysis of the vulnerability (e.g. exploitability) should be performed.

The organisation should identify all internal stakeholders that require notification of a specific incident or vulnerability and ensure that these stakeholders receive all necessary information on the incident or vulnerability in order to act effectively and in a timely manner to support the required detection and response periods.

GM1 IS.I.OR.215(a)&(b) Information security internal reporting scheme

RELATIONSHIP BETWEEN INTERNAL AND EXTERNAL REPORTING

Organisations should collect and report internally incidents and vulnerabilities aiming at covering all items within the scope of this Regulation. This does not preclude external reporting, nor does external reporting replace the need for internal reporting. Internal reports should be assessed in a timely manner and where the potential impact on safety is found to exceed the threshold for mandatory reporting, organisations should initiate reporting of these internal reports according to IS.I.OR.230.

GM2 IS.I.OR.215(a)&(b) Information security internal reporting scheme

ORGANISATION OF COLLECTION AND EVALUATION OF INFORMATION SECURITY EVENTS

It is a common practice in large organisations to centralise security operations in a security operations centre (SOC) and make use of a security information and event management (SIEM) system. A SIEM system collects all events from sources such as log files in a common database and allows the analysts and responders in joint SOC to review and act on these events. Organisations may choose to use a SOC for events relevant to Part-IS in isolation or in combination with events not subject to Part-IS but of interest to the organisation, such as events relating to business interests.

Organisations that do not have a SOC capability and do not use a SIEM system need to consider how to establish processes to meet the required detection capabilities as well as detection and response times.

GM3 IS.I.OR. 215(a)&(b) Information security internal reporting scheme

RELEVANT INFORMATION FOR INCIDENTS AND VULNERABILITIES

Understanding the causes and contributing factors of information security incidents and vulnerabilities allows lessons learned to be gained and to introduce corrections to processes and asset design. However, understanding causes and contributing factors may not always be possible or may not aid in continuous improvement of aviation safety. Where vulnerabilities arise from assets developed solely or primarily for aviation, it is expected to be possible to perform the necessary investigation on the root causes. These root causes will inform the affected organisation(s) to improve processes and asset design to remediate vulnerability and to ensure that such vulnerabilities are not introduced in other assets. Understanding the root causes of vulnerabilities also allows the aviation community to learn and thus avoid similar vulnerabilities in the future.

GM1 IS.I.OR.215(c) Information security internal reporting scheme

If contracted organisations are also subject to this Regulation, the exchange of information and reporting should be covered under the management of shared risks and through the establishment of an external agreement between the organisations. Guidance regarding the development of external agreements can be found in EUROCAE ED-201A – 4.4 External Agreements.

More in general, and in all other cases, any service contract should include standard clauses concerning obligations for the contracted organisation to:

— report within an agreed time security incidents that may have an impact on the contracting organisation. Incidents and vulnerabilities which could lead to unsafe conditions should be reported as soon as possible and in such a manner that the external reporting obligation under IS.I.OR.230 can be ensured;

— designate a point of contact for the incident management and possible crisis management.

In some cases contracted organisations, such as service providers with distributed resources, may not be able to offer any ad hoc reporting. In these cases the internal reporting requirement may be fulfilled through other means that satisfy the objective of this provision. For instance, the contracted organisations may provide an up-to-date list of vulnerabilities affecting the systems within the scope

of the contracted services. This list should be monitored by the contracting organisation as part of the internal reporting of security events.

GM1 IS.I.OR.215(d) Information security internal reporting scheme

The cooperation under point IS.I.OR.215(d) can be substantiated by sharing elements from incident records that can support other organisations' information security activities. In case the organisations are bound by contractual obligations, this contract may also include commitment to cooperate.

Moreover, commitment to cooperate may also be achieved through the active participation of the organisation in information security sharing initiatives; for instance, information sharing and analysis centre(s) (ISAC(s)). Additionally, for their own awareness, organisations may also subscribe to receive vulnerability and threat alerts, like those distributed by computer emergency response teams (CERTs).

GM1 IS.I.OR.220 Information security incidents – detection, response and recovery

Without prejudice to the definition of 'information security event' in Article 3, those events that indicate the potential materialisation of unacceptable risks include both occurrences (i.e. anything that causes harm or have the potential to cause harm) and discovery of vulnerabilities. In fact, information security risks are associated with the potential that threats will exploit vulnerabilities, therefore the discovery of an exploitable vulnerability is an information security event.

In light of this, in the context of this Regulation:

— detection activities required under IS.I.OR.220(a) include vulnerability discovery;

— response activities under IS.I.OR.220(b) include vulnerability management.

AMC1 IS.I.OR.220(a) Information security incidents – detection, response and recovery

DETECTION

When complying with the requirement in IS.I.OR.215(a), the organisation should define and implement a strategy to detect information security events having an impact on safety.

This should be done in a way to ensure that at least the detection strategy is able to cover all known information security threats to their assets that may materialise in a safety hazard having unacceptable consequences.

DETECTION STRATEGY

In order to determine the scope of the event detection, the organisation should:

(a) identify a list of threat scenarios from the risks identified under IS.I.OR.205;

(b) identify, as a minimum, those assets that contribute to the scenario(s) that may materialise in an unsafe condition. For this identification of the assets, the measures introduced under IS.I.OR.210 should also be considered.

Note: The contribution of an asset to the threat scenario and the materialisation of an unsafe condition should be assessed by considering the whole functional chain. In some cases, the asset may be at the end of a functional chain and if it is compromised, the effect on safety is direct and may be

immediate; conversely if the asset is far from the end of functional chain and it is compromised, the effect should propagate and may be delayed.

GM1 IS.I.OR.220(a) Information security incidents – detection, response and recovery

DETECTION STRATEGY

When developing the detection strategy, for those items within the scope of event detection, the organisation should define the conditions that trigger a process that, for example, would require personnel intervention and further analysis. These conditions on the items may be defined using elements from:

(a) expected functional baseline: engage in the identification of deviations from the expected functional operation of the system (excluding security functions/controls);

(b) expected security baseline: engage in the identification of deviations from the expected information security operation of security controls.

These conditions should consider both abnormal behaviour and substantial deviations from the baselines and relevant correlation of multiple independent events.

Further guidance on the objectives for the establishment of a detection strategy can be consulted in EUROCAE ED-206 – Chapter 4.

AMC1 IS.I.OR.220(b) Information security incidents – detection, response and recovery

(a) INCIDENTS

The organisation should take into account the following aspects when establishing compliance with the objectives contained in point IS.I.OR.220(b) relative to incidents:

(1) Preparation of procedures and delineation of roles and responsibilities to manage timely, effective and orderly response to any relevant security incidents.

(2) The response procedure should:

(i) consider the warnings, unitary or combined, from IS.I.OR.220(a)(2), and assess their potential impacts on aviation safety;

(ii) establish, in accordance with IS.I.OR.220(b)(2), a containment strategy for each asset category in relation with the potential worst-case effect and the mission constraints, and provide criteria indicating when the attack is contained;

(iii) define, in accordance with IS.I.OR.220(b)(3), the acceptable impact on safety and security of each asset within the scope when they fail due to the materialisation of a threat scenario.

(3) The response time should be commensurate with the impact level assessed in (2)(iii).

(4) The response measures implemented under IS.I.OR.220(b) should be based on the response procedure referred to in the above point (a)(2) and it should, in particular, consider the following:

(i) the maximum acceptable safety level degradation of the items within the scope of the threat scenario;

(ii) the actions, such as resistance, containment, deception and control of the possible ways systems can fail, which will contribute to achieving the acceptable safety level degradation identified in point (i) while minimising the impact on operations;

(iii) the resources required to implement the actions specified in point (ii).

(b) VULNERABILITIES

The organisation should take into account the following aspects when establishing compliance with the objectives contained in point IS.I.OR.220(b) relative to vulnerabilities:

(1) Establishment of a vulnerability management plan defining procedures, roles and responsibilities to manage quick, effective, and orderly response to any detected relevant vulnerabilities.

(2) The response measures implemented under point IS.I.OR.220(b) should be based on the maximum acceptable risk of the items within the scope of the vulnerability, considering the worst-case scenario of the vulnerability being exploited.

(3) The response time should be commensurate with the pre-triage done on the warnings and the assessment of the potential impact of the vulnerability, if it is exploited.

GM1 IS.I.OR.220(b) Information security incidents – detection, response and recovery

An attack is considered contained (i.e. it is not spreading any further) when the boundaries of the incident have been identified and the threat does not propagate beyond these boundaries. Further guidance can be found in EUROCAE ED-206 – Chapter 5.

Guidance about the vulnerability strategy can be found in EUROCAE ED-206 – Chapter 3.4.2.

AMC1 IS.I.OR.220(c) Information security incidents – detection, response and recovery

When complying with the requirement in IS.I.OR.220(c), the organisation should develop an incident recovery procedure including at least the following:

(a) a list of those assets that enable safe operations, as well as the dependencies among them, this constituting the scope of the recovery;

(b) a description of the process with the necessary priority actions to be executed for a return to a safe and secure state for the assets within the scope of the recovery;

(c) the resources required to execute the actions defined in point (b) to ensure that these resources are readily available after an incident has occurred;

(d) the objectives for recovery time that should be set in relation to the safety criticality of the assets within the scope of the recovery.

GM1 IS.I.OR.220(b)&(c) Information security incidents – detection, response and recovery

RECOVERY OBJECTIVES AND TIMING

This Regulation focuses on incidents that have an impact on safety and requires response and recovery measures to be in place to ensure that operational safety remains above a minimum acceptable level.

The level of operations and safety may be interrelated, so in some cases when the level of operations is compromised by an information security incident and drops, the level of safety does the same. This is, for instance, the case of air traffic control, if air traffic services are reduced or become unreliable, the safety of flights is reduced too.

However, in other cases the relation between the level of operations and safety may be the inverse, or they may be decoupled, so when an incident occurs and the operations drop, the level of safety is preserved. One example is the compromise of software loading process on board the aircraft. In this case a detected incident followed by the decision to interrupt the software loading operations would preserve the existing level of safety.

The following Figure 1 depicts a conceptual framework that may be considered for the definition of the response and recovery objectives, including the recovery time. It represents, in the worst-case scenario, how the expected level of operational safety (safety level) for a process or an activity may vary over time when a security incident occurs. In this scenario, the safety level: first is reduced by the incident and then it degrades as long as the time passes. The figure also shows the expected effect that mitigations and controls should have, respectively: in containing the operational safety drop as soon as an incident occurs, and in improving the recovery, i.e. the return to the expected safety level.

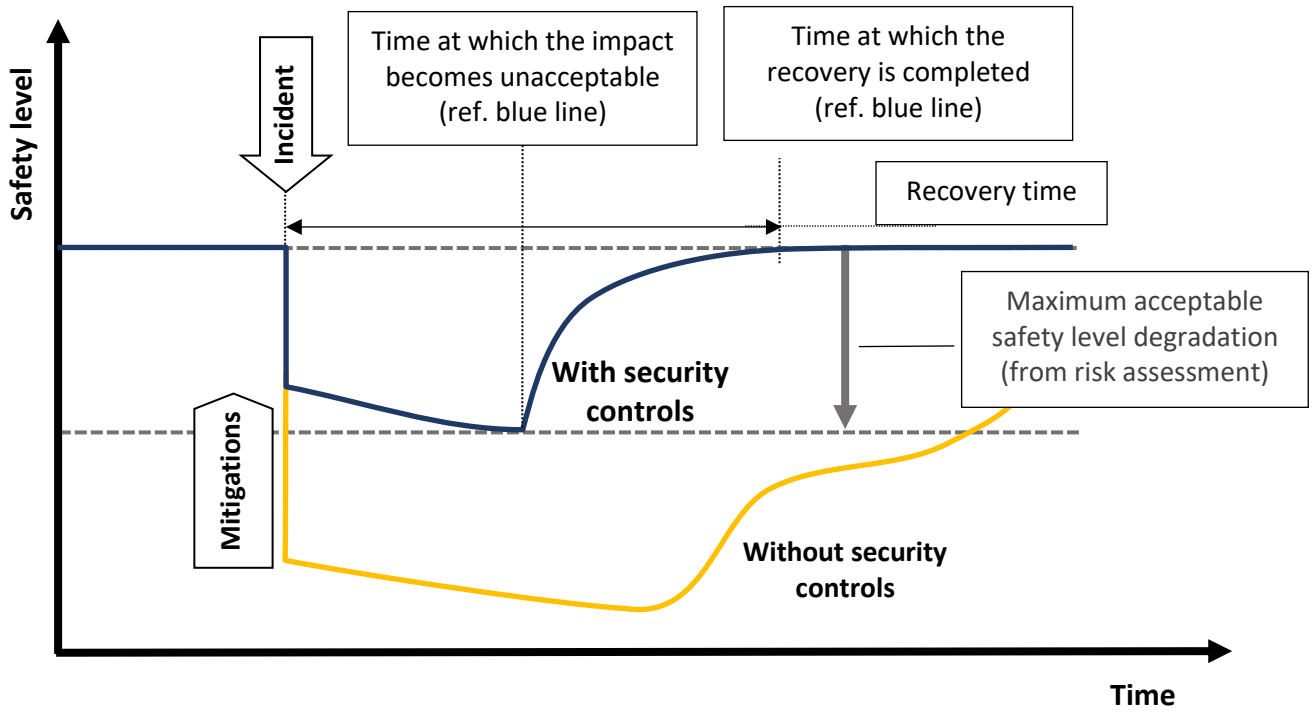

Figure 1: Conceptual framework for the definition of the response and recovery objectives

As mentioned, there might be different relations between the level of operations and safety that would lead to a different representation of the above figure. In certain cases, an incident may have a

delayed effect on the safety level (e.g. a compromised development environment) as depicted in Figure 2, or it may have no impact if properly controlled, as in the case of the compromised software loading process mentioned before that is depicted in Figure 3.

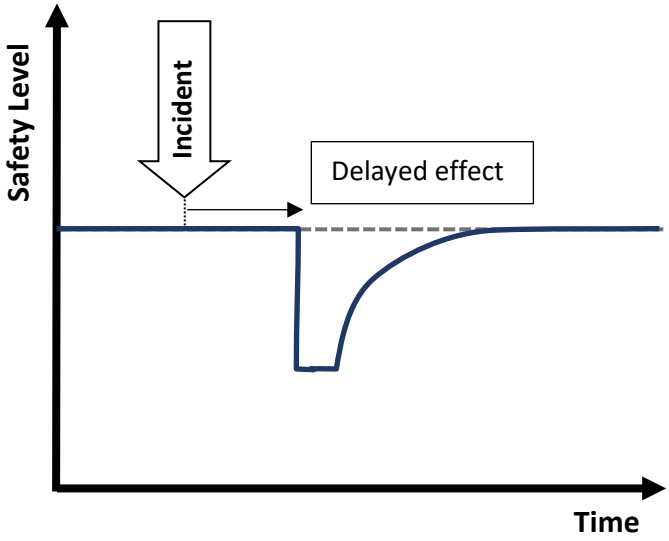

Figure 2: Incident with a delayed effect on safety

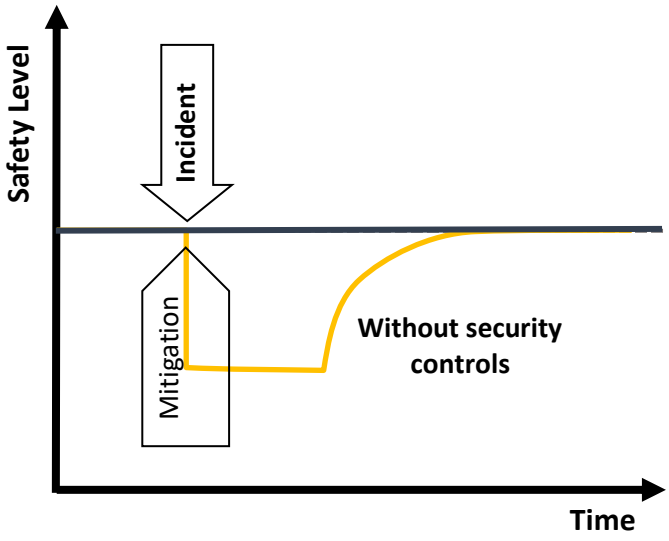

Figure 3: Incident with fully mitigated effect on safety

Moreover, it should be noticed that there might be different ways the same incident can be dealt with, since there are several factors that may affect safety.

In practical terms, the objectives for recovery time referred to in AMC1 IS.I.OR.220(c) may be expressed as a list of resources and services to be restored by order of priority, within the scope of the recovery. Guidance about objectives for recovery time can be found in EUROCAE ED-206 – Chapter 7.3.5.

GM1 IS.I.OR.220 (c) Information security incidents – detection, response and recovery

A recovery procedure or recovery plan should describe incident recovery actions and the internal or external resources that are involved (e.g. staff, IT, buildings, providers). Guidance about incident recovery plan can be found in EUROCAE ED-206 – Chapter 7 – Recover.

The resources required to apply the recovery measures should be available in order to implement recovery actions in a timely manner after an incident has occurred. Those resources may be internally available or provided by contracted organisations as foreseen by IS.I.OR.235. The contracting of recovery activities should be established before an incident occurs (proactive), and the contract should include provisions for the contracted party to react in a timely manner.

The return to a safe and secure state may initially require emergency measures, which are actions that are initiated based on the best information available at the time, before a complete understanding of the situation is achieved and these measures can potentially degrade the level of service or functionalities. The return to a safe and secure state should be evaluated against the initial risk assessment and may only temporarily differ from the normal operational conditions. However, any increase of the residual risk and the duration of this risk increase, i.e. due to the implementation of emergency measures, should be documented and accepted at the right level of accountability.

The recovery activities mentioned herein may also be the outcome of the response to incidents for which the organisation has received information that requires the implementation of adequate measures in order to react to security incidents or vulnerabilities with a potential impact on aviation safety.

In such context the organisation may not have a process or a recovery plan covering the specific occurrence. Therefore, the definition from the organisation of a specific recovery plan and its approval by the competent authority is usually required.

AMC1 IS.I.OR.225 Response to findings notified by the competent authority

The compliance with IS.I.OR.225 should be demonstrated as required under the implementing regulation for the applicable organisation's domain.

GM1 IS.I.OR.225 Response to findings notified by the competent authority

The requirement for the categorisation of findings and the period within which the actions in IS.I.OR.225(a) should be performed can be found in the implementing regulation for the domain, under the authority requirements. For the opening of findings related to this Regulation, the competent authority will follow the above-mentioned requirement.

GM1 IS.I.OR.230 Information security external reporting scheme

Organisations are required to report occurrences to their competent authority. In most cases, the competent authority is the one which has certified or approved the organisation.

EXAMPLES

Design organisations approved by EASA: EASA is the competent authority.

Air operators certified by the competent authority of a Member State: the competent authority of the Member State is the competent authority.

SPECIAL CASES

In a situation where an organisation has two air operator certificates (AOCs) under two different States (State A and B), it shall report occurrences involving aircraft operating under the State A AOC to the State A competent authority and occurrences involving aircraft operating under the State B AOC to the State B competent authority.

For organisations which are not certified or approved, the competent authority is that of the State in which the organisation has established its legal representation, for example: a ground handling organisation reports its occurrences under Regulation (EU) No 376/2014 to the State in which it is established.

For organisations holding multiple approvals, the reporting will be done to the competent authority of the approved part of the organisation where the incident has occurred or the vulnerability discovered. In case the incident/vulnerability affects multiple approvals, the reporting will be done to all the competent authorities.

For organisations holding an approval but operating outside EU (e.g. Part-145), EASA is the competent authority and they have to report to the Agency.

Dual-use aircraft — a vulnerability may need to be reported through both the military and civil reporting systems if it affects a dual-use function/system. Information reported through the civil reporting system should be sanitised (i.e. all sensitive information has been properly removed).

AMC1 IS.I.OR.230(a)&(b) Information security external reporting scheme

In order to comply with the provisions under IS.I.OR.230 (a) and (b), the organisation should report:

(a) under the Regulation (EU) No 376/2014 framework, any occurrence covered by this Regulation that is originated from intentional unauthorised electronic interactions. It is the responsibility of the competent authorities under Part-IS to ensure compliance with Article 7 of this Regulation and to filter out the part of the information security incident that needs to be shared with the information security competent authorities designated under Article 8 of Directive (EU) 2016/1148;

(b) information security incidents having a potential significant risk to aviation safety not covered under Regulation (EU) No 376/2014;

(c) vulnerabilities that pose a significant risk to aviation safety and are not patched through an approved vulnerability management strategy in accordance with AMC1 IS.I.OR.215(a)&(b).

GM1 IS.I.OR.230(a)&(b) Information security external reporting scheme

RELATION BETWEEN IS.I.OR.230(b) AND REGULATION (EU) NO 376/2014

Regulation (EU) No 376/2014 of the European Parliament and of the Council lays down requirements on the reporting, analysis and follow-up of occurrences in civil aviation. Compliance with point IS.I.OR.230(b) does not exempt organisations from compliance with Regulation (EU) No 376/2014.

For each category of reporter, Regulation (EU) 2015/1018 defines the nature of items to be mandatorily reported. Regulation EU) No 376/2014 also considers voluntary reporting of other items that are perceived by the reporter as a threat to aviation safety.

Furthermore, compliance with Regulation (EU) No 376/2014 does not exempt organisations from compliance with point IS.I.OR.230(b). However, this should not give rise to two parallel reporting systems, and point IS.I.OR.230(b) and Regulation (EU) No 376/2014 should be seen as complementary in that respect.

In practice, this means that reporting obligations under point IS.I.OR.230(b) on one hand and reporting obligations under Regulation (EU) No 376/2014 on the other hand are compatible. These reporting obligations may be discharged using one reporting channel. In addition, any natural or legal person that has more than one role subject to the obligation to report may discharge all those obligations through a single report. Organisations are encouraged to properly describe this in their organisation manual, to address cases in which the responsibilities are discharged on behalf of the organisation.

FOLLOW-UP ANALYSIS

When the analysis of an occurrence reported under Regulation (EU) No 376/2014 later identifies that the root cause or the contributing factor of the occurrence was an intentional unauthorised electronic interaction, the organisation should update its notification to the competent authority.

VULNERABILITY MANAGEMENT STRATEGY

Guidance regarding the vulnerability management strategy can be found in EUROCAE ED-206, Chapter 3.4 — Vulnerability Management Considerations. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

SIGNIFICANT RISK TO AVIATION SAFETY

Significant risk to aviation means unsafe condition, i.e. one that can result in an accident or a serious incident (as defined in ICAO Annex 13).

Note: The notion of unsafe condition also covers cases when the security incident violates the independence assumptions on system failure that are considered independent from a safety assessment perspective.

AMC1 IS.I.OR.230(c) Information security external reporting scheme

Within the overall limit of 72 hours the degree of urgency for submission of a report should be determined by the level of hazard judged to have resulted from the occurrence. Where an occurrence is judged by the person identifying the possible unsafe condition to have resulted in an immediate and particularly significant hazard, the competent authority expects to be advised immediately and by the fastest possible means (telephone, fax, email, telex, etc.) of whatever details are available at that time.

This initial notification should be followed up by a report within 72 hours. Where the occurrence is judged to have resulted in a less immediate and less significant hazard, the report submission may be delayed up to the maximum of 3 additional days in order to provide more details.

GM1 IS.I.OR.230(c) Information security external reporting scheme

Guidance regarding the reporting of security incidents and vulnerabilities can be found in EUROCAE ED-206, Chapter 6.4.2.2 – Reporting Timeline and Chapter 6.4.5 – Reporting Information Content. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

Note: The person reporting an occurrence under Regulation (EU) No 376/2014 may not have the capability to determine the nature of the occurrence. This is particularly true for information security and the result can come from forensic analysis that determines the information security nature of the occurrence. The evaluation will be done as part of the initial internal reporting process (see IS.I.OR.215 and relevant AMC). The evaluation of the occurrence can demonstrate the possibility that it materialises into an unsafe condition taking into account the likelihood of realisation.

GM1 IS.I.OR.235 Contracting of information security management activities

The objectives of point IS.I.OR.235 are:

(a) to protect critical and sensitive information and assets when being handled by contracted organisations (including organisations in the supply chain) either at their facilities or organisation facilities, or when being transmitted between the organisation and contracted organisations, or being remotely accessed by contracted organisations;

(b) to prevent information security risks from being introduced through products and services developed or provided by the contracted organisations to the organisation, in the frame of the provision of information security management activities;

(c) to ensure that information security risks are managed throughout all the stages of the relation with the contracted organisations.

GM2 IS.I.OR.235 Contracting of information security management activities

The contracting of information security management activities is a means to allocate tasks from the contracting organisation to third parties (contracted organisations). The contracting organisation remains accountable for compliance with this Regulation.

GM3 IS.I.OR.235 Contracting of information security management activities

EXAMPLES

Examples of security management activities required under IS.I.OR.200 that can be contracted.

IS.I.OR.200 activity	Contracted activity
a-1: establishes a policy on information security describing the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;	Security policy drafting and consultancy
a-2: identifies and reviews information security risks in accordance with point IS.I.OR.205;	Identify activities, facilities and resources. Identify interfaces with other organisations which could be exposed to information security risks. Perform risk analysis or part of it, e.g. identify and classify information security risks.
a-3: defines and implements information security risk treatment measures in accordance with point IS.I.OR.210;	Define, develop and implement measures. Verify the initial and the continued effectiveness of the implemented measures (e.g. Red-Team/Blue-Team exercises, penetration testing, vulnerability scanning, etc.). Communicate to the involved stakeholders the outcome of the risk assessment and their responsibilities as part of the risk treatment process.
a-4: implements an information security internal reporting scheme in accordance with point IS.I.OR.215;	Define, develop and implement an internal reporting scheme to enable the collection and evaluation of information security events and vulnerabilities of equipment, processes and services.

IS.I.OR.200 activity	Contracted activity
a-5: defines and implements, in accordance with point IS.I.OR.220, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety except as permitted by point IS.I.OR.205(e), and responds to, and recovers from, those information security incidents;	Define, develop and implement measures to detect events. Define, develop and implement measures to respond to any event conditions. Define, develop and implement measures aimed at recovering from information security incidents.
a-6: implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;	Implement immediate reaction measures to a security incident or vulnerability as notified by the competent authority.
a-7: takes appropriate action, in accordance with point IS.I.OR.225, to address findings notified by the competent authority;	Identify root cause. Define corrective action plan. Provide evidence of the corrective actions implemented to close the finding.
a-8: implements an external reporting scheme in accordance with point IS.I.OR.230 in order to allow the competent authority to take appropriate actions;	Define, develop and implement an external reporting scheme to enable the communication of the information security incidents and vulnerabilities of equipment, processes and services to the competent authority and when required to the design approval holder or the organisation responsible for the design.
a-9: complies with the requirements contained in point IS.I.OR.235 when contracting any part of the activities described in point IS.I.OR.200 to other organisations;	
a-10: complies with the personnel requirements contained in point IS.I.OR.240;	Activities of the accountable manager / head of design in the frame of the provisions for a 'common responsible person' as referred to in IS.I.OR.240 Compliance monitoring as foreseen by IS.I.OR.240 Contracted organisation to ensure that sufficient personnel is on duty to perform the activities related to this Regulation Define, develop and deliver adequate training to achieve the competencies required by the staff. Perform pre-employment checks

IS.I.OR.200 activity	Contracted activity
a-11: complies with the record-keeping requirements contained in point IS.I.OR.245;	Define, develop and implement secured archiving. Provision of secure data centre (as a service) Provision of records updates
a-12: monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager or, in the case of design organisations, to the head of the design organisation, to ensure effective implementation of corrective actions;	Compliance monitoring (as foreseen by IS.I.OR.240) including the execution of independent audits
a-13: protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.	Define, develop and implement solutions to protect the confidentiality of any information.
b: In order to continuously meet the objectives described in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.I.OR.260.	Execute independent effectiveness and maturity assessments. Define, develop and implement the necessary improvement measures.
c: The organisation shall document, in accordance with point IS.I.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.I.OR.200(a), and shall establish a process for amending this documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.I.OR.255.	Production of documentation to detail all key processes, procedures, roles and responsibilities required to comply with point IS.I.OR.200(a) (e.g. information security policies, general description of the staff, procedures to specify compliance). Define, develop and implement processes for approving amendments and changes.

AMC1 IS.I.OR.235(a) Contracting of information security management activities

(a) OVERSIGHT OF THE CONTRACTED ORGANISATION

In order to demonstrate proper oversight of the contracted organisation, the organisation should have:

(1) a process to ensure compliance with the provisions regarding contracted activities contained in this Regulation;

(2) a structured process to follow the expected execution of the contract that includes:

(i) definition and agreement of the scope of the activities;

(ii) definition and review of key performance indicators;

(iii) reaction to deviation from contractual obligations;

(iv) performance of audits, according to the predefined scope and objectives, with the aim of evaluating operational and associated assurance activities.

(b) MANAGEMENT OF THE RISKS ASSOCIATED WITH THE CONTRACTED ACTIVITIES

In order to demonstrate proper management of the risks associated with the contracted activities, the organisation should meet the following criteria:

(1) A prior assessment of the suppliers is conducted before outsourcing any security management activities. The assessment should evaluate suppliers' competencies, sustainability as well as qualifications in relation to the activities to be contracted.

(2) There is an assessment of the risks associated with the provision of the contracted activities that has been agreed between the organisation under Part-IS and the contracted organisation.

(3) The organisation establishes and maintains an information security focal point with the contracted organisation.

GM1 IS.I.OR.235(a) Contracting of information security management activities

RISK ASSESSMENT ASSOCIATED WITH THE PROVISION OF THE CONTRACTED ACTIVITIES

The risk assessment should take into account the maturity level of the contracted organisation, and should consider the following:

(a) Identification and assessment of critical and sensitive information and assets that may be shared with, or provided by, external suppliers;

(b) Identification of the information security requirements of the organisation that are applicable to the contracted organisation;

(c) Evaluation, by means of a supplier assessment, of the ability of the contracted organisation (both existing and new contracted organisations) to meet the information security requirements of the contracting organisation;

(d) Assessment of risks that may be introduced by the contracted organisation.

This agreed risk assessment should also include the roles and responsibilities of the parties (i.e. contracting and contracted organisation).

GM2 IS.I.OR.235(a) Contracting of information security management activities

AUDIT OF CONTRACTED ORGANISATIONS

The following aspects should be considered by the organisation when auditing an supplier contracted to perform security management activities:

— the scope of the audit as well as the objective should be limited to processes, resources and data used for the execution of Part-IS contracted activities;

— compliance and/or implementation audits should be done at the contracting organisation's discretion;

— findings identified during an audit shall be addressed through a remediation plan with a time frame to be validated by the contracting organisation.

AMC1 IS.I.OR.235(b) Contracting of information security management activities

In order to ensure access upon request to the contracted organisation, the organisation under Part-IS should include proper clauses and requirements in the contractual documents.

The competent authority's access to the contracted organisations should be at least equivalent to that granted to the contracting organisation and, in any case, sufficient to ensure the assessment of continued compliance with the requirements within the scope of the contracted activities.

GM1 IS.I.OR.235(b) Contracting of information security management activities

Access to the contracted organisation means to have visibility of evidence for compliance of the contracted activities (such as artefacts, documents, independent certifications).

Evidence of compliance could be achieved either by transfer of documents and/or access to information at the premises in accordance with the 'audit scope' as defined in the contract.

The opportunity to visit the premises should be evaluated considering different aspects such as the sensitivity of the related information or the practical accessibility to the contracted organisation (e.g. the contracted organisation is a service provider with distributed resources).

GM1 IS.I.OR.240 Personnel requirements

The objectives of the requirements contained in points (a) through (e) are:

(a) to ensure that an effective organisational structure is in place in order to comply with the requirements of this Regulation;

(b) to provide trust to other organisations with whom they share risks.

AMC1 IS.I.OR.240(a)(2) Personnel requirements

PROMOTION OF INFORMATION SECURITY POLICY

The accountable manager of the organisation or, in the case of design organisations, the head of the design organisation should make sure that the information security policy is known and easily accessible for all staff members.

AMC1 IS.I.OR.240(a)(3) Personnel requirements – basic understanding

BASIC UNDERSTANDING OF THE REGULATION

In order to demonstrate a basic understanding of this Regulation, the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation should have:

(a) the ability to explain the overarching objectives of the Regulation and its implications for the organisation;

(b) records of training on the content of the Regulation and the technical basis to comply with it,

as well as documented work experience in areas of activities pertinent to this Regulation.

GM1 IS.I.OR.240(a)(3) Personnel requirements

BASIC UNDERSTANDING OF THE REGULATION

The training material should cover the overarching objectives of the Regulation, and the assessment should evaluate the understanding of these regulatory objectives.

AMC1 IS.I.OR.240(b)&(c) Personnel requirements

APPOINTMENT OF A PERSON OR GROUP OF PERSONS

The person or group of persons appointed under point IS.I.OR.240(b) with the responsibility to ensure compliance with the requirements of this Regulation should represent the management structure of the organisation.

The person or group of persons should be directly responsible to the accountable manager for providing guidance, direction and support for the planning, implementation and operation of the process and standards to comply with the Regulation. They should have direct access to keep the accountable manager properly informed on compliance and security matters (for instance, through meetings organised on a regularly basis).

Appointments should take into account the possibility that a person may not be able to carry out the organisational tasks assigned to them for a period of time, and thus also identify the necessary deputies.

These nominated persons should demonstrate a complete understanding of the requirements of this Regulation, to be able to ensure that the organisation's processes and standards accurately reflect the applicable requirements. It is their role to ensure that compliance is proactively managed, and that any early warning signs of non-compliance are documented and acted upon.

A description of the functions and the responsibilities of the appointed persons and deputies, including their names, should be contained in the ISMM (see point IS.I.OR.250).

GM1 IS.I.OR.240(b) Personnel requirements

A condition of a lengthy absence occurs when a person is unable to fulfil the assigned organisational duties and therefore a potential vulnerability may arise.

GM1 IS.I.OR.240(b)&(c) Personnel requirements

Appointments should be made by email, organisational chart, roles & responsibilities table, etc. usually in use by the organisation. The organisation may adopt any titles for the foregoing managerial positions, but it should identify to the competent authority the titles and the persons chosen to carry out these functions.

AMC1 IS.I.OR.240(d) Personnel requirements

COORDINATION

The criteria to establish coordination that ensures adequate integration of the information security management within the organisation are the following:

(a) the scope and boundaries of the organisations have been established and communicated to the common responsible person;

(b) the requirements of this Regulation have been communicated to and shared with the common responsible person;

(c) the common responsible person has direct access to the accountable manager;

(d) issues are proactively managed and any early warning signs of non-compliance are documented and acted upon.

GM1 IS.I.OR.240(e) Personnel requirements

COMMMON RESPONSIBLE PERSON

The common responsible person should be capable of managing the organisation's cybersecurity strategy and its implementation to ensure the achievement of the objectives described in Article 1. If this person is delegated by the accountable manager or, in the case of design organisations, by the head of the design organisation, for the activities under this Regulation, this person should also be given the appropriate delegation that is necessary to implement the provisions of IS.I.OR.200, including the authority and the financial means to mobilise and control the resources across the organisations, or parts of the organisation involved.

According to the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022, this person may be described, for instance, as (Chief) Information Security Officer, Cybersecurity Programme Director or Information Security Manager.

AMC1 IS.I.OR.240(f) Personnel requirements

PERSONNEL SUFFICIENCY

To determine the sufficiency of the personnel, the following elements should be taken into consideration:

— the organisational structures, policies, processes and procedures subject to information security management;

— the amount of coordination required with other organisations, contractors and suppliers;

— the level of risk associated with the activities performed by the organisation.

GM1 IS.I.OR.240(f) Personnel requirements

PERSONNEL SUFFICIENCY

For the purpose of this Regulation, personnel refers to the combination of the personnel directly employed by the organisation, as well as the personnel contracted as specified in IS.I.OR.235.

The activities reported in Appendix II 'Main tasks stemming from the implementation of the Part-IS Regulation' should be considered when establishing the organisational structure necessary to comply with the requirements of this Regulation.

AMC1 IS.I.OR.240(g) Personnel requirements

PERSONNEL COMPETENCE

To determine the competence needed by the personnel performing the activities, the following elements should be taken into consideration:

— work roles and the associated tasks;

— required knowledge, skills and abilities.

As part of the process to ensure that personnel maintain the necessary competence, the organisation should:

— assess the personnel qualifications and experience with respect to the required competence for the assigned work roles to identify gaps;

— align the personnel qualifications and experience with the expected competence by either organising adequate learning programmes for existing personnel members, recruiting new resources, or a combination thereof.

GM1 IS.I.OR.240(g) Personnel requirements

TRAINING PROGRAMME

A training programme should start with the identification of the competence required by the personnel for each role, followed by the identification of the gaps between the existing competence and the required one.

In order to develop the list of competencies an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the NICE (National Initiative for Cybersecurity Education) based on the NIST Cybersecurity Framework (NIST CF).

The competencies listed in Appendix II, stemming from the NIST CF, that are mapped to the main tasks of this Regulation may be used to establish a baseline to identify the aforementioned competence gaps.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the organisation's needs considering the size, scope, required competencies, and complexity of the organisation.
Finally, as information security/cybersecurity evolves due to the rise of new threats, the organisation should periodically review the adequacy of the training programme.

AMC1 IS.I.OR.240(h) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Regarding any assigned role and task, the organisation should specify all information security responsibilities an employee has in a clear and transparent manner.

As part of this, the employee should acknowledge, in a traceable and verifiable manner, understanding of the instructions received as well as the expected roles and responsibilities.

GM1 IS.I.OR.240(h) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Acknowledgement of receipt such as a valid electronic or wet signature, confirmation email, etc., is a traceable proof of acknowledgement.

AMC1 IS.I.OR.240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

(a) The establishment of a person's identity should be determined on the basis of documentary evidence.

(b) Regarding the establishment of trustworthiness, a standard level of vetting, which includes verification of:

(1) employment, education and any gaps during at least the preceding 5 years;

(2) criminal records in all states of residence during at least the preceding 5 years,

should always be completed, taking also into account the relevant national laws and regulations.

(c) In case the information system and data to be accessed have been associated with a high severity of the safety consequences in accordance with GM1 IS.I.OR.205(c), an enhanced level of vetting should be performed for persons having administrator rights or unsupervised and unlimited access, or having been otherwise identified in the risk assessment in accordance with IS.I.OR.205.

(d) An enhanced level of vetting should include the verification, to be completed in accordance with relevant national laws and regulations, of:

(1) employment, education and any gaps during at least the preceding 5 years;

(2) criminal records in all states of residence during at least the preceding 5 years;

(3) intelligence and any other relevant information (e.g. available to the national competent authorities) that is considered to be relevant for the suitability of a person to work in a function which requires an enhanced level of vetting.

GM1 IS.I.OR.240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

Enhanced level of vetting may be used when already existing controls or mitigation measures for risk treatment identified during the risk analysis rely on organisational/operational procedures. Thus, enhanced level of vetting is needed for personnel who applies such measures —for instance, correct configuration and administration of information technologies, database operations, security monitoring, etc.

Intelligence and any other relevant information should be gathered by screening and analysing public sources such as social media and websites.

Standard and enhanced background check, as defined in Regulation (EU) 2015/1998, are suitable for the standard and enhanced level of vetting respectively. However, it should be noted that the standard and enhanced levels of vetting referred to in AMC1 IS.I.OR.240(i) do not constitute compliance with the provisions on background checks as defined in Regulation (EU) 2015/1998.

GM1 IS.I.OR.245 Record-keeping

Records are required to document results achieved or to provide evidence of activities performed. Records become factual when recorded and cannot be modified. Therefore, they are not subject to version control. Even when a new record is produced covering the same issue, the previous record remains valid.

The ‘approval received’ referred to in point (a)(1)(i) includes any ‘certificate’ received by the organisation when it is foreseen by the implementing rule for its domain.

AMC1 IS.I.OR.245(a)(1)(vi)&(a)(5) Record-keeping

When complying with the requirements under points (a)(1)(vi) and (a)(5), the organisation should establish a data retention policy defining procedures to:

(a) manage relevant security data files;

(b) establish the periodical assessment of their content; and

(c) define the criteria to allow deletion of events when the objective of the requirement under (a)(5) is no longer met.

GM1 IS.I.OR.245(a)(1)(vi)&(a)(5) Record-keeping

The objective of the requirement under (a)(1)(vi) is to ensure detection of possible indication of compromise or vulnerabilities which are not obvious by normal operation (e.g. previously unknown situations), while the objective of the requirement under (a)(5) is to allow the necessary flexibility to control the volume of the stored security events.

Records of information security events include those events identified to be within the scope of the detection activities under IS.I.OR.220(a), as well as other security data produced by assets that have been identified under IS.I.OR.205.

A data retention policy clarifies what information should be stored or archived and for how long. Some guidance about data retention can be found in EUROCAE ED-206 Chapter 2.6.

Once a data set completes its retention period, it can be deleted or moved as permanent historical data to a secondary or tertiary storage.

AMC1 IS.I.OR.245(c)&(d) Record-keeping

When complying with the requirements under points (c) and (d) for all the records required by points IS.I.OR.245 (a) and (b), the organisation should consider the following:

(a) Records should be kept in paper form or in electronic format or a combination of both media. The records should remain accessible whenever needed within a reasonable time and usable throughout the required retention period. The retention period starts when the record has been created.

(b) Records data integrity and availability should be protected in consistency with protection of corresponding operational data, and as such, should be within the scope of the ISMS.

(c) Backup/archiving systems should be protected against unauthorised access (i.e. data leakage attempts against personal data/modification of records) and thus should have security measures implemented in consistency with the level of cyber risk associated with them.

(d) Once records shall not be retained anymore, the destruction of records and decommissioning of assets used for their storage should be implemented appropriately.

GM1 IS.I.OR.245(c)&(d) Record-keeping

RECORDS ACCESSIBILITY THROUGHOUT THE RETENTION PERIOD

It is recommended to follow best practices for data retention and backup strategies, such as using automated backup tools, segregation or geographical separation of the backup storage location(s), and to consider offline backups to prevent ransomware risks. These criteria should be considered also when record-keeping is contracted to service providers with distributed resources.

Special attention should be paid to significant hardware and software changes, ensuring that stored digital records remain accessible and readable. (e.g. file system, application file format, forward compatible database versions, etc.). Paper-based information needs to be archived in an adequate environment, in which records are protected against long-term degradation factors (e.g. heat, light, humidity).

RECORDS DATA INTEGRITY AND PROTECTION FROM UNAUTHORISED ACCESS

A commonly used method to achieve authenticity and integrity protection is the use of digital signatures at document level. Digital signatures can be added to the document's file (e.g. PDF) to ensure that a record has not been modified by someone other than its author (integrity) and that the author is who is expected to be (authenticity).

Moreover, to prevent unauthorised access, a record can be protected with a password at file level. Commercial applications feature built-in basic password protection functions for their file formats. Access protection can also be achieved by protecting the environment where the individual records are stored (e.g. access protection on databases, file shares, directories, etc.).

GM1 IS.I.OR.255 Changes to the information security management system

Point IS.I.OR.255 is structured as follows:

Point (a) introduces the possibility for the organisation to agree with the competent authority that changes to the ISMS can be implemented without prior approval as long as these changes are covered in a change procedure.

Point (b) introduces an obligation of prior approval (by the competent authority) for changes not covered by the procedure mentioned above, and also indicates how those changes should be handled.

The organisation should consider the establishment of a procedure in order to manage and notify changes to the competent authority as foreseen under IS.I.OR.255(a). In case of lack of any approved procedure, the organisation will have, for any change, to apply for and obtain an approval as required under IS.I.OR.255(b). In any case, all changes should be notified to the competent authority upon implementation.

GM1 IS.I.OR.250(a) Information security management manual (ISMM)

The organisation may choose to document some of the information required under point IS.I.OR.250(a) in separate documents (e.g. procedures). In this case, it should ensure that the manual contains adequate references to any document kept separately. Any such documents are then to be considered an integral part of the organisation's information security management system manual.

AMC1 IS.I.OR.255 Changes to the information security management system

The procedure should cover the change management and the criteria for the notification of changes. The change management should explain how changes are managed, including the evidence that should be produced to describe a change and its impact.

With regard to prior approval of changes, the organisation may, upon valid justification in the developed procedure, propose changes that can be implemented without the need for such prior approval by the competent authority.

Without prejudice to the communication regarding changes as required under the implementing rule for the domain, the procedure should take into account the criticality of the changes when proposing how they will be managed. In particular, those changes that could have a significant impact on achieving or maintaining compliance with the provisions under Part-IS, or which could lead to an unacceptable level of risk (e.g. as per the guidance provided in GM1 IS.I.OR.205(c)) should be subjected to rigorous scrutiny.

When applying for prior approval of a change not covered under the approved procedure, at least the following information should be provided:

— the nature and purpose of the change;

— the implementation plan of the change;

— the verification plan of the change;

— the impact on aviation safety introduced by the change.

A significant deviation from the original plan during the change process should be considered as a new change to be communicated to the competent authority to obtain approval.

GM2 IS.I.OR.255 Changes to the information security management system

Changes within the following areas should be considered as potentially resulting in a significant impact on establishing or maintaining compliance with the provisions under Part-IS:

(a) changes to the scope of the ISMS, as per AMC1 IS.I.OR.200(a)(1), interfaces or related policies;

(b) changes in responsibilities and accountability as well as in the organisational structure involving the implementation and continuing monitoring of compliance with this Regulation;

(c) changes to the methodology used for risk management;

(d) changes to the incident management process.

GM3 IS.I.OR.255 Changes to the information security management system

RELATION BETWEEN CHANGES TO THE ISMS AND CONTINUOUS IMPROVEMENT

Changes stemming from the continuous improvement process established by the organisation (see IS.I.OR.260) should be handled as any other change according to the guidelines in AMC1 IS.I.OR.255 and GM2 IS.I.OR.255.

EXAMPLE SCENARIOS OF CHANGES WITH A SIGNIFICANT IMPACT ON ESTABLISHING OR MAINTAINING COMPLIANCE WITH THE PROVISIONS UNDER PART-IS, OR WHICH COULD LEAD TO AN UNACCEPTABLE LEVEL OF RISK

With reference to GM2 IS.I.OR.255, below are some examples of changes that could have a significant impact on achieving or maintaining compliance with the provisions under Part-IS, or which could lead to an unacceptable level of risk:

(a) Changes to the scope of the ISMS, as per AMC1 IS.I.OR.200(a)(1), interfaces or related policies:

- The organisation expands its business functions, and integrates another company within its organisational structure.
- The organisation has identified non-conformities indicating an incorrect scope.
- The organisation amends its information security policy and/or information security objectives with a potential impact on aviation safety.
- Changes to the interfaces of the organisation resulting e.g. from modification in the insourced or outsourced activities.

(b) Changes in responsibilities and accountability as well as in the organisational structure involving the implementation and continuing monitoring of compliance with this Regulation:

- The accountable manager or, in the case of design organisations, the head of the design organisation, has delegated certain responsibilities under Part-IS to a person or a group of persons.
- The organisation contracts information security management activities as per IS.I.OR.235.

(c) Changes to the methodology used for risk management:

— The organisation changes the classification for likelihood or impact in their risk management methodology e.g. to obtain more granularity.

— The organisation implements changes to their risk treatment methodology.

— The organisation integrates its information security risk management into existing management systems.

(d) Changes to the incident management process:

— The organisation decides to contract incident management activities.

— The organisation changes the process to notify incidents and the criteria to escalate to higher management for a quicker resolution.

— The organisation changes its incident recovery procedure.

EXAMPLE SCENARIOS OF CHANGES WITHOUT A SIGNIFICANT IMPACT

— After a successfully detected security event which could have easily evolved to an incident, the organisation decides to roll out an extensive cyber security awareness campaign for all employees.

— Update in the staff training programme and/or training content as a result of the continuous improvement processes established within the organisation

— The organisation replaces the software tool that it uses for encrypting sensitive files with another software solution.

— The organisation has decided to make an internal restructuring for business reasons, changing the names of departments or sections, without making any changes in the responsibilities and accountability (e.g. accountable manager) involving the ISMS of the organisation.

— The organisation decides to update an existing preventive control e.g. configuring a new firewall in its internal network

AMC1 IS.I.OR.260 Continuous improvement

The continuous improvement process (CIP), as required by IS.I.OR.200(b), should aim to continuously improve the effectiveness, suitability and adequacy of the ISMS. This should be achieved by a proactive and systematic assessment of the ISMS and all of its elements including its maturity. The assessment should take into account the outcomes and conclusions of other information security and assurance processes including audits, management reviews, evaluation of performance, effectiveness and maturity, as well as the outcomes of the derived corrective actions and corrections.

The steps to be performed should be at least the following:

(a) Identify improvement opportunities based on the outcomes of the assessment of the ISMS with respect to its suitability, effectiveness, adequacy and, if deemed necessary, efficiency, as well as any other suggestion for improvement. The assessment should consider performance indicators which reflect its processes and elements and the defined objectives for effectiveness and maturity.

(b) Evaluate the identified opportunities regarding cost benefit, absence or reduction of undesired effects and achievement of the targeted objectives and intended outcomes.

(c) Propose the evaluated improvement opportunities to the management, and recommend actions to support their review and decision-making.

(d) According to the decision taken under point (c), plan, develop and implement actions and changes to the ISMS, its processes or elements to achieve the improvements.

(e) Evaluate the effectiveness of the implemented actions and ISMS changes, and, as applicable, verify that the root cause of identified deficiencies has been eliminated.

The management should assess and review the outcomes of the CIP at planned intervals to ensure the continuing effectiveness, adequacy and suitability of the ISMS, to decide on the prioritisation of the implementation of actions and changes, as well as to revise or set new objectives or targets for continuous improvement.

GM1 IS.I.OR.260 Continuous improvement

Point IS.I.OR.260 covers assurance processes for the ISMS in a manner that can be considered equivalent to the safety assurance in ICAO Doc 9859 'Safety Management Manual (SMM)', which includes performance monitoring and measurement, management of change and continuous improvement of the SMS.

In this Regulation:

— IS.I.OR.260(a) addresses, using adequate performance indicators, the effectiveness and maturity assessment of the ISMS;

— IS.I.OR.260(b) addresses the improvement measures, i.e. corrections and corrective actions, for the deficiencies detected in IS.I.OR.260(a) and the continuous improvement process.

Similar provisions for continuous improvement are foreseen in other information management systems such as ISO 27001 (see Appendix II to this document).

The context and risk environment of organisations are never static and therefore require a dynamic adaptation, evolution and change of the entity's objectives, architectures, organisational structures and processes to maintain the information security risks at an acceptable level. Consequently, the ISMS should be considered as an evolving and learning part/element of the entity which needs to be continuously monitored and improved to ensure alignment with the entity's safety objectives and effectiveness.

The CIP aims to continuously improve the effectiveness, suitability, adequacy and, if deemed necessary, the efficiency of the ISMS. An entity may integrate the Part-IS CIP in some other already operated CIP and may apply methods such as Plan-Do-Check-Act (PDCA) Cycle or Define-Measure-Analyse-Improve-Control (DMAIC) (see also GM1 IS.I.OR.200).

The CIP is based on a proactive and systematic assessment of the ISMS and all its elements including the information security processes and controls driven by the ISMS. The assessment should be carried out against organisational targets for desired levels of performance, effectiveness and maturity. These targets, besides ensuring the achievement of compliance with the requirements under this Regulation,

may also aim to include objectives established by the entity's policy or standards and by management decisions.

The above-mentioned assessment is based on the outcome of performance evaluations, audits, risk and incident processes, as well as already applied corrections and corrective actions. Some factors that should be considered when performing the assessment are the following:

— **Adequacy** refers to whether the system uses industry standards for information security in a sufficient manner with regard to compliance with the requirements of this Regulation.

— **Effectiveness of the ISMS** and the effective implementation of processes and controls driven by the ISMS is assessed by analysing whether:

  — the information security risks are managed to achieve the safety objectives;

  — the intended outcomes of the ISMS are achieved, and the requirements or objectives are met;

  — all types of deficiencies are managed including failures to fulfil or correctly implement a requirement or control.

— **Efficiency** of the ISMS refers to the implementation of streamlined processes; however, efficiency improvements should not adversely impact effectiveness.

Identification of improvement opportunities

Improvement opportunities may be identified from the results of the CIP assessment or may be introduced as suggestions from other sources. The identification often involves deviations or corrective actions as well as ineffective processes or controls which are not remediated.

Suggestions for improvements stem from sources including:

— Risk management: the results of regular risk analysis and subsequent risk treatment are a primary factor in improving the ISMS, where the risk treatment process involves monitoring of the implemented security measures and evaluating their effectiveness.

— Performance & effectiveness evaluation: conclusions from (key) performance indicators, their measurement, analysis and continued monitoring as well as the result of the assessment of the effectiveness including the outcomes of the subsequently applied corrections and corrective actions

— Evaluation of maturity including the results of the subsequent corrections and corrective actions

— Lessons learned from the security incident detection, handling and response process and from a potential treatment of a root cause

— Results of (internal) audits may be used to verify whether the ISMS and controls within the audit scope meet the entity's requirements, and to determine where there are potential areas for improvement.

— Review and evaluation by management, review of the current action plan, setting or revision of the objectives or decision on improvement opportunities and actions

— Entity's suggestion programme (suggestions for improvement), reviews, surveys or assessments with employees or feedback from suppliers or interfacing parties

Any outcome of this process should be documented. The resulting actions may be integrated into an overarching action plan which is centrally consolidated and periodically reviewed according to the relevant policies. The resulting action plan may be further divided into a tactical, short-/mid-term action plan and a strategic, long-term action plan.

AMC1 IS.I.OR.260(a) Continuous improvement

(a) **ISMS EFFECTIVENESS EVALUATION**

When complying with IS.I.OR.260(a), the organisation should have a process in place to monitor, measure, evaluate and review the effectiveness of its ISMS that defines:

(1) who monitors, measures, analyses and evaluates the results and takes accountable decisions;

(2) when the above steps should be performed;

(3) which methods for monitoring, measurement, analysis and evaluation are applied to ensure comparable and reproducible results.

The frequency of the assessments should be commensurate with the level of risk established under IS.I.OR.205.

The process to monitor, measure, evaluate and review the effectiveness of the organisation's ISMS referred to under AMC1 IS.I.OR.260(a) should include as a minimum:

(1) the gathering and retention of metrics of the activities, and additional information that could be useful for monitoring purposes;

(2) the analysis of the metrics in order to identify trends and deviations from predefined performance targets.

(b) **ISMS MATURITY EVALUATION**

The organisation should assess the maturity of its ISMS using a suitable maturity model in order to identify areas for improvement to the ISMS. To do so, the organisation should:

(1) define or adopt a maturity model which represents a set of important and relevant processes and capabilities that are expected to be implemented and maintained;

(2) for each assessed process or capability, define in the model criteria against which specific aspects, characteristics and effectiveness should be assessed and evaluated when determining a maturity level;

(3) define for each assessed process or capability its desired target maturity level.

(c) For each assessed security process or capability contained in the maturity model, the organisation should:

(a) evaluate and justify the current maturity level;

(b) identify any area for improvement it should make to reach the targeted maturity level;

(c) collect and record the evidence regarding strengths and weaknesses of the implemented ISMS and its evaluated maturity.

GM1 IS.I.OR.260(a) Continuous improvement

(a) As general guidance, the elements of the ISMS that should be monitored, measured and evaluated should be, as a minimum:

(1) the risk assessment and treatment process (including risks at the interfaces with other organisations);

(2) the management of non-conformities and corrective actions;

(3) the incident and vulnerability management;

(4) the personnel competence management.

(c) Existing maturity models for ISMS maturity evaluation

As general guidance, for the definition or the adoption of a maturity model (MM), the following existing models may be considered:

— Cybersecurity Capability Maturity Model (C2M2), version 1.1: this model was published by the US Department of Energy in 2014. It introduces the notion of Maturity Indicator Levels (MIL) ranging from 0 to 3 and addresses not only performance levels but also performance practices (under Approach Objectives and approach progression) as well as assurance practices (under Management Objectives and institutionalization progression).

— Systems Security Engineering – Capability Maturity Model (SSE-CMM): published by ISO as ISO 21827 in 2008. It focuses on engineering practices, much less on operational practices that are split in 11 'Security Base Practices', and 11 'Project and Organizational Base Practices'. It introduces the notion of five Capability Levels, from 'Performed Informally' to 'Continuously Improving'.

— NIST Cybersecurity Framework (NIST CF), version 1.1: published by NIST in April 2018. Although it is not proposed as a MM, the framework defines four 'Implementation Tiers', from 'Partial' to 'Adaptive', which are a qualitative measure of organisational cybersecurity risk management practices. It focuses on the functionality and repeatability of cybersecurity risk management.

— ATM Cybersecurity Maturity Model, edition 1: published in February 2019 by the EUROCONTROL NM for organisations in the ATM domain. Whilst not being designed for wider application, it can be adapted as necessary. It defines five maturity levels, ranging from 'Non-existent' to 'Adaptive' inspired by the 'Tier' terminology from the NIST CSF. In fact, the model is founded on NIST CSF, together with some elements of ISO 27001.

The following Table 1 maps the MM mentioned above to a hypothetical five-level MM.

Mapping with a five levels MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial	MIL 0	Non-Existent	Performed Informally	
Defined	MIL 1 (Initial)	Partial	Planned & Tracked	Partial
Implemented	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved		Adaptive	Continuously Improving	Adaptive

Table 1: Mapping matrix of an existing MM to a hypothetical five-level MM

AMC1 IS.I.OR.260(b) Continuous improvement

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

Based on an evaluation of the impact and extent of the deficiency and the potential consequences on the ISMS, the process should include as criteria for compliance:

(a) deciding on corrections and their implementation without undue delay in order to limit the impact of the deficiency and deal with its consequences as well as, as applicable, to control or eliminate it;

(b) deciding on the need for, and the implementation of, corrective actions to eliminate the cause and contributing factors of the deficiency based on a root cause analysis and an evaluation of actions remediating the cause aimed at being proportionate to the consequences and impact of the deficiency;

(c) verifying the implemented actions:

- to be effective and to result in acceptable residual risks,
- not to have unintended side effects leading to other deficiencies, new risks, or an ISMS not aligned with the applicable requirements, as well as
- for corrective actions, to effectively remediate or eliminate the root cause;

(d) reporting to and reviewing the identified deficiencies, action plan and results of the action taken with the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s) and, as necessary, with other involved or affected roles and parties;

(e) documenting as evidence the detected deficiencies, the planned and implemented corrections and/or corrective actions with deadlines and responsible persons, the management feedback,

the outcomes of the process step under point (c) above and, if necessary, the change decisions made for the ISMS itself.

GM1 IS.I.OR.260(b) Continuous improvement

The 'necessary improvement measures' referred to in IS.I.OR.260(b) refer to correction or corrective actions to eliminate deficiencies or actions aimed at improving the effectiveness as well as the maturity of the ISMS.

A process satisfying the criteria defined in AMC1 IS.I.OR.260 should include the following aspects:

(a) identifying the extent, impact, context and triggers of the deficiency, evaluating it according to some established criteria, analysing potential consequences on the ISMS including a potential existence in other areas;

(b) deciding on corrections and their implementation to immediately limit the impact and manage the consequences of the deficiency as well as, as applicable, to control or eliminate it;

(c) deciding on corrective actions required to eliminate the (root) cause(s) of the deficiency that are proportionate to the consequences;

(d) reassessing the elements of the ISMS which may be affected by the implemented actions to ensure that no further risk is introduced;

(e) verifying the implemented actions referred to in point (c) of AMC1 IS.I.OR.260(b);

(f) reporting to and reviewing the outcomes of the process steps with the management (see point (d) of AMC1 IS.I.OR.260(b));

(g) documenting and evidencing the result of the process steps above (see point (e) of AMC1 IS.I.OR.260(b)).

APPENDIX I

Examples of threat scenarios with a potential harmful impact on safety

The following is a non-exhaustive list of examples of information security threat scenarios with a potential harmful impact on safety that may be considered by authorities and organisations.

Example 1: Aircraft cockpit communications used for air traffic control (ATC) and aircraft pilot voice and datalink communications

— Threat vector assets/domain

  — ATC voice and ground automation systems

  — ground communications providers

  — air-ground/ground-air RF communications service providers

  — aircraft and the assets used for voice and datalink communications

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety.

— Non-exhaustive summary of potential threats

  — threat (availability): jamming

  — threat (integrity): man-in-the-middle or injection attacks

  — threat (confidentiality): insider threat

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety

  — Disruption of services prevent ATC communication with a single or multiple aircraft and/or ATC ground system

  — The manipulation of data through a man-in-the-middle attack would present false information to the pilot and/or ATC system with the potential of creating a safety hazard or injection of data to the aircraft or ground systems to disrupt the service and capability.

  — There are no specific requirements for encryption of data or voice for datalink communications; however, for confidentiality purposes, the assets used to provide and deliver the services should be controlled and limited to only those resources that require access to ensure that the services cannot be disrupted and manipulated in any way.

  *NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide

supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— If the directly interconnected organisation is not an organisation that will be directly evaluated by the authority, as either part of this assessment or a separate assessment, both organisations must be prepared to follow the safety support assessment processes identified under point ATM/ANS.OR.C.005 of Regulation (EU) 2017/373 and under point IS.I.OR.205(e) of this Regulation if they are included within the scope of the end-to-end data flow.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Example 2: Use of GPS for navigation by aircraft and ATM ground systems

— Non-exhaustive summary of potential threats

  — threat (availability): jamming, system (hardware/software) vulnerability exploitation

  — threat (integrity): spoofing (GPS signal), man-in-the-middle or injection attacks (PNT data)

  — threat (confidentiality): insider threat

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety

  — Disruption of services prevents effective aircraft navigation by the aircraft pilot and crew and ATC

  — Disruption of GPS or manipulation of a GPS signal used for ATC ground-based navigation devices and automation systems that rely on GPS for ATC synchronisation affects the ability of ANSPs to provide a single or multiple aircraft with services.

  — The manipulation of data through a man-in-the-middle attack presents false information to the pilot and/or ATC system with the potential of creating a safety hazard or injection of data to the aircraft or ground systems and thus disrupts the service and capability.

  — Uncontrolled access to navigation systems and the assets used to provide navigation services allows manipulation and disruption of services.

  *NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— If the directly interconnected organisation is not an organisation that will be directly evaluated by the authority, as either part of this assessment or a separate assessment, both organisations must be prepared to follow the safety support assessment processes identified under point ATM/ANS.OR.C.005 of Regulation (EU) 2017/373 and under point IS.I.OR.205(e) of this Regulation if they are included within the scope of the end-to-end data flow.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Application of bow-tie analysis to this example

Two coordinated bow-tie analyses of different risk dimensions are combined, as the ultimate interest lies only in the aviation safety consequence.

Information security bow-tie analysis element	Aviation safety bow-tie analysis element
Information security threats 1) jamming of GPS spectrum 2) system vulnerability exploitation 3) man-in-the-middle attack 4) insider intentional interaction	
Information security preventive barriers	
Information security hazards & top events 1) disturbed GPS spectrum (hazard) → *unreliable GPS position* 2) system integrity compromised (hazard) → *system function unpredictable* 3) manipulation of information during communication (hazard) → *undetectable falsification of information* 4) access to resources not adequately controlled (hazard) → *insider gets access to system resources*	**Safety threats** 1) unreliable GPS navigation function 2) unpredictable system function 3) undetectable falsification of information 4) insider gets access to system resources
Information security mitigative barriers	**Safety preventive barriers**

	1) provision of different navigation systems (dissimilarity) 2) etc.
Information security consequences 1) loss of GPS availability (= in case of sole navigation function) 2) loss of system function integrity (= some system function inoperative) 3) loss of information integrity (= some information is incorrect) 4) loss of availability, integrity, or confidentiality (= all types of compromise possible)	**Safety hazards & top events** 1) loss of GPS signal (hazard) → unavailability of GPS information on the aircraft 2) loss of individual system function (hazard) → degraded aircraft system performance 3) loss of information integrity (hazard) → presentation of incorrect information to pilots or systems 4) loss of availability, integrity, or confidentiality (hazard) → unreliable system performance
	Safety mitigative barriers 1) Use of dissimilar navigation means 2) etc.
	Safety consequences 1) loss of airspace separation (disruption of services that prevent effective aircraft navigation by the aircraft pilot and crew and ATC) 2) disruption of ATC function or manipulation of information impacts the ability to provide services to aircraft 3) loss of airspace separation, disruption of ATC functions and services 4) disruption of ATC function or manipulation of information impacts the ability to provide services to aircraft

Example 3: Aircraft operator and aircraft maintenance organisations' software supply chain and ground infrastructure used to support aircraft management and operations

— Threat vector assets/domain

  — Aircraft operator or maintenance ground supply chain for aircraft parts, hardware and software

  — Aircraft operator or maintenance ground internal infrastructure used to manage aircraft operations (hardware/software) and other information technology assets

  — Aircraft operator information technology assets used to update systems on an aircraft (software/hardware) used for maintenance operations

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety.

— Non-exhaustive summary of potential threats

  — threat (availability): hardware/software vulnerability exploitation, system disruption

  — threat (integrity): vulnerability exploitation, compromised hardware/software/system

  — threat (confidentiality): vulnerability exploitation, compromised hardware/software/system

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety

  — threat (availability): disruption of production systems

  — threat (integrity): vulnerability exploit, compromised hardware/software/system of production systems

  — threat (confidentiality): vulnerability exploit, compromised hardware/software/system of production systems

  *NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— If the directly interconnected organisation is not an organisation that will be directly evaluated by the authority, as either part of this assessment or a separate assessment, both organisations must be prepared to follow the safety support assessment processes identified under point ATM/ANS.OR.C.005 of Regulation (EU) 2017/373 and under point IS.I.OR.205(e) of this Regulation if they are included within the scope of the end-to-end data flow.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Application of bow-tie analysis to this example

Two coordinated bow-tie analyses of different risk dimensions are combined, as the ultimate interest lies only in the aviation safety consequence.

Information security bow-tie analysis element	Aviation safety bow-tie analysis element
Information security threats 1) hardware/software vulnerability exploitation: disturbed system function 2) hardware/software vulnerability exploitation: system integrity compromised 3) hardware/software vulnerability exploitation: confidentiality of information processed by system(s) compromised	

Information security preventive barriers	
Information security hazards & top events 1) disturbed system functionality (hazard) → disrupted/unreliable system functionality 2) system integrity compromised (hazard) → system function unpredictable 3) information disclosable (hazard) → undetectable information exfiltration	**Safety threats** 1) disrupted/unreliable system functionality 2) system function unpredictable 3) undetectable information exfiltration
Information security mitigative barriers	**Safety preventive barriers** 1) Use of access controls for system administration 2) etc.
Information security consequences 1) loss of system function (= production system down) 2) loss of system function integrity (= some system function wrong/inoperative) 3) loss of confidentiality of information (= some information can leak)	**Safety hazards & top events**: 1) loss of system function (hazard) →*in operational maintenance system* 2) loss of system function integrity (hazard) → *systems operate with wrong information* 3) loss of information confidentiality (hazard) → *confidential maintenance information leaks*
	Safety mitigative barriers 1) use of back-up procedures to prevent faulty maintenance actions 2) etc.
	Safety consequences 1) faulty maintenance actions 2) incorrectly completed maintenance actions 3) exfiltration of information allows for identification of vulnerabilities

Example 4: Design and production organisations' software, supply chain, design and manufacturing ground infrastructure

— Threat vector assets/domain

  — Design and production organisations' supply chain for parts, hardware and software

  — Design and production organisations' ground internal infrastructure used to manage software/hardware used in the manufacturing and development of products that will be used by aircraft manufacturers, operators or ATM/ANS ground automation systems (hardware/software) information technology assets

  — Design and production organisations' information technology assets used by their customers to updated systems on an aircraft (software/hardware) used for maintenance operations or ATM/ANS ground automation systems

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Non-exhaustive summary of potential threats

  — threat (availability): systems used to store, transmit and exchange information are rendered unavailable for essential operations through denial of service attacks.

— threat (integrity): systems used to store, transmit and exchange information are compromised through man-in-the middle attacks.

— threat (confidentiality): systems used to store, transmit and exchange information are accessed by insider or external threats.

*NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Summary of threats and their potential harmful impacts on safety

— Disruption of systems used to store, transmit and exchange information in a manner that would prevent the proper management of the aircraft and its systems and adversely affect the operations of the aircraft

— Systems used to store, transmit and exchange information can no longer be considered trusted. If they are not maintained at a level to ensure that all information exchange, data and software can be considered trusted, both ground and aircraft operations are disrupted.

— Uncontrolled access to systems used to store, transmit and exchange information (including information that is received and exchanged with the supply chain) can provide technical details that could be used to craft more sophisticated attacks targeting safety-critical systems.

*NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— If the directly interconnected organisation is not an organisation that will be directly evaluated by the authority, as either part of this assessment or a separate assessment, both organisations must be prepared to follow the safety support assessment processes identified under point ATM/ANS.OR.C.005 of Regulation (EU) 2017/373 and under point IS.I.OR.205(e) of this Regulation if they are included within the scope of the end-to-end data flow.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Example 5: Training system

— Threat vector assets/domain

  — Supply chain of all software and hardware that will be used in the training systems or training devices (including flight simulators) used to train pilot or ATM/ANS ground systems personnel.

  — Internal infrastructure used in of all software and hardware that will be used in the design, manufacturing or production of products (hardware or software) that will be used in aircraft or ATM/ANS ground systems.

  — Management of internal operating domains and system of all software and hardware that will be used in the design, manufacturing or production of products (hardware or software) that will be used in aircraft or ATM/ANS ground systems.

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Non-exhaustive summary of potential threats

  — threat (availability): training systems or training devices are rendered unavailable by means of denial of service attacks when they are needed to be used.

  — threat (integrity): training systems or training devices are compromised through man-in-the middle attacks.

  — threat (confidentiality): functional models, information and data that are embedded in training systems or training devices are accessed by insider or external threats.

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Summary of threats and their potential harmful impacts on safety

  — Disruption of training systems (hardware and software) will have an impact on the organisations' ability to maintain qualified staff. It would also prevent the aircraft and its systems from being properly operated and affect maintenance operations for ATM/ANS ground systems.

  — The training model or the failure modes and associated emergency conditions differ from the real aviation system behaviour and therefore induce inappropriate responses. If the training systems cannot be trusted, this will affect the ability of organisations to maintain sufficiently qualified staff for their operations (pilots, maintenance or ATM/ANS ground personnel who have been exposed to improper training should be re-qualified).

  — Lack of control and access to training systems affects the ability of organisations to maintain a training system that is known to be in a trusted state. In addition, uncontrolled

access to training systems that embed functional models, information and data can provide technical details that could be used to craft more sophisticated attacks on the training system itself or on the real-world safety-critical system.

*NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— If the directly interconnected organisation is not an organisation that will be directly evaluated by the authority, as either part of this assessment or a separate assessment, both organisations must be prepared to follow the safety support assessment processes identified under point ATM/ANS.OR.C.005 of Regulation (EU) 2017/373 and under point IS.I.OR.205(e) of this Regulation if they are included within the scope of the end-to-end data flow.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

APPENDIX II

Main tasks stemming from the implementation of the Part-IS Regulation, including references to NIST CF 1.1 and ISO/IEC 27001:2013

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
Establish and operate an information security management system (ISMS)	Both	Management	IS.AR.200(a) IS.I.OR.200(a)	IDENTIFY	ID.RM	4 6.1.1	
Establish the scope of the ISMS according to Part-IS requirements	Both	Management	IS.AR.205(a) IS.I.OR.205(a)	IDENTIFY		4.3	
Implement and maintain a security policy	Both	Management	IS.AR.200(a)(1) IS.I.OR.200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1
Identify and review information security risks	Both	Management	IS.AR.200(a)(2) IS.AR.205 IS.I.OR.200(a)(2) IS.I.OR.205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2	
Implement security risk treatment measures	Both	Management	IS.AR.200(a)(3) IS.AR.210 IS.I.OR.200(a)(3) IS.I.OR.210	PROTECT	PR.PT	6.1.3 8.1 8.3	
Implement measures to detect security events and identify those related to aviation safety	Both	Management	IS.AR.200(a)(4) IS.AR.215 IS.I.OR.200(a)(5) IS.I.OR.215	DETECT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7
Implement measures that have been notified by the competent authority	Organisation	Operational	IS.I.OR.200(a)(6)			10.1	A6.1.3
Take appropriate remedial actions to address findings notified by the competent authority (non-compliances)	Organisation	Both	IS.I.OR.200(a)(7)			10.1	A6.1.3
Implement an external information security reporting scheme	Organisation	Management	IS.I.OR.200(a)(8) IS.I.OR.230	RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	7.4	A6.1.3 A16.1.2 A16.1.3

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
Monitor compliance with this Regulation and report findings to top management	Both	Operational	IS.AR.200(a)(8) IS.OI.R.200(a)(12)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2
Protect confidentiality of exchanged information	Both	Operational	IS.AR.200(a)(9) IS.I.OR.200(a)(13)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2
Communicate to the Agency changes regarding capability and responsibilities	Authority	Operational	IS.AR.200(a)(10)				A6.1.3
Share information to assist other competent authorities, agencies and organisations	Authority	Operational	IS.AR.200(a)(11)	IDENTIFY	ID.RA-2 ID.BE-2		A6.1.4
				PROTECT	PR.IP-8		
				RESPOND	RS.CO-3 RS.CO-5		
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Both	Management	IS.AR.200(b) IS.AR.235 IS.I.OR.200(b) IS.I.OR.260	IDENTIFY	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1
				PROTECT	PR.IP-7 PR.IP-10		
				DETECT	DE.DP-5		
				RESPOND	RS.MI-3 RS.IM-2		
				RECOVER	RC.IM-2		
Document and maintain all key processes, procedures, roles and responsibilities	Both	Management	IS.AR.200(c) IS.I.OR.200(c)	IDENTIFY	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1
				PROTECT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12		
				DETECT	DE.DP-1		
				RESPOND	RS.CO-1 RS.AN-5		
Identify all elements which could be exposed to information security risks	Both	Management	IS.AR.205(a) IS.I.OR.205(a)	IDENTIFY	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
Identify the interfaces with other organisations which could result in exposure to information security risks	Both	Management	IS.AR.205(b) IS.I.OR.205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3	
Identify information security risks and assign a risk level	Both	Management	IS.AR.205(c) IS.I.OR.205(c)	IDENTIFY	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2	
Review and update the risk assessment based on certain criteria	Both	Operational	IS.AR.205(d) IS.I.OR.205(d)	IDENTIFY	ID.RM	8.2	
Organisations under Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373 share the safety support assessment	Organisation	Operational	IS.I.OR.205(e)				
Develop and implement measures to address risks and verify their effectiveness	Both	Operational	IS.AR.210(a) IS.I.OR.210(a)	PROTECT	PR.IP PR.PT	6.1.3 8.3	
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Both	Operational	IS.AR.210(b) IS.I.OR.210(b)	IDENTIFY	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1	
				PROTECT	PR.IP-7		
Establish an internal information security reporting scheme to enable the collection and evaluation of information security events from personnel	Organisation	Management	IS.I.OR.200(a)(4) IS.I.OR.215(a) IS.I.OR.215(e)	IDENTIFY	ID.AM-3	7.4	A16.1.1 A16.1.2
Ensure that contracted organisations report information security events	Organisation	Management	IS.I.OR.215(c)	RESPOND	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Organisation	Operational	IS.I.OR.215(b)(1)-(b)(3)	IDENTIFY	ID.RA-1		A12.6.1 A16.1.1 A16.1.4
				DETECT	DE.AE-2 DE.AE-3 DE.AE-5		
Implement measures to detect in processes and operations security events which may have a potential impact on aviation safety	Both	Operational	IS.AR.215(a) IS.I.OR.220(a)	DETECT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5
				PROTECT	PR.PT-1		
Implement measures to respond to security events that may cause a security incident	Both	Operational	IS.AR.215(b) IS.I.OR.220(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5
Cooperate on investigations with other organisations that contribute to information security of its own activities	Organisation	Management	IS.I.OR.215(d)	RESPOND	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7
Implement measures to recover from information security incidents	Both	Operational	IS.AR.215(c) IS.I.OR.220(c)	RECOVER	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6
Manage risks associated with contracted activities with regard to the management of information security	Both	Management	IS.AR.220 IS.I.OR.235	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2
Define a person with the authority to establish and maintain the organisational structures, policies, processes, and procedures necessary to implement this Regulation	Authority	Management	IS.AR.225(a)	IDENTIFY	ID.AM-6	7.1	A6.1.1

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Both	Management	IS.AR.225(b) IS.I.OR.240(f)	IDENTIFY	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding information security management	Both	Management	IS.AR.225(c) IS.I.OR.240(g)	IDENTIFY	ID.AM-5 ID.AM-6	7.2	A7.1.5
				PROTECT	PR.AT-1		
Create and maintain a process to ensure that the personnel acknowledge the responsibilities with the assigned roles and tasks	Both	Management	IS.AR.225(d) IS.I.OR.240(h)	IDENTIFY	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2
Verify identity and trustworthiness of personnel who have access to information systems	Both	Management	IS.AR.225(e) IS.I.OR.240(i)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1
Archive, protect and retain records traceability for a specified time	Both	Operational	IS.AR.230 IS.I.OR.245	IDENTIFY	ID.RA-4	7.5	A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3
				PROTECT	PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1		
Correct non-compliance findings upon notification by the competent authority	Organisation	Operational	IS.I.OR.225(a) IS.I.OR.225(b)			10.1	A18.1 A18.2
Implement an information security reporting system in accordance with Regulation (EU) No 376/2014	Organisation	Management	IS.I.OR.230(a)				
Report information security incidents or vulnerabilities to the competent authority and, under certain conditions, to others	Organisation	Operational	IS.I.OR.230(b) IS.I.OR.230(c)	DETECT	DE.DP-3	7.4	A16.1.1 A16.1.2 A16.1.3
				RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5		

Part-IS main task	Applicability	Activity type	Reference			Reference	
	Authority, Organisation	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
				Function	Category	Paragraph Clause	Annex A Control
				RECOVER	RC.CO-3		
Regularly assess the effectiveness and maturity of the ISMS	Both	Operational	IS.AR.235(a) IS.I.OR.260(a)			9	A5.1.2 A12.7.1 A16.1.6
Take actions to improve the ISMS if required. Re-assess the implemented measures of the ISMS elements.	Both	Operational	IS.AR.235(b) IS.I.OR.260(b)			10	A5.1.2
Ensure accessibility of the competent authority to the contracted organisation	Organisation	Management	IS.I.OR.235(b)			9.3	A6.1.3 A15.1 A15.2
Ensure that all necessary resources are available to comply with the Regulation	Organisation	Management	IS.I.OR.240(a)(1)	IDENTIFY	ID.AM-5 ID.AM-6	7.1	A6.1.1
Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Organisation	Management	IS.I.OR.240(a)(2)& (a)(3)	IDENTIFY	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2
				PROTECT	PR.AT-1 PR.AT-4		
Nominate a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Organisation	Management	IS.I.OR.240(b) IS.I.OR.240(c) IS.I.OR.240(d)	IDENTIFY	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2
				PROTECT	PR.AT-1 PR.AT-4		
Create and maintain an Information security management manual ISMM	Organisation	Management	IS.I.OR.250			7.5.1	A6.1.3
Develop a procedure on how to notify the competent authority upon changes to the ISMS	Organisation	Management	IS.I.OR.255(a)	IDENTIFY	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2
Manage changes to the ISMS and notify the competent authority and/or request for approval of changes	Organisation	Management	IS.I.OR.255(a) IS.I.OR.255(b)	IDENTIFY	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2

Appendix III

Examples of aviation services

The following is a non-exhaustive and not complete list of aviation services that can be used as a basis to identify the scope of risk assessment for the organisation.

Aerodrome ATM- MET services provider
Aeronautical digital map service
AIM (external)
Airport
APP ACC
ATC (external)
ATC superior
ATM
ATM-MET services provider
Civil AU operations centre
Communication infrastructure
ER ACC
FIS/TIS data integrator
National AIM
Navigation infrastructure — ground-based
Navigation Infrastructure — satellite-based
Non-ATM MET services provider
Non-aviation users (external)
Regional AIM
Regional ASM
Regional ATFCM
State AU operations centre
Static aeronautical data service
Sub-regional DCB common service provision
Sub-regional/local ATFCM
Sub-regional/national ASM
Surveillance infrastructure airport
Surveillance infrastructure en-route
Surveillance infrastructure TMA
Time reference (external)
Tower (TWR)

Annex II

AMC & GM to Commission Delegated Regulation (EU) 2022/1645

GM1 Article 1 — Subject matter

When taking measures under this Regulation, the affected organisations and competent authorities are encouraged to consider the principle of proportionality to ensure that such measures are appropriate to the nature and risk of their activities.

GM1 Article 3 — Definitions

For the sake of common understanding, the following is a description of the terms used in this document:

Audit	It refers to a systematic, independent, and documented process for obtaining evidence, and evaluating it objectively to determine the extent to which requirements are complied with. *Note: Audits may include inspections.*
Assessment	In the context of management system performance monitoring, continuous improvement and oversight, it refers to a planned and documented activity performed by competent personnel to evaluate and analyse the achieved level of performance and maturity in relation to the organisation's policy and objectives. *Note: An assessment focuses on desirable outcomes and the overall performance, looking at the organisation as a whole. The main objective of the assessment is to identify the strengths and weaknesses to drive continuous improvement.* *Remark: For 'risk assessment', please refer to the definition below.*
Competency	It is a combination of individual skills or standard of performance, practical and theoretical knowledge, attitudes, training, and experience.
Control	It is a measure that maintains and/or modifies risk.
Correction	It is the action taken to eliminate a detected non-compliance.
Corrective action	It is the action taken to eliminate or mitigate the root cause(s) and prevent the recurrence of an existing detected non-compliance or other undesirable conditions or situations.
Deficiency	It is as a deviation from compliance with or a non-fulfilment of any requirement or objectives, either from a regulatory or an organisation's perspective, and either completely or partially.
Experience	It is the fact or state of having been affected by or gained knowledge and skills through observation, participation or doing.
Functional chain	The concept of functional chain pursues the objective of supporting the management of risks, through consideration of all the involved functions starting from the aircraft downstream. This shall allow a holistic perspective for identifying and assessing risks, including the involved support functions. An example could be when the cyber risk for FMS data integrity is assessed, the following functions require consideration: MRO (maintenance of the FMS), wireless access to FMS, FMS supply chain for the sourcing of components, other potential wireless data communication means (e.g. with airport, AOC, etc.).
Hazard	It is a condition or an object with the potential to cause or contribute to an aircraft incident or accident.
Human factors	They are concerned with the application of what we know about human beings, their abilities, characteristics and limitations, to the design of equipment they use, environments in which they function, and jobs they perform.

Just culture	It means a culture in which front-line operators or other persons are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but in which gross negligence, wilful violations and destructive acts are not tolerated, as defined in Article 2 of Regulation (EU) No 376/2014.
Knowledge	Content of information needed to perform adequately in the job at an acceptable level, usually obtained through formal education and on-the-job experience. This knowledge is necessary for job performance but is not sufficient on its own.
Management (activity)	In the general organisational context, it refers to the activities aimed at directing, controlling, and continually improving the organisation within appropriate structures. In the context of this Regulation it means, more specifically, the supervision and making of decisions necessary to achieve the organisation's safety and information security objectives.
Management system	It refers to a set of interrelated or interacting system elements to establish policies, objectives and processes to achieve those objectives, where the system elements include the organisational structure, roles and responsibilities, planning and operations.
Qualification	It is the combination of knowledge, aptitude, skill, quality, ability, accomplishment or capacity that makes a person suitable to take on a certain role or to carry out a task or gives the justification to do so.
Professional background	It is the combination of knowledge, experience and current on-the-job training.
Risk assessment	It is an evaluation that is based on engineering and operational judgement and/or analysis methods in order to establish whether the achieved or perceived risk is acceptable or tolerable.
Risk register	It refers to a physical or digital means of documentation used as a risk management tool that acts as a repository for all identified risks and contains additional information about each risk, such as the nature of the risk, mitigation measures, ownership, status, etc.
Safety risk	It refers to the predicted likelihood and severity of the consequences or outcomes of a hazard.

GM1 Article 6 — Competent authority

A competent authority may be a ministry, a national aviation authority, or any aviation body designated by the Member State and located within that Member State. A Member State may designate more than one competent authority to cover different areas of responsibility, as long as the designation decision contains a list of the competencies of each authority and there is only one competent authority responsible for each given area of responsibility. In certain cases, the competent authority may be the Agency.

GM1 IS.D.OR.200 Information security management system

An **information security management system (ISMS)** is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security aimed to protect the information assets in order to achieve the organisation's operational and safety objectives in a risk-managed, effective and efficient manner.
The ISMS applies an information security requirement analysis and an information security risk management process to decide on, and manage the selection, implementation and operation of controls over all architectural layers (governance, business, application, technology, data), domains (organisational, human, physical, technical) and the perspectives of governance, risk management and compliance (GRC) within the ISMS scope. The risk management process is based on an aviation safety

risk assessment and the risk acceptance levels designed to effectively treat and manage risks with a potential impact on aviation safety caused by threats exploiting vulnerabilities of information assets in aeronautical systems, as depicted in Figure 1.

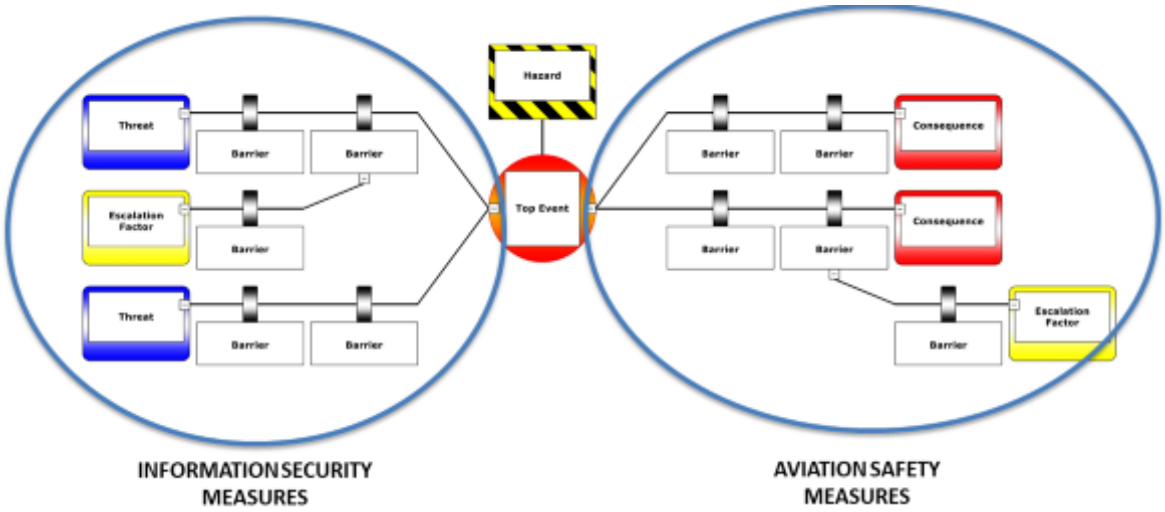

Figure 1: Bow-tie representation of management of aviation safety risks posed by IS threats

The ISMS in this Regulation should bring together the information security and aviation safety competencies in most of the processes, including, for instance, identifying critical systems, or threats, and assessing potential impacts on and risks to aviation safety.

ISMS implementation and maintenance

An ISMS, as per this Regulation, employs the perspectives of governance, risk and compliance, and an approach that combines the dimensions of safety risk and performance to determine the information security controls that are appropriate for and compliant with the specific context and can effectively provide the required level of protection to achieve the aviation safety objectives:

— **Governance** perspective refers to providing management direction and leadership aimed to achieve the entity's own overarching objectives:

  — leadership and commitment of the senior management defining and ensuring the close involvement of the management and a 'top-down' ISMS implementation

  — information security and safety objectives derived from, aligned and consistent with the entity's business objectives and monitored by, e.g., management reviews

  — information security policies stating the principles and objectives to be achieved

  — roles, responsibilities, competencies and resources required for an effective ISMS

  — effective, target-group-oriented communication to internal & external stakeholders

— **Risk** perspective refers to a key aspect of an ISMS in an aviation safety context according to this Regulation and serves as a basis for transparent decision-making and prioritisation of controls and risk treatment options. It further refers to the assessment, treatment and monitoring of information security risks in support of the management of aviation safety risks for the key processes and information assets upon which they depend. This includes protection requirements, risk exposure, attitude towards risks and risk acceptance criteria, methods and industry standards.

— **Compliance** perspective refers to the compliance with regulatory, legal and contractual (supply chain and operational peers) requirements. This includes:

  — this Regulation,

  — the entity's own policies and standards and may further include international or industry standards adopted by the entity from ISO, EUROCAE, etc.

  The perspective comprises the definition, implementation and maintenance of the required security provisions whose effectiveness and compliance shall be regularly monitored and assured by, e.g., (internal) audits.

Based on these perspectives, we may identify 14 core components or building blocks that have been shown to be relevant for the establishment of an effective ISMS. These ISMS core components can be summarised as follows:

(o) context establishment defining the scope, interfaces, dependencies and requirements of interested parties;

(p) leadership and commitment of the senior management;

(q) information security and safety objectives;

(r) information security policies;

(s) roles, responsibilities, competencies and resources required for an effective ISMS;

(t) communication to internal and external stakeholders, and a sufficient level of security awareness among employees, managers and third parties;

(u) information security risk management including risk assessment and treatment;

(v) information security incident management establishing processes for the handling of information security incidents and vulnerabilities;

(w) performance & effectiveness monitoring, measurement and evaluation;

(x) internal audits and management reviews;

(y) corrections and corrective actions;

(z) continuous improvement;

(aa) relationship with suppliers;

(bb) documentation and evidence collection.

Additional critical success factors for the implementation and operation of an ISMS include the following:

— The ISMS should be integrated with the entity's processes and overall management structure or even — at least partially, with safeguards for their respective integrity, and as reasonably applicable — with an overarching management system comprising information security, aviation safety and quality management.

— Information security has to be considered at an early stage in the overall design of processes and procedures, of systems and of information security controls, to be seamlessly integrated, for maximum effectiveness, minimal functional interference and optimised cost. None of these benefits can be achieved by integrating it later.

— The risk management process determines appropriate characteristics of preventive controls to reach and maintain acceptable risk levels.

— The incident management process ensures that the organisation detects, reacts and responds to information security incidents in a timely manner. This is achieved by defining responsibilities, procedures, scenarios and response plans in advance to ensure a coordinated, targeted and efficient response.

— Continuous monitoring and reassessment are undertaken and improvements are made in response.

The above-mentioned core components are related to the requirements in this Regulation, for which Figure 2 provides a high-level depiction of the aspects that are more prominent in the implementation phase and those that characterise the operational phase, as well as the review and possible improvement.

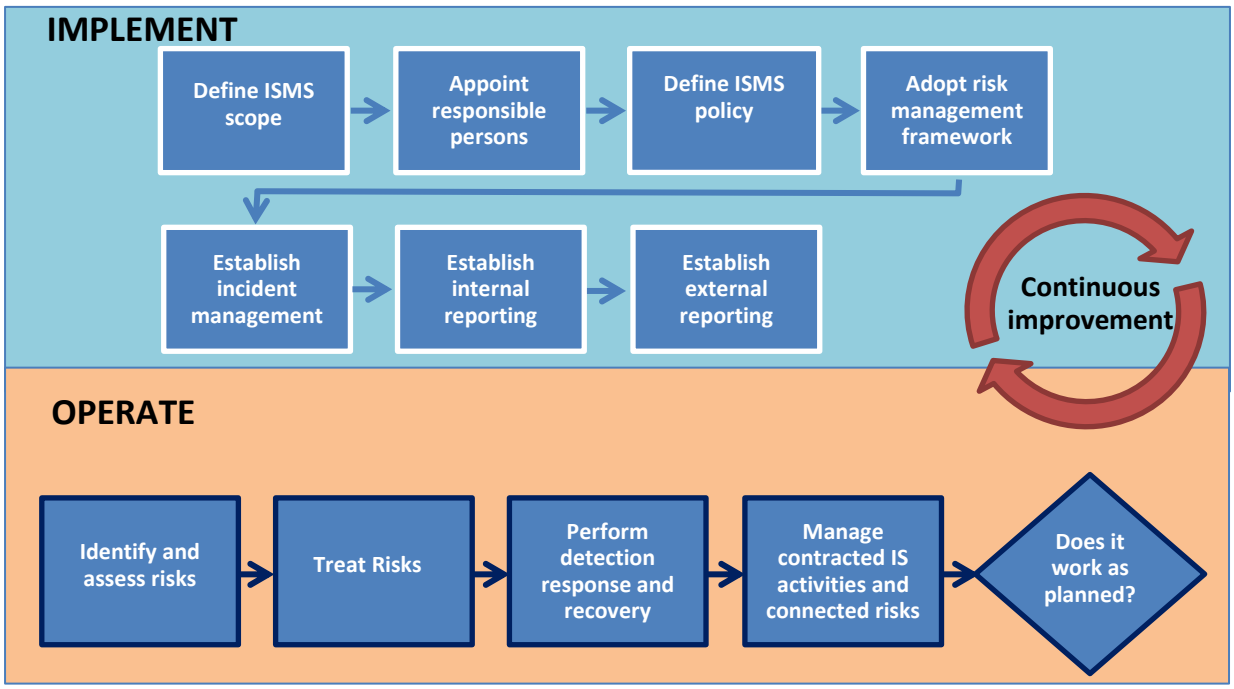

Figure 2: Representation of Part-IS requirements from an ISMS's lifecycle perspective

Plan-Do-Check-Act approach

The Plan-Do-Check-Act (PDCA) refers to a process approach that is often used to establish, implement, operate, monitor, review and improve management systems. Figure 3 depicts the PDCA applied to an ISMS.

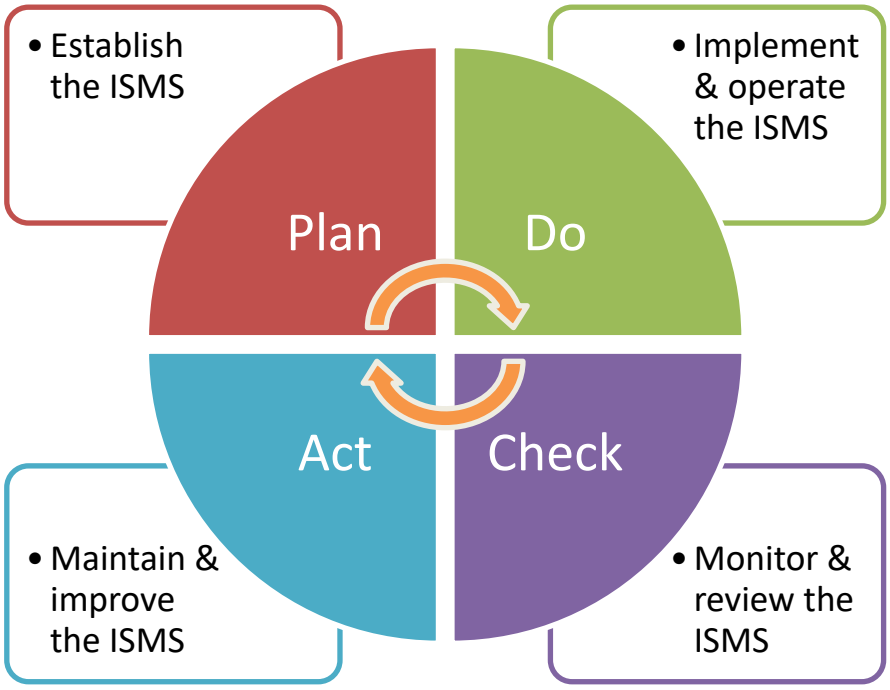

Figure 3: Plan-Do-Check-Act approach applied to ISMS

An alternative cyclical process is Define-Measure-Analyse-Improve-Control (DMAIC, six sigma).

Benefits of an ISMS

The benefits of a management system operating in a dynamic, uncertain or unpredictable risk environment are realised over the long term only when the organisation improves existing controls, processes and solutions based on the assessments of risks, performance and maturity as well as the learnings from incidents, audits, non-conformities and their root causes. A successful adoption and deployment of an ISMS allows an entity to:

— achieve greater assurance to the management and interested parties that its information assets are adequately protected against threats on a continual basis;

— increase its trustworthiness and credibility providing confidence to interested parties that IS risks with an impact on aviation safety are adequately managed;

— increase the resilience of the entity's key processes against unauthorised electronic interactions and maintains the entity's ability to decide and act;

— support the timely detection of control gaps, vulnerabilities or deficiencies aimed to prevent security incidents or at least to minimise their impact;

— detect and timely react to changes in the entity's environment including system architecture and threat landscape or the adoption of new technologies;

— provide a foundation for effective and efficient implementation of a comprehensive security strategy in times of digital transformation, increasing interconnectivity of systems, emerging information security threats and new technologies.

Relation to ISO 27001

The international standard ISO 27001 is a widely adopted standard for ISMS: it specifies generic requirements for establishing, implementing, maintaining and continually improving an ISMS and also includes requirements for the assessment and treatment of IS risks. The requirements are applicable to all entities, regardless of type, size or nature. The conformity of an ISMS with the ISO 27001 standard can be certified by an external qualified auditor on behalf of a reputable certification authority. ISO 27001 is compatible with other management system standards (quality, safety, etc.) that have also adopted the structure and terms defined in Annex SL to ISO/IEC Directives, Part 1, Consolidated ISO Supplement: this compatibility allows an entity to operate a single management system that meets the requirements of multiple management system standards.

The requirements for an ISMS specified by this Regulation are in most parts consistent and aligned with ISO 27001; however, this Regulation introduces provisions specific to the context of aviation safety. If an ISO 27001-based ISMS is already operated by an entity for a different scope and context, it can be adapted and extended to the scope and context of this Regulation in a straightforward manner based on an analysis of the scope and the gaps.

PART-IS versus ISO 27001 cross reference table

For a comparison between the main tasks required under Part-IS and the clauses and relevant controls in ISO 27001, refer to Appendix II.

AMC1 IS.D.OR.200(a)(1) Information security management system (ISMS)

The organisation should define and document the scope of the ISMS, by determining activities, processes, supporting systems, and identifying those which may have an impact on aviation safety.

The information security policy should cover at least the following aspects with a potential impact on aviation safety by:

(a) endorsement by the accountable manager or, in the case of design organisations, the head of the design organisation and review at planned intervals or if significant changes occur;

(b) committing to comply with applicable legislation, consider relevant standards and best practices;

(c) setting objectives and performance measures for managing information security;

(d) defining general principles, activities, processes for the organisation to appropriately secure information and communication technology systems and data;

(e) integrating ISMS requirements into the processes of the organisation;

(f) committing to continually improve towards higher levels of information security process maturity as per IS.D.OR.260;

(g) committing to satisfy applicable requirements regarding information security and its proactive and systematic management and to the provision of appropriate resources for its implementation and operation;

(h) assigning information security as one of the essential responsibilities for all managers;

(i) continuously promoting the information security policy within the organisation to all personnel;

(j) encouraging the implementation of a 'just culture' and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents;

(k) communicating the information security policy to all relevant parties, as appropriate.

GM1 IS.D.OR.200(a)(1) Information security management system (ISMS)

INFORMATION SECURITY POLICY AND OBJECTIVES

The information security policy should suit the entity's purpose and direct its IS activities. Such policy should contain the needs for IS in the entity's context, a high-level statement of direction and intent of the IS activities, the principles and most important strategic and tactical objectives to be achieved by the ISMS, as well as the general IS objectives or a specification of a framework (who, how) for setting IS objectives. The IS policy should also contain a description of the established ISMS including roles, responsibilities and references to topic-specific policies and standards.

The IS objectives should be:

— consistent and aligned with the IS policy and consider the applicable IS requirements, derived from the overarching entity's objectives, and the results from the risk assessment and treatment (which, in turn, supports the implementation of the entity's strategic goals and IS policy);

— regularly reviewed to ensure that they are up to date and still appropriate;

— measurable if practicable (to be able to determine whether or not the objective has been met), aimed to be SMART (specific, measurable, attainable, realistic, timely) and aligned with all affected responsible persons.

When defining IS objectives, e.g., based on the overarching entity's objectives, the IS requirements, or the results of risk assessments, it should be determined how these objectives will be achieved. The degree to which IS objectives are achieved must be measurable. If possible, it should be measured by KPIs which have been defined in advance (refer to resources such as COBIT 5 for Information Security). It is recommended to start with the definition of a limited number of IS objectives which are relevant for the entity, more of a long-term nature and measurable with a reasonable effort relative to the delivered benefits.

AMC1 IS.D.OR.200(a)(12)&(a)(13) Information security management system (ISMS)

When establishing compliance with the provisions under IS.D.OR.200 (a)(12) and (a)(13), the organisation should:

(a) implement a function to periodically monitor compliance of the management system with the relevant requirements and adequacy of the procedures including the establishment of an internal audit process and an information security risk management process. When the organisation has already established a compliance monitoring function under the implementing regulation for its domain, such function should include the monitoring of the management system with the relevant requirements in the scope of its activities. Compliance monitoring should include a feedback system of audit findings to the accountable manager or, in the case of design organisations, the head of the design organisation or delegated persons to ensure

implementation of corrective actions as necessary;

(b) implement and maintain suitably robust information security controls for the protection of information, ensuring the principle of need-to-know. It should protect the source of information in accordance with the relevant provisions established in Regulation (EU) 2018/1139. It should also comply with Regulation (EU) No 376/2014.

GM1 IS.D.OR.200(a)12 Information security management system (ISMS)

COMPLIANCE MONITORING

For the purpose of compliance monitoring, internal audits should be conducted at planned intervals to provide assurance on the status of the ISMS to the management and to provide information on the following:

— conformity of the ISMS to the requirements of this Regulation and the organisation's own requirements either stated in the IS policy, procedures and contracts or derived from information security objectives or outcomes of the risk treatment process;

— effective implementation and maintenance of the ISMS.

Internal audits should follow an independent, evidence-based approach and set up an audit programme taking into consideration the importance of the processes concerned and definitions of the audit criteria and scopes. Documented information should be retained evidencing the audit results, their reporting to the relevant management and the audit programme.

AMC1 IS.D.OR.200(c) Information security management system (ISMS)

When establishing compliance with the provisions under point IS.D.OR.200(c), the organisation should:

(a) provide an outline of the structure of the specific security resources (internal and external), including their roles and responsibilities that will be used to manage and maintain the assets and resources included within the scope and approved by the accountable manager or, in the case of design organisations, by the head of the design organisation and review at planned intervals or if significant changes occur;

(b) identify and categorise all relevant contracted organisations used to implement the ISMS. The organisation should define and document procedures for the management of interfaces and coordination between the organisation and other organisations, including contracted organisations;

(c) identify and define all key processes and procedures, and internal and external reporting schemes that will be used to maintain compliance with the objectives over the life cycle of the ISMS. The organisation may adjust existing processes or procedures for compliance;

(d) identify and document any other information that will be used to maintain compliance with the objectives;

(e) when creating and updating documented information, ensure appropriate identification and description (e.g. a title, date, author, or reference number) as well as a review and an approval for suitability and adequacy;

(f) control documented information required by the ISMS to ensure that:

(3) it is available and suitable for use, where and when it is needed;

(4) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

GM1 IS.D.OR.200(c) Information security management system (ISMS)

The amount of information that should be documented to maintain compliance with the objectives of this Regulation may vary between organisations due to various factors, such as size and complexity, or the need for harmonisation with other management processes already in place. As general guidance, taking into account the documents required to comply with point IS.I.D.OR.200(a), the record-keeping requirements referred to in point IS.D.OR.245 and the information security management manual requirements referred to in ISD.OR.250, the following is a non-exhaustive list of information that should be documented:

(a) information security policy that should include the organisation's information security objectives information security objectives — see IS.D.OR.200(a)(1);

(b) responsibilities and accountabilities for roles relevant to information security;

(c) scope of the ISMS and the interfaces with, and dependencies on, other parties — see IS.D.OR.200(a)(2) and the information security requirements referred to in point IS.D.OR.205;

(d) information security risk management process;

(e) archive of risks with results of the information security risk assessment and treatment measures (often referred to as 'risk register', or 'risk ledger') — see IS.D.OR.245;

(f) evidence of the competencies necessary for the personnel performing the activities required under this Regulation;

(g) evidence of the current competencies of the personnel performing the activities required under this Regulation;

(h) (key) performance indicators derived from evidence of the monitoring and measurement of the ISMS processes.

GM1 IS.D.OR.200(d) Information security management system (ISMS)

PROPORTIONALITY IN ISMS IMPLEMENTATION

When implementing the processes and procedures, as well as establishing the roles and responsibilities required under point IS.D.OR.200(d), the organisation should primarily consider the risks that it may be posing to other organisations, as well as its own risk exposure. Other aspects that may be relevant include the organisation's needs and objectives, information security requirements, its own processes and the size, complexity and structure of the organisation, all of which may change over time.

SMALL ORGANISATIONS IMPLEMENTING THE ISMS

Small organisations should consider seeking third-party service providers that can provide additional personnel and expertise to support the ISMS and to this end consider the provision of IS.D.OR.235 and

the related AMC. Outsourcing specific ISMS functions, such as security monitoring or incident response to a third-party service provider can help ensure that the organisation has access to the necessary personnel and expertise. Similarly, small organisations may want to be supported by a third party in performing the risk assessment.

Regarding the establishment of the appropriate personnel to implement and comply with the provisions of this Regulation, small organisations should always refer to AMC1 IS.D.OR.240(f) and GM1 IS.D.OR.240(f), however by considering that multiple responsibilities may be assigned to one person, while always ensuring the compliance monitoring independence.

As an introduction to the nature of information security risks and their management by small businesses, organisations may use, as initial guidance, the NIST Interagency Report (NISTIR) 'Small Business Information Security: The Fundamentals'.

INTEGRATION OF ISMS UNDER THIS REGULATION WITH EXISTING MANAGEMENT SYSTEMS

An organisation may take advantage of existing management systems when implementing an ISMS by integrating it with those existing systems.

By integrating the ISMS with existing management systems, the organisation may reduce the effort and costs required to implement and maintain the ISMS, while also ensuring consistency and alignment with the organisation's overall management approach. Below is a non-exhaustive list of potential synergies that can be exploited when integrating the ISMS with an existing management system:

— Leverage existing policies and procedures: an organisation may use its existing policies and procedures as a foundation for its ISMS. This may help to ensure consistency and minimise the need for additional documentation.

— Align ISMS with other management systems: an organisation may align the ISMS with other management systems, such as safety management systems (SMS), to ensure that the ISMS is consistent with the organisation's overall management approach.

— Use existing risk management processes: an organisation may use their existing risk management processes to identify and assess the security risks to their sensitive information.

— Reuse existing controls: an organisation may reuse existing controls, such as access controls or incident management process, to implement the security controls required by the ISMS.

— Continuous improvement process: an organisation may use the continuous improvement process of existing management systems to improve the ISMS over time.

AMC1 IS.D.OR.200(e) Information security management system (ISMS)

EXEMPTIONS

Organisations should follow the directions provided in AMC1 IS.D.OR.205(a) and AMC1 IS.D.OR.205(b) to perform a documented information security risk assessment to seek the approval from the competent authority of an exemption under point IS.D.OR.200(e). In order to justify the grounds for an exemption, the risk assessment is expected to provide explanations for the exclusion of all assets from the scope of the ISMS.

Organisations that would like to have the risk assessment performed by a third party should consider the provision of IS.D.OR.235 and the related AMC.

GM1 IS.D.OR.200(e) Information security management system (ISMS)

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for exemption by the competent authority following the procedure outlined in AMC1 IS.D.OR.200(e). It is up to the authority to determine whether this assessment is deemed satisfactory for an exemption to be granted.

Some examples of organisations that may consider asking for an exemption might include:

— A DOA or POA organisation that designs or produces only components or parts that are not involved in ensuring the structural integrity of the aircraft (e.g. carpets, interiors), nor any aircraft navigation or control functionality.

— An air operator that performs commercial (non-transport) specialised operations (SPO) with non-complex aircraft if the nature of the operations justifies the grounds for an exemption.

— An air operator that operates ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012 with the exception of e.g. one aircraft in predefined operational conditions or under certain operational limitations e.g. taking off and landing in the same aerodrome or operating site, operating in VFR, etc.

The aforementioned examples are not exhaustive and are only indicative of potential scenarios that might provide an initial basis for the preparation of an information security risk assessment that justifies the exclusion of all assets of an organisation from the scope of the ISMS.

AMC1 IS.D.OR.205(a) Information security risk assessment

The organisation, when conducting an information security risk assessment, should ensure that all aviation safety-relevant assets (e.g. physical, human, information) are identified and included in the ISMS scope as per IS.D.OR.200 and related AMC. Additionally, the organisation should provide the justification for those assets that are included and those that are excluded from the scope based on the outcome of its risk assessment. The organisation should identify the criteria to be used.

The organisation should identify all the elements of its own organisation which are within the scope of its ISMS and which could be exposed to information security risks, and should include at least those listed in IS.D.OR.205(a).

GM1 IS.D.OR.205(a) Information security risk assessment

For aviation, there are specific regulations and standards that govern the aircraft operating environment. Aircraft operators, aircraft manufacturers and suppliers whose equipment will be within the aircraft domain should continue to follow that same structure. For organisations managing their ground environment, no specific security framework, such as ISO, NIST or others, is explicitly mentioned for the development of their risk assessment. Each framework offers different benefits and none of these frameworks is perfect for an individual organisation and should be customised and

tailored to meet the overall needs of an organisation, as well as the specific needs related to the aviation assets to be included within the scope of the ISMS.

Organisations whose security frameworks have achieved industry certifications can provide this information as supporting artefacts; however, these organisations should show the applicability of the industry certification to the scope of this Regulation.

To help guide organisations, aviation-specific guidance defined in the most current version of the EUROCAE ED-201x document 'Risk Management' chapter and in the ED-204x, ED-205x and ED-206x document supporting chapters for 'Risk Management' appropriate for their unique operating environment, may be considered.

Regardless of the framework used, the organisation should demonstrate a clear and comprehensive understanding of all relevant data flows and information exchanges. The organisation should provide corresponding documentation on resources and dependencies related to computing, networking, supply chain and contracted services which have the potential to affect the information security and safety of the functions, services or capabilities within the scope of the risk assessment.

The following non-exhaustive list provides examples of items that should also be included in the aforementioned documentation. The level of detail should be commensurate with the expected level of risk. The purpose is to establish an understanding of all relevant assets, resources and dependencies that are directly a part of the functions, services and capabilities through the following information:

(e) Identification of inputs and outputs of the risk assessment:

- internal;
- external;
- internal leased or managed services, supply chain or other dependency;
- external leased or managed services, supply chain or other dependency;

(f) Identification of all relevant resources (i.e. hardware, software, network and computing resources) used to create, transmit, store or receive the inputs and outputs;

(g) Identification and definition of the physical operating environments and locations for all relevant resources;

(h) For each asset included within the scope, identification and association of the specific methods or resources that will be used by the organisation to manage, operate and maintain each asset over the life cycle of each asset including:

- internal resources;
- contracted resources;
- supply chain;
- managed service provider.

The organisation should also demonstrate a clear and comprehensive understanding of the resources that are used by the organisation to ensure effective operations, management and oversight (internal and external).

AMC1 IS.D.OR.205(b) Information security risk assessment

To establish compliance with IS.D.OR.205(b), the organisation should, based on the exchange of data and information and the assets used for this, identify within the scope of the information security risk assessment, the interfaces it has with other parties such as service providers, supply chains and other third parties, and which could result in a situation where information security risks either:

— pose a threat to other parties; and/or

— pose a threat to the organisation,

as a result of mutual exposure to those risks amongst the involved parties.

GM1 IS.D.OR.205(b) Information security risk assessment

Organisations may follow any security framework such as ISO, NIST or other when developing their risk assessment. The method needs to allow for the consideration of risk sharing between interconnected organisations. As an example, EUROCAE ED-201A, Figure 4-1 'Risk Assessment and Sharing Stages' represents a risk assessment process which can support organisations in identifying, assessing and agreeing on shared risks with others.

Organisations should follow the guidance defined in chapters 'Risk Management' and 'The concept of functional chains' of EUROCAE ED-201A. Additional guidance from supporting chapters regarding 'Risk Management' that is appropriate for their unique operating environment can be found in the ED-204x, ED-205x and ED-206x documents.

Risk information sharing

Risk information sharing means that interfacing organisations should inform each other about the potential exposure to information security risks by following, for instance, the approach detailed in ED-201A Appendix B.1, B.2 and B.3. The purpose of this exchange of information is to enable the organisations to establish a matching mapping for those services which are identified under IS.D.OR.205(a), including all flows of information and data in order to:

(f) illustrate (e.g. through a functional diagram) the relationships of logical and physical paths connecting the different involved parts;

(g) clearly identify all assets and resources that will be used in the exchange;

(h) identify and categorise all functions, activities and processes, including their respective information and data, which will be created, transmitted, received and stored and associate those with the responsible party which provides or performs those functions, activities and processes;

(i) determine for these paths, constituting the so-called functional chains, the role of the interfacing party as a producer, processor, dispatcher or consumer of the involved information or data;

(j) determine whether one interfacing party acts as an originator or receiver of a flow across such path.

GM2 IS.D.OR.205(b) Information security risk assessment

EXAMPLES OF AVIATION SERVICES

Examples of aviation services are provided in Appendix III.

AMC1 IS.D.OR.205(c) Information security risk assessment

The organisation should use a risk management framework that includes a methodology for assigning risks with a risk level and establishing criteria for determining risk acceptance or further treatment.

The organisation should provide documented evidence of risks which have a potential impact on aviation safety including the level of risks. The organisation should relate each risk to the relevant elements and interfaces identified under IS.D.OR.205 (a) and (b), and document whether the risk is acceptable or requires further treatment.

The organisation should provide the assurance that the risk assessment process is performed with the necessary rigour and discipline by documenting the process and its robustness. By doing so, the organisation should consider:

(d) reproducibility of the assessment's inputs and results;

(e) repeatability of the assessment over time in a way that the results of the different prior assessments can be compared to determine the changes;

(f) the gathering of inputs that are relevant and up to date, in particular:

— the information that allows the determination of the safety consequences;

— the information that allows the determination of the potential of occurrence of the threat scenario.

GM1 IS.D.OR.205(c) Information security risk assessment

RISK ASSESSMENT

The risk classification levels for the potential of occurrence of the threat scenario and severity of the safety consequences listed below may be applied, however this does not prevent the organisation from developing additional intermediate categories if it deems this necessary for risk assessments. The organisation should specify and document the applied, entity-specific, classification levels with an accurate qualitative definition and a quantitative definition in terms of a range or interval of real numbers in order to enable a sufficiently calibrated, consistent estimation, evaluation and communication within the entity or at the interfaces. The potential of occurrence of the threat scenario may be expressed as an interval of likelihoods including the duration of the observation. Supporting documentation and methods can be found in EUROCAE ED-203A Chapter 3.6 which references the evaluation of the potential of occurrence of the threat scenario in the Security Risk Assessment of EUROCAE ED-202A.

In order to facilitate the mutual comparability of risk assessments methodologies between interfacing organisations, the organisation may associate the assessment of the potential of occurrence of the threat scenario with one of the following categories:

— High potential of occurrence: the threat scenario is likely to occur. The attack related to the

threat scenario is feasible and similar threat scenarios have occurred many times in the past.

— Medium potential of occurrence: the threat scenario is unlikely to occur. The attack related to the threat scenario is possible and a similar threat scenario may have occurred in the past.

— Low potential of occurrence: the threat scenario is very unlikely to occur. The materialisation of the threat scenario is theoretically possible; however, it is not known to have occurred.

The evaluation of the potential of occurrence of the threat scenario can be based on the following aspects:

Protection (as defined in EUROCAE ED-203A)

— Security measures and architecture that deny access to assets: the degree to which an asset is open to access from compromised systems.

— Access to security measures: the degree to which a security measure prevents access/attack to itself from compromised systems.

— Failure of mechanism: the degree to which the known implementation of a security measure will fail to prevent an attack.

— Detection methods or procedures to recognise the attack and appropriately respond to reduce the potential of occurrence of the threat scenario.

Exposure reduction (as defined in EUROCAE ED-203A)

— Conditions under which an external access connection can be used by a user or attacker

— Limits on the functionality of an external access connection

— Organisational policies that control the time-to-feasibility for developing attack tools specific to the product

— Vulnerability management including intelligence, scanning, treatment and retesting aimed to discover, detect and treat newly reported or detected vulnerabilities in a fast, risk-prioritised manner with high assurance in order to reduce the attack surface

Attack attempt (as defined in EUROCAE ED-203A)

— The capability of the attackers which is determined by the resources and expertise required for their attack

The capability of the attackers can be assessed through several ways, for instance:

— information from CERTs/CSIRTs, ISACs;

— analyses of past activities, techniques and procedures (TTPs) and success rate of attacks.

For the same reason the organisation may associate the outcome of the evaluation of the severity of the safety consequences with one of the following categories:

— High severity: those immediate or delayed scenarios that can cause or contribute to an accident where an accident means an occurrence associated with the operation of an aircraft in which:

— a person is fatally or seriously injured;

- the aircraft sustains damage or structural failure;
- the aircraft is missing or completely inaccessible;

— Moderate severity: those immediate or delayed scenarios that can cause or contribute to safety incidents where an incident means any occurrence other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operations;

— Low severity: those immediate or delayed scenarios that can cause or contribute to negligible safety consequences.

Additional information can also be found in Regulation (EU) 2015/1018 on mandatory reporting of occurrences. Further examples for aviation domains can be found in EUROCAE ED-201A – Appendix B — Tables B-5, B-6 and B-7.

Risk acceptance criteria

Risk acceptance criteria are critical and should be developed, specified and documented. The criteria may define multiple thresholds, with a desired target risk level, but including also provision for the accountable manager or, in the case of design organisations, the head of the design organisation or delegated persons to accept risks above this level under defined circumstances and conditions.

In order to facilitate the mutual comparability of risk assessments between interfacing entities, the organisation should classify the risks in the following categories:

— unacceptable risk;

— conditionally acceptable risk;

— acceptable risk.

For what concerns the conditional acceptance of risks, the criteria for acceptance should take into account how long a risk is expected to exist (temporary or short-term activity or exposure), or may include requirements for the commitment of future treatments to reduce the risk at an acceptable level within a defined time duration and show how the risk will be managed over time through the organisation’s risk governance processes.

Moreover, risks should be conditionally accepted only under the condition that the organisation demonstrates the presence of a comprehensive risk management structure that includes risk assessment, risk treatment and risk monitoring processes for operations. This is typically achieved when the organisation reaches a higher level of maturity that is representative of functionality and repeatability of cybersecurity risk management — see GM1 IS.D.OR.260(a).

The following Figure 1 depicts a risk acceptance matrix based on the aforementioned categories that can be used by interfacing organisations for mutual comparability.

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Figure 1: Risk acceptance matrix

* The potential of occurrence of the threat scenario is reassessed in a timely manner (refer to IS.D.OR.205(d)) and monitored to ensure that it remains low and that if the risk materialises, it is early detected and dealt with.

A comprehensive risk management structure typically entails the following aspects and processes:

— a repeatable and reproduceable risk assessment. If the risk factors are considered fairly uncertain and within some wide value range or not sufficiently precise, further iterations of the risk assessment are performed involving additionally gathered or detailed information and a more in-depth assessment in order to reduce uncertainty and increase precision;

— a thorough review of those risks proposed to be conditionally acceptable that is performed by the accountable manager or, in the case of design organisations, the head of the design organisation or delegated person(s) who may impose additional conditions for the risk retention;

— strict monitoring of the key risk indicators that includes a defined, reliable detection of the potentially evolving risk materialisation;

— an incident response scheme is in place with reactive measures that are triggered by detection mechanisms in order to immediately contain the consequences, in particular, for risk scenarios involving a high severity level.

Note: A risk assessment process can be classified as ‘repeatable’ when under the same conditions an entity or a person delivers the same result. Conditions can include:

— use of the same information security risk assessment framework, or methodology;

— use of the same inputs, assumptions, security context and threat environment, considering the time period where long breaks can significantly affect the repeatability;

— use of the same observing entity / person.

Similarly, a risk assessment processes can be classified as ‘reproduceable’ when another entity or another person given the same inputs, assumptions, security context and threat environment can reproduce the assessment in its entirety.

Threat scenario identification

A threat scenario is one of the possible ways a threat could materialise. Typically, a threat scenario describes a potential attack targeting one or more vulnerabilities of assets, as well as processes.

The purpose of the threat scenario identification under this Regulation is to develop a list of scenarios that may lead to an information security threat having an impact on aviation safety.

A threat scenario, in general, is characterised by the following:

— a threat source of the information security attack;

— an attack vector and a path through the organisation up to the asset;

— the security controls that would mitigate the attack;

— the consequence of the attack including the affected safety aspects.

Threat scenario identification guidance can be found in ED-202A Chapter 3.4. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

Additional methods to identify relevant threat scenarios

When conducting this analysis, both security and safety aspects should be coordinated throughout the process to ensure mutual understanding of the threat preventive measures and mitigations being applied. In the following Figure 2 the interactions between information security and aviation safety are depicted through a 'bow-tie' diagram that highlights the links between risk controls and the underlying management system.

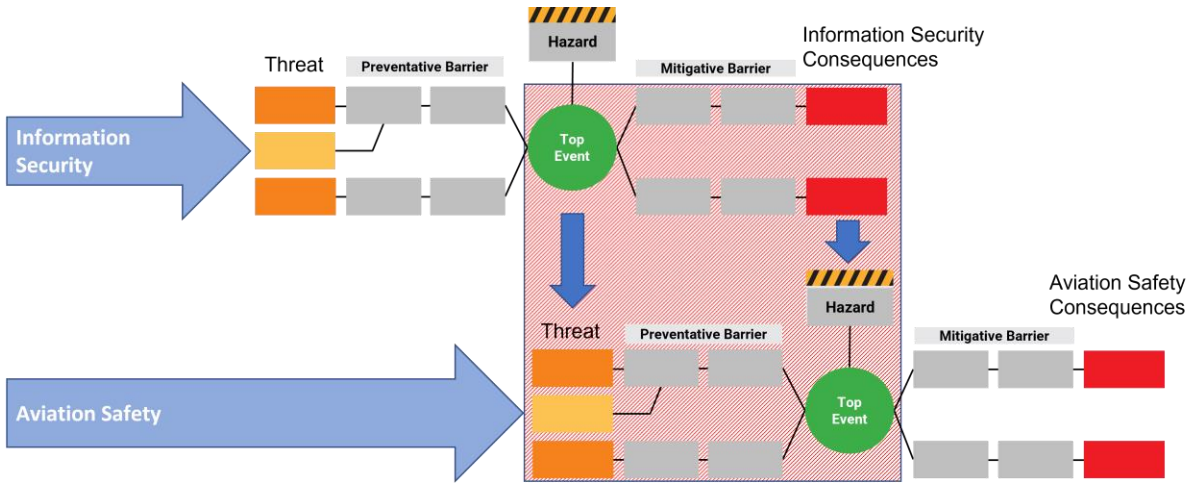

Figure 2: Interactions between information security and aviation safety risk management areas

Examples of threat scenarios

Threat catalogues may provide guidance and elements for the elaboration of threat scenarios that are relevant for the organisation. References can be found in ARINC 811 – Att. 3 – Tables 3-6 to 3-8 for the threat catalogue examples and other threat catalogue examples as they are provided by EU institutions. However, this is not an exhaustive list of examples; the identification of threat scenarios should therefore not be limited to those examples only. In addition, other relevant resources

containing information on information security threats and the information security threat landscape should be consulted to support the risk assessment process with relevant inputs.

A set of examples of threat scenarios can be found in Appendix I.

AMC1 IS.D.OR.205(d) Information security risk assessment

The organisation should take into account the following criteria when establishing compliance with the objectives contained in point IS.D.OR.205 (d):

(a) The risk assessment performed under points IS.D.OR.205 (a), (b) and (c) should be reviewed at regular intervals, the periodicity being determined by the organisation performing the assessment considering the criticality of the assets within the scope of the risk assessment, levels of post-assessment risk of the assets within the scope of the risk assessment and any customer or regulatory requirements. A higher criticality or level of risk will require more frequent review.

(b) The periodicity of risk assessment reviews should be documented by the organisation and include the justification, date of approval and information about the risk owner.

GM1 IS.D.OR.205(d) Information security risk assessment

Risks are not static and will not stay the same forever. Risk assessments can be undertaken on different levels where one pursues a high-level risk assessment and another one a more granular approach to support the identification of changes and the need for a more detailed risk assessment. Risk assessments should be subject to regular reviews to:

(a) allow for continuous improvement of the quality of risk assessment;

(b) ensure efficiency and effectiveness of risk controls and mitigations in both their design and operation;

(c) review plans and actions for risk treatment;

(d) update any changes which may require revision of risk treatments and priorities;

(e) maintain an overview of the complete risk picture; and

(f) identify any emerging risks.

The objective of a risk assessment review is to re-evaluate the risks, their likelihood and impact. One possible approach is to tier risk assessments with a higher-level risk assessment which is used to identify changes. In a next step, the higher-level risk assessment could allow the identification of the detailed risks that should be reviewed.

Risk assessment reviews should involve the risk owners, project teams and other stakeholders as applicable.

GM2 IS.D.OR.205(d) Information security risk assessment

Risk assessments should be reviewed regularly and may be reviewed more or less frequently depending on whether the assets within the scope of the risk assessment are of sufficient criticality or complexity, the levels of post-assessment risk warrant more frequent analysis, or to adhere to any

regulatory or customer requirements. The criticality of assets can be determined through an assessment of the impacts of a loss of the assets i.e. an impact assessment.

The periodicity of risk assessment reviews should be documented by the organisation in security manuals, processes or procedures and should align with wider change management activities and management reviews of information security. Further guidance on criteria and frequency of risk assessment review can be found in EUROCAE ED-201A Chapter 4, as well as ED-205A Chapter 3.2 (for ATMS/ANS).

Risk assessments should also be reviewed when:

(a) there is a change in the elements subject to information security risks as identified in IS.D.OR.205(a); changes may be identified through management reviews or change control processes. Change in the elements will include:

— additions to or removals from elements within the scope of the risk assessment (as identified in IS.D.OR.205(a));

— changes to design or configuration of elements in scope of the risk assessment (as identified in IS.D.OR.205(a)) that have the potential to alter the risk assessment outcomes; or

— changes to values, which would potentially trigger changes to impact levels, of elements within the scope of the risk assessment (as identified in IS.D.OR.205(a));

(b) there is a change in the interfaces between the organisation and other organisations with which the organisation shares information security risks or relies upon to mitigate information security risks (e.g. supply chains, service providers, cloud providers and customers), as identified in IS.D.OR.205(b), or between the system within the scope of the risk assessment and any other interconnected systems, or in the risks notified to the organisation by other organisations, as identified in IS.D.OR.205(b), or owners or managers of the other systems including:

— establishment of new interfaces;

— removal of existing interfaces;

— changes to existing interfaces that would have the potential to alter the risk assessment outcomes.

Note: Some organisational or system interconnections may be with organisations that are not within the scope of this Regulation as defined in Article 2 and therefore are not subject to the requirements of Part-IS. Where this is the case, these organisations should be informed of their responsibility to report such changes as listed above through contractual arrangement and reporting requirements between the affected organisations on a case-by-case basis and where applicable;

(c) there is a change in the information or knowledge used for the identification, analysis and classification of risks including:

— changes to threats and their values or addition of new threats that have not previously been assessed;

— changes to vulnerabilities or addition of new vulnerabilities that have not previously been assessed;

— changes in impacts or consequences of assessed threats or vulnerabilities;

— changes in aggregation of risks that may result in unacceptable levels of risks;

— changes or improvements in the risk management process, risk assessment approach and related activities;

— changes or improvements in the treatments of risks;

— changes in the criteria used to determine acceptance and treatments of risks;

(d) there are lessons learned from the analysis of information security incidents including:

— understanding of why and how incidents have occurred; and

— reviewing all types of incidents including those due to external factors, technical reasons, human factors or processes. For human factors a distinction can be made between malign and benign actions.

Evidence of risk assessment review should be documented and should include:

— evidence of approval of the review by the designated risk owner; and

— the rationale behind or basis for the risk owner's approval of the review.

Such evidence may comprise, but is not limited to:

— reports which constitute a form of documentation to track information security risks potentially impacting an organisation;

— the documentation of the information security risk assessment;

— exerts from a business or security risk register.

Note: In some cases the information contained in the risk report, security cases or risk register may be sensitive to the organisation and may need to be redacted in agreement with the authority, or a method may need to be established for the authority to view such content on the organisation's systems.

GM1 IS.D.OR.210 Information security risk treatment

The risk management options referred to in IS.D.OR.210(a) may be used in combination; however, there is no obligation for the organisation to do so.

The application of risk treatment options under points IS.D.OR.210 (a)(1) and (a)(2) lead to the introduction of security measures, often referred to as security controls.

GM2 IS.D.OR.210 Information security risk treatment

For each identified risk, the organisation should define the specific risk treatments, methods or resources that will be used over the life cycle of each asset to:

— manage risk reduction;

— monitor and maintain each asset;

— update and fulfil activities for configuration management;

— manage supply chain;

— manage contracted services or service provider.

The review of risk treatment measures should include life cycle considerations which are introduced by equipment, procedures and personnel.

A risk treatment plan as an outcome of the risk management process should include a prioritisation of risks, the corresponding information on the objectives and means for risk treatment to reach an acceptable level of risk, as well as agreed timelines specifying when responsible personnel should have implemented the risk treatment measures. The timelines for the implementation of a risk treatment measure should be agreed by the personnel responsible for the implementation and shall be communicated to and accepted by the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s).

Any subsequent implementation delay, together with its cause, reason, rationale or necessity, should be documented in the risk treatment plan. The delay should also be communicated to the competent authority in case the materialisation of risk would lead to an unsafe condition. The delay is also subject to the acceptance by the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s). This person may condition such acceptance on the implementation or availability of compensating controls or reactive measures to monitor, early detect and timely respond to the materialisation of the risk in treatment. In order to timely respond, the incident response team may be informed to trigger their preparedness.

The risk treatment plan can act as a means of communication with the competent authority to demonstrate effective treatment of unacceptable risks. Similarly, this plan can be utilised to communicate to interfacing organisations how shared risks are controlled.

In accordance with IS.D.OR.205(d), a regular or conditional review of the risk assessment is necessary, and this includes the review of the risk treatment measures developed under IS.D.OR.210(a) to identify whether they are still effective or they require adaptations.

In addition, the organisation should also consider the potential impact on the effectiveness of risk treatment measures where a shared information security risk may arise as a result of the interaction between interfacing entities (see IS.D.OR.235 and related AMC).

AMC1 IS.D.OR.210(a) Information security risk treatment

The organisation should take into account the following criteria when establishing compliance with point IS.D.OR.210(a):

(d) the measures developed under point IS.D.OR.210(a)(1) should be implemented according to a risk treatment plan with defined, risk-based priorities, objectives and agreed timelines and owners;

(e) identification and association of the life cycle considerations to ensure continuous effectiveness of the security measures including exchange of data with other entities;

(c) the organisation should review and update the risk assessment, according to IS.D.OR.205(d), to evaluate whether the measures developed under point IS.D.OR.210(a) do not introduce new

unacceptable risks or modify existing risks in a way that they become unacceptable.

Risk treatment should be documented in the risk registry even if the risk has been avoided.

AMC1 IS.D.OR.215(a)&(b) Information security internal reporting scheme

Organisations will have the means to detect security incidents and vulnerabilities in accordance with IS.D.OR.220. Organisations should have a mechanism to collect notifications of events by personnel and by sources outside of the company including suppliers, partners, customers and security researchers. The mechanism for collecting information by personnel and external sources should be easily accessible and communicated.

The organisation should collect all events gathered through the detection means for internal analysis. Each event should be analysed to identify whether it is indicative of suspicious behaviour and if yes, what potential or actual impact on aviation safety has occurred. Events should be considered in combination with other events to provide correlation to identify incidents.

The organisation should develop a vulnerability management strategy in order to ensure that a proper evaluation of all known, relevant information relating to the information security vulnerabilities is carried out when new vulnerabilities are identified. This strategy should consider the outcome of the risk assessment to determine whether further analysis of the vulnerability (e.g. exploitability) should be performed.

The organisation should identify all internal stakeholders that require notification of a specific incident or vulnerability and ensure that these stakeholders receive all necessary information on the incident or vulnerability in order to act effectively and in a timely manner to support the required detection and response periods.

GM1 IS.D.OR.215(a)&(b) Information security internal reporting scheme

RELATIONSHIP BETWEEN INTERNAL AND EXTERNAL REPORTING

Organisations should collect and report internally incidents and vulnerabilities aiming at covering all items within the scope of this Regulation. This does not preclude external reporting, nor does external reporting replace the need for internal reporting. Internal reports should be assessed in a timely manner and where the potential impact on safety is found to exceed the threshold for mandatory reporting, organisations should initiate reporting of these internal reports according to IS.D.OR.230.

GM2 IS.D.OR.215(a)&(b) Information security internal reporting scheme

ORGANISATION OF COLLECTION AND EVALUATION OF INFORMATION SECURITY EVENTS

It is a common practice in large organisations to centralise security operations in a security operations centre (SOC) and make use of a security information and event management (SIEM) system. A SIEM system collects all events from sources such as log files in a common database and allows the analysts and responders in joint SOC to review and act on these events. Organisations may choose to use a SOC for events relevant to Part IS in isolation or in combination with events not subject to Part-IS but of interest to the organisation, such as events relating to business interests.

Organisations that do not have a SOC capability and do not use a SIEM system need to consider how to establish processes to meet the required detection capabilities as well as detection and response

times.

GM3 IS.D.OR.215(a)&(b) Information security internal reporting scheme

RELEVANT INFORMATION FOR INCIDENTS AND VULNERABILITIES

Understanding the causes and contributing factors of information security incidents and vulnerabilities allows lessons learned to be gained and to introduce corrections to processes and asset design. However, understanding causes and contributing factors may not always be possible or may not aid in continuous improvement of aviation safety. Where vulnerabilities arise from assets developed solely or primarily for aviation, it is expected to be possible to perform the necessary investigation on the root causes. These root causes will inform the affected organisation(s) to improve processes and asset design to remediate vulnerability and to ensure that such vulnerabilities are not introduced in other assets. Understanding the root causes of vulnerabilities also allows the aviation community to learn and thus avoid similar vulnerabilities in the future.

GM1 IS.D.OR.215(c) Information security internal reporting scheme

If contracted organisations are also subject to this Regulation, the exchange of information and reporting should be covered under the management of shared risks and through the establishment of an external agreement between the organisations. Guidance regarding the development of external agreements can be found in EUROCAE ED-201A – 4.4 External Agreements.

More in general, and in all other cases, any service contract should include standard clauses concerning obligations for the contracted organisation to:

— report within an agreed time security incidents that may have an impact on the contracting organisation. Incidents and vulnerabilities which could lead to unsafe conditions should be reported as soon as possible and in such a manner that the external reporting obligation under IS.D.OR.230 can be ensured;

— designate a point of contact for the incident management and possible crisis management.

In some cases contracted organisations, such as service providers with distributed resources, may not be able to offer any ad hoc reporting. In these cases the internal reporting requirement may be fulfilled through other means that satisfy the objective of this provision. For instance, the contracted organisations may provide an up-to-date list of vulnerabilities affecting the systems within the scope of the contracted services. This list should be monitored by the contracting organisation as part of the internal reporting of security events.

GM1 IS.D.OR.215(d) Information security internal reporting scheme

The cooperation under point IS.D.OR.215(d) can be substantiated by sharing elements from incident records that can support other organisations' information security activities. In case the organisations are bound by contractual obligations, this contract may also include commitment to cooperate.

Moreover, commitment to cooperate may also be achieved through the active participation of the organisation in information security sharing initiatives; for instance, information sharing and analysis centre(s) (ISAC(s)). Additionally, for their own awareness, organisations may also subscribe to receive vulnerability and threat alerts, like those distributed by computer emergency response teams (CERTs).

GM1 IS.D.OR.220 Information security incidents – detection, response and recovery

Without prejudice to the definition of 'information security event' in Article 3, those events that indicate the potential materialisation of unacceptable risks include both occurrences (i.e. anything that causes harm or have the potential to cause harm) and discovery of vulnerabilities. In fact, information security risks are associated with the potential that threats will exploit vulnerabilities, therefore the discovery of an exploitable vulnerability is an information security event.

In light of this, in the context of this Regulation:

— detection activities required under IS.D.OR.220(a) include vulnerability discovery;

— response activities under IS.D.OR.220(b) include vulnerability management.

AMC1 IS.D.OR.220(a) Information security incidents – detection, response and recovery

DETECTION

When complying with the requirement in IS.D.OR.215(a), the organisation should define and implement a strategy to detect information security events having an impact on safety.

This should be done in a way to ensure that at least the detection strategy is able to cover all known information security threats to their assets that may materialise in a safety hazard having unacceptable consequences.

DETECTION STRATEGY

In order to determine the scope of the event detection, the organisation should:

(a) identify a list of threat scenarios from the risks identified under IS.D.OR.205;

(b) identify, as a minimum, those assets that contribute to the scenario(s) that may materialise in an unsafe condition. For this identification of the assets, the measures introduced under IS.D.OR.210 should also be considered.

Note: The contribution of an asset to the threat scenario and the materialisation of an unsafe condition should be assessed by considering the whole functional chain. In some cases, the asset may be at the end of a functional chain and if it is compromised, the effect on safety is direct and may be immediate; conversely if the asset is far from the end of functional chain and it is compromised, the effect should propagate and may be delayed.

GM1 IS.D.OR.220(a) Information security incidents – detection, response and recovery

DETECTION STRATEGY

When developing the detection strategy, for those items within the scope of event detection the organisation should define the conditions that trigger a process that, for example, would require personnel intervention and further analysis. These conditions on the items may be defined using elements from:

(a) expected functional baseline: engage in the identification of deviations from the expected functional operation of the system (excluding security functions/controls);

(b) expected security baseline: engage in the identification of deviations from the expected information security operation of security controls.

These conditions should consider both abnormal behaviour and substantial deviations from the baselines and relevant correlation of multiple independent events.

Further guidance on the objectives for the establishment of a detection strategy can be consulted in EUROCAE ED-206 – Chapter 4.

AMC1 IS.D.OR.220(b) Information security incidents – detection, response and recovery

(a) INCIDENTS

The organisation should take into account the following aspects when establishing compliance with the objectives contained in point IS.D.OR.220(b) relative to incidents:

(a) Preparation of procedures and delineation of roles and responsibilities to manage timely, effective and orderly response to any relevant security incidents.

(b) The response procedure should:

(i) consider the warnings, unitary or combined, from IS.D.OR.220(a)(2), and assess their potential impacts on aviation safety;

(ii) establish, in accordance with IS.D.OR.220(b)(2), a containment strategy for each asset category in relation with the potential worst-case effect and the mission constraints and provide criteria indicating when the attack is contained;

(iii) define, in accordance with IS.D.OR.220(b)(3), the acceptable impact on safety and security of each asset within the scope when they fail due to the materialisation of a threat scenario.

(c) The response time should be commensurate with the impact level assessed in (2)(iii).

(d) The response measures implemented under IS.D.OR.220(b) should be based on the response procedure referred to in the above point (a)(2) and it should, in particular, consider the following:

(i) the maximum acceptable safety level degradation of the items within the scope of the threat scenario;

(ii) the actions, such as resistance, containment, deception and control of the possible ways systems can fail, which will contribute to achieving the acceptable safety level degradation identified in point (i) while minimising the impact on operations;

(iii) the resources required to implement the actions specified in point (ii).

(b) VULNERABILITIES

The organisation should take into account the following aspects when establishing compliance with the objectives contained in point IS.D.OR.220(b) relative to vulnerabilities:

(1) Establishment of a vulnerability management plan defining procedures, roles and responsibilities to manage quick, effective, and orderly response to any detected relevant vulnerabilities.

(2) The response measures implemented under point IS.D.OR.220(b) should be based on the maximum acceptable risk of the items within the scope of the vulnerability, considering the worst-case scenario of the vulnerability being exploited.

(3) The response time should be commensurate with the pre-triage done on the warnings and the assessment of the potential impact of the vulnerability, if it is exploited.

GM1 IS.D.OR.220(b) Information security incidents – detection, response and recovery

An attack is considered contained (i.e. it is not spreading any further) when the boundaries of the incident have been identified and the threat does not propagate beyond these boundaries. Further guidance can be found in EUROCAE ED-206 – Chapter 5.

Guidance about the vulnerability strategy can be found in EUROCAE ED-206 – Chapter 3.4.2.

AMC1 IS.D.OR.220(c) Information security incidents – detection, response and recovery

When complying with the requirement in IS.D.OR.220(c), the organisation should develop an incident recovery procedure including at least the following:

(e) a list of those assets that enable safe operations, as well as the dependencies among them, this constituting the scope of the recovery;

(f) a description of the process with the necessary priority actions to be executed for a return to a safe and secure state for the assets within the scope of the recovery;

(g) the resources required to execute the actions defined in point (b) to ensure that these resources are readily available after an incident has occurred;

(h) the objectives for recovery time that should be set in relation to the safety criticality of the assets within the scope of the recovery.

GM1 IS.D.OR.220(b)&(c) Information security incidents – detection, response and recovery

RECOVERY OBJECTIVES AND TIMING

This Regulation focuses on incidents that have an impact on safety and requires response and recovery measures to be in place to ensure that operational safety remains above a minimum acceptable level.

The level of operations and safety may be interrelated, so in some cases when the level of operations is compromised by an information security incident and drops, the level of safety does the same. This is, for instance, the case of air traffic control, if air traffic services are reduced or become unreliable, the safety of flights is reduced too.

However, in other cases the relation between the level of operations and safety may be the inverse, or they may be decoupled, so when an incident occurs and the operations drop, the level of safety is

preserved. One example is the compromise of the software loading process on board the aircraft. In this case a detected incident followed by the decision to interrupt the software loading operations would preserve the existing level of safety.

The following Figure 1 depicts a conceptual framework that may be considered for the definition of the response and recovery objectives, including the recovery time. It represents, in the worst-case scenario, how the expected level of operational safety (safety level) for a process or an activity may vary over time when a security incident occurs. In this scenario, the safety level: first is reduced by the incident and then it degrades as long as the time passes. The figure also shows the expected effect that mitigations and controls should have, respectively: in containing the operational safety drop as soon as an incident occurs, and in improving the recovery i.e. the return to the expected safety level.

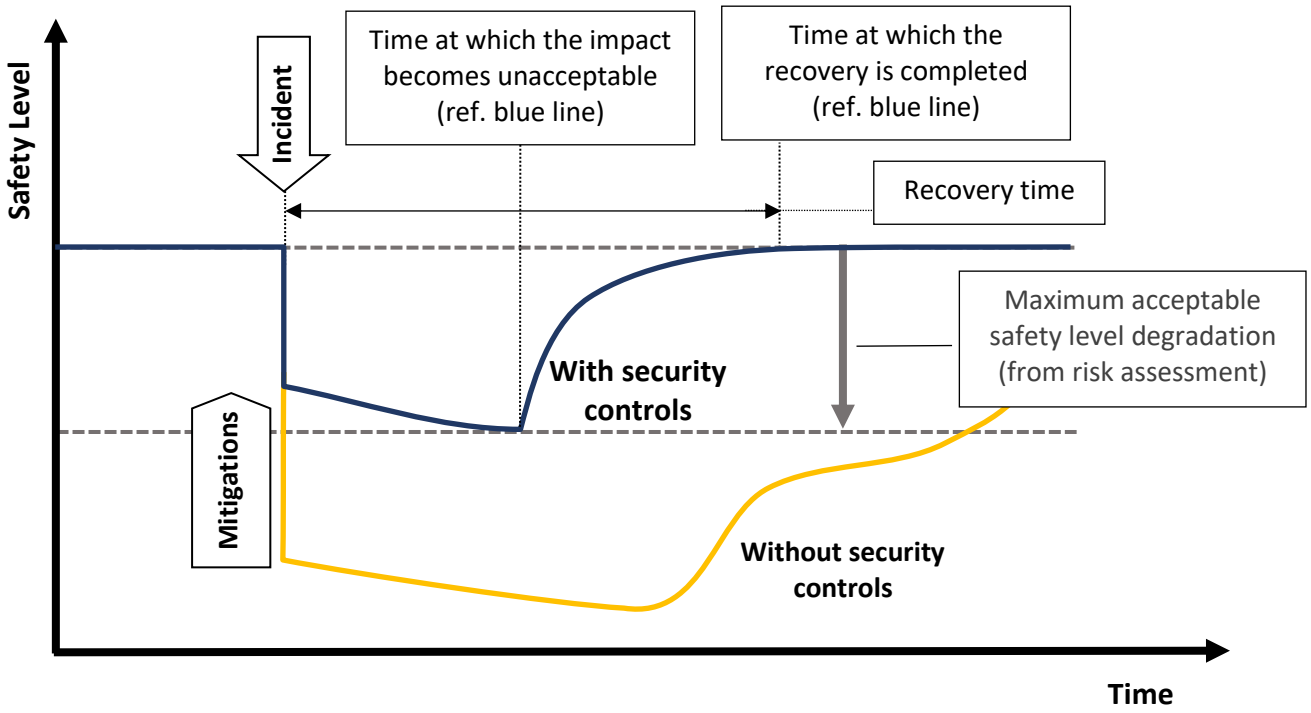

Figure 1: Conceptual framework for the definition of the response and recovery objectives

As mentioned, there might be different relations between the level of operations and safety that would lead to a different representation of the above figure. In certain cases, an incident may have a delayed effect on the safety level (e.g. a compromised development environment) as depicted in Figure 2, or it may have no impact if properly controlled, as in the case of the compromised software loading process mentioned before that is depicted in Figure 3.

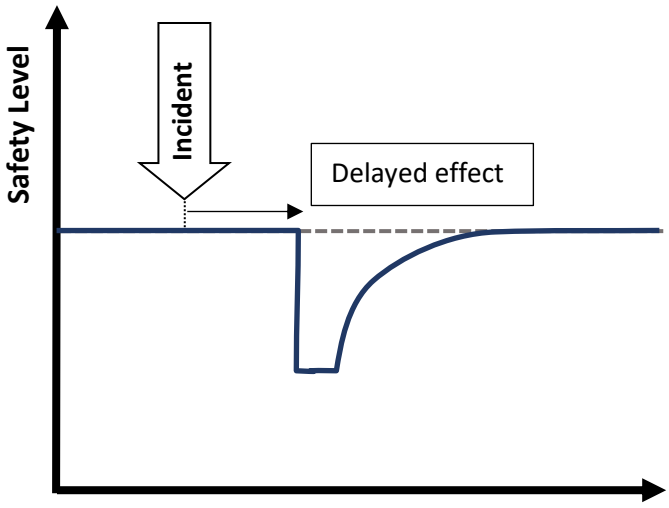

Figure 2: Incident with a delayed effect on safety

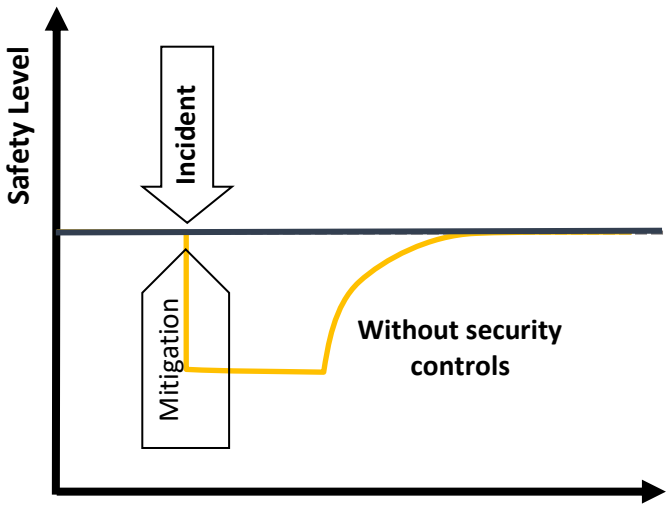

Figure 3: Incident with fully mitigated effect on safety

Moreover, it should be noticed that there might be different ways the same incident can be dealt with, since there are several factors that may affect safety.

In practical terms, the objectives for recovery time referred to as in AMC1 IS.D.OR.220(c) may be expressed as a list of resources and services to be restored by order of priority, within the scope of the recovery. Guidance about objectives for recovery time can be found in EUROCAE ED-206 – Chapter 7.3.5.

GM1 IS.D.OR.220(c) Information security incidents – detection, response and recovery

A recovery procedure or recovery plan should describe incident recovery actions and the internal or external resources that are involved (e.g. staff, IT, buildings, providers). Guidance about incident recovery plan can be found in EUROCAE ED-206 – Chapter 7 – Recover.

The resources required to apply the recovery measures should be available in order to implement recovery actions in a timely manner after an incident has occurred. Those resources may be internally available or provided by contracted organisations as foreseen by IS.D.OR.235. The contracting of recovery activities should be established before an incident occurs (proactive), and the contract should include provisions for the contracted party to react in a timely manner.

The return to a safe and secure state may initially require emergency measures, which are actions that are initiated based on the best information available at the time, before a complete understanding of the situation is achieved and these measures can potentially degrade the level of service or functionalities. The return to a safe and secure state should be evaluated against the initial risk assessment and may only temporarily differ from the normal operational conditions. However, any increase of the residual risk and the duration of this risk increase, i.e. due to the implementation of emergency measures, should be documented and accepted at the right level of accountability.

The recovery activities mentioned herein may also be the outcome of the response to incidents for which the organisation has received information that requires the implementation of adequate measures in order to react to security incidents or vulnerabilities with a potential impact on aviation safety.

In such context the organisation may not have a process or a recovery plan covering the specific occurrence. Therefore, the definition from the organisation/authority of a specific recovery plan and its approval by the competent authority is usually required.

AMC1 IS.D.OR.225 Response to findings notified by the competent authority

The compliance with IS.D.OR.225 should be demonstrated as required under the implementing regulation for the applicable organisation's domain.

GM1 IS.D.OR.225 Response to findings notified by the competent Authority

The requirement for the categorisation of findings and the period within which the actions in IS.D.OR.225(a) should be performed can be found in the implementing regulation for the domain, under the authority requirements. For the opening of findings related to this Regulation, the competent authority will follow the above-mentioned requirement.

GM1 IS.D.OR.230 Information security external reporting scheme

Organisations are required to report occurrences to their competent authority. In most cases, the competent authority is the one which has certified or approved the organisation.

EXAMPLES

Design organisations approved by EASA: EASA is the competent authority.

Air operators certified by the competent authority of a Member State: the competent authority of the Member State is the competent authority.

SPECIAL CASES

In a situation where an organisation has two air operator certificates (AOCs) under two different States (State A and B), it shall report occurrences involving aircraft operating under the State A AOC to the State A competent authority and occurrences involving aircraft operating under the State B AOC to the State B competent authority.

For organisations which are not certified or approved, the competent authority is that of the State in which the organisation has established its legal representation, for example: a ground handling organisation reports its occurrences under Regulation (EU No 376/2014 to the State in which it is established.

For organisations holding multiple approvals, the reporting will be done to the competent authority of the approved part of the organisation where the incident has occurred or the vulnerability discovered. In case the incident/vulnerability affects multiple approvals, the reporting will be done to all the competent authorities.

For organisations holding an approval but operating outside EU (e.g. Part-145), EASA is the competent authority and they have to report to the Agency.

Dual use aircraft — a vulnerability may need to be reported through both the military and civil reporting systems if it affects a dual-use function/system. Information reported through the civil reporting system should be sanitised (i.e. all sensitive information has been properly removed).

AMC1 IS.D.OR.230(a)&(b) Information security external reporting scheme

In order to comply with the provisions under IS.D.OR.230 (a) and (b), the organisation should report:

(a) under the Regulation (EU) No 376/2014 framework, any occurrence covered by this Regulation that is originated from intentional unauthorised electronic interactions. It is the responsibility of the competent authorities under Part-IS to ensure compliance with Article 7 of this Regulation and to filter out the information security incident part that needs to be shared with the information security competent authorities designated under Article 8 of Directive (EU) 2016/1148;

(b) information security incidents having a potential significant risk to aviation safety not covered under Regulation (EU) No 376/2014;

(c) vulnerabilities that pose a significant risk to aviation safety and are not patched through an approved vulnerability management strategy in accordance with AMC1 IS.D.OR.215(a)&(b).

GM1 IS.D.OR.230(a)&(b) Information security external reporting scheme

RELATION BETWEEN IS.D.OR.230(b) AND REGULATION (EU) NO 376/2014

Regulation (EU) No 376/2014 of the European Parliament and of the Council lays down requirements on the reporting, analysis and follow-up of occurrences in civil aviation. Compliance with point IS.D.OR.230(b) does not exempt organisations from compliance with Regulation (EU) No 376/2014.

For each category of reporter, Regulation (EU) 2015/1018 defines the nature of items to be mandatorily reported. Regulation EU) No 376/2014 also considers voluntary reporting of other items that are perceived by the reporter as a threat to aviation safety.

Furthermore, compliance with Regulation (EU) No 376/2014 does not exempt organisations from compliance with point IS.D.OR.230(b). However, this should not give rise to two parallel reporting systems, and point IS.D.OR.230(b) and Regulation (EU) No 376/2014 should be seen as complementary in that respect.

In practice, this means that reporting obligations under point IS.D.OR.230(b) on one hand and reporting obligations under Regulation (EU) No 376/2014 on the other hand are compatible. These reporting obligations may be discharged using one reporting channel. In addition, any natural or legal person that has more than one role subject to the obligation to report may discharge all those obligations through a single report. Organisations are encouraged to properly describe this in their organisation manual, to address cases in which the responsibilities are discharged on behalf of the organisation.

FOLLOW-UP ANALYSIS

When the analysis of an occurrence reported under Regulation (EU) No 376/2014 later identifies that the root cause or the contributing factor of the occurrence was an intentional unauthorised electronic interaction, the organisation should update its notification to the competent authority.

VULNERABILITY MANAGEMENT STRATEGY

Guidance regarding the vulnerability management strategy can be found in EUROCAE ED-206, Chapter 3.4 — Vulnerability Management Considerations. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

SIGNIFICANT RISK TO AVIATION SAFETY

Significant risk to aviation means unsafe condition, i.e. one that can result in an accident or a serious incident (as defined in ICAO Annex 13).

Note: The notion of unsafe condition also covers cases when the security incident violates the independence assumptions on system failure that are considered independent from a safety assessment perspective.

AMC1 IS.D.OR.230(c) Information security external reporting scheme

Within the overall limit of 72 hours the degree of urgency for submission of a report should be determined by the level of hazard judged to have resulted from the occurrence. Where an occurrence is judged by the person identifying the possible unsafe condition to have resulted in an immediate and particularly significant hazard, the competent authority expects to be advised immediately and by the fastest possible means (telephone, fax, email, telex, etc.) of whatever details are available at that time.

This initial notification should be followed up by a report within 72 hours. Where the occurrence is judged to have resulted in a less immediate and less significant hazard, the report submission may be delayed up to the maximum of 3 additional days in order to provide more details.

GM1 IS.D.OR.230(c) Information security external reporting scheme

Guidance regarding the reporting of security incidents and vulnerabilities can be found in EUROCAE ED-206, Chapter 6.4.2.2 – Reporting Timeline and Chapter 6.4.5 – Reporting Information Content. This is not the only source where guidance can be found, and the organisation may refer to different guidance more appropriate for their application.

Note: The person reporting an occurrence under Regulation (EU) No 376/2014 may not have the capability to determine the nature of the occurrence. This is particularly true for information security and the result can come from forensic analysis that determines the information security nature of the occurrence. The evaluation will be done as part of the initial internal reporting process (see IS.D.OR.215 and relevant AMC). The evaluation of the occurrence can demonstrate the possibility that it materialises into an unsafe condition taking into account the likelihood of realisation.

GM1 IS.D.OR.235 Contracting of information security management activities

The objectives of point IS.D.OR.235 are:

(d) to protect critical and sensitive information and assets when being handled by contracted organisations (including organisations in the supply chain) either at their facilities or organisation facilities, or when being transmitted between the organisation and contracted organisations, or being remotely accessed by contracted organisations;

(e) to prevent information security risks from being introduced through products and services developed or provided by the contracted organisations to the organisation, in the frame of the provision of information security management activities;

(f) to ensure that information security risks are managed throughout all the stages of the relation with the contracted organisations.

GM2 IS.D.OR.235 Contracting of information security management activities

The contracting of information security management activities is a means to allocate tasks from the contracting organisation to third parties (contracted organisations). The contracting organisation remains accountable for compliance with this Regulation.

GM3 IS.D.OR.235 Contracting of information security management activities

EXAMPLES

Examples of security management activities required under IS.D.OR.200 that can be contracted.

IS.D.OR.200 activity	Contracted activity
a-1: establishes a policy on information security describing the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;	Security policy drafting and consultancy
a-2: identifies and reviews information security risks in accordance with point IS.D.OR.205;	Identify activities, facilities and resources. Identify interfaces with other organisations which could be exposed to information security risks. Perform risk analysis or part of it, e.g. identify and classify information security risks.
a-3: defines and implements information security risk treatment measures in accordance with point IS.D.OR.210;	Define, develop and implement measures. Verify the initial and the continued effectiveness of the implemented measures (e.g. Red-Team/Blue-Team exercises, penetration testing, vulnerability scanning, etc.). Communicate to the involved stakeholders the outcome of the risk assessment and their responsibilities as part of the risk treatment process.
a-4: implements an information security internal reporting scheme in accordance with point IS.D.OR.215;	Define, develop and implement an internal reporting scheme to enable the collection and evaluation of information security events and vulnerabilities of equipment, processes and services.
a-5: defines and implements, in accordance with point IS.D.OR.220, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety except as permitted by point IS.D.OR.205(e), and responds to, and recovers from, those information security incidents;	Define, develop and implement measures to detect events. Define, develop and implement measures to respond to any event conditions. Define, develop and implement measures aimed at recovering from information security incidents.

IS.D.OR.200 activity	Contracted activity
a-6: implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;	Implement immediate reaction measures to a security incident or vulnerability as notified by the competent authority.
a-7: takes appropriate action, in accordance with point IS.D.OR.225, to address findings notified by the competent authority;	Identify root cause. Define corrective action plan. Provide evidence of the corrective actions implemented to close the finding.
a-8: implements an external reporting scheme in accordance with point IS.D.OR.230 in order to allow the competent authority to take appropriate actions;	Define, develop and implement an external reporting scheme to enable the communication of the information security incidents and vulnerabilities of equipment, processes and services to the competent authority and when required to the design approval holder or the organisation responsible for the design.
a-9: complies with the requirements contained in point IS.D.OR.235 when contracting any part of the activities described in point IS.D.OR.200 to other organisations;	
a-10: complies with the personnel requirements contained in point IS.D.OR.240;	Activities of the accountable manager / head of design in the frame of the provisions for a 'common responsible person' as referred to in IS.D.OR.240. Compliance monitoring as foreseen by IS.D.OR.240 Contracted organisation to ensure that sufficient personnel is on duty to perform the activities related to this Regulation Define, develop and deliver adequate training to achieve the competencies required by the staff. Perform pre-employment checks
a-11: complies with the record-keeping requirements contained in point IS.D.OR.245;	Define, develop and implement secured archiving. Provision of secure data centre (as a service) Provision of records updates

IS.D.OR.200 activity	Contracted activity
a-12: monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager or, in the case of design organisations, to the head of the design organisation, to ensure effective implementation of corrective actions;	Compliance monitoring (as foreseen by IS.D.OR.240) including the execution of independent audits
a-13: protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.	Define, develop and implement solutions to protect the confidentiality of any information
b: In order to continuously meet the objectives described in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.D.OR.260.	Execute independent effectiveness and maturity assessments. Define, develop and implement the necessary improvement measures.
c: The organisation shall document, in accordance with point IS.D.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.D.OR.200(a), and shall establish a process for amending this documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.D.OR.255.	Production of documentation to detail all key processes, procedures, roles and responsibilities required to comply with point IS.D.OR.200(a) (e.g. information security policies, general description of the staff, procedures to specify compliance). Define, develop and implement processes for approving amendments and changes.

AMC1 IS.D.OR.235(a) Contracting of information security management activities

(a) OVERSIGHT OF THE CONTRACTED ORGANISATION

In order to demonstrate proper oversight of the contracted organisation, the organisation should have:

(a) a process to ensure compliance with the provisions regarding contracted activities contained in this Regulation;

(b) a structured process to follow the expected execution of the contract that includes:

(i) definition and agreement of the scope of the activities;

(ii) definition and review of key performance indicators;

(iii) reaction to deviation from contractual obligations;

(iv) performance of audits, according to the predefined scope and objectives, with the aim of evaluating operational and associated assurance activities.

(b) MANAGEMENT OF THE RISKS ASSOCIATED WITH THE CONTRACTED ACTIVITIES

In order to demonstrate proper management of the risks associated with the contracted activities, the organisation should meet the following criteria:

(1) A prior assessment of the suppliers is conducted before outsourcing any security management activities. The assessment should evaluate suppliers' competencies, sustainability as well as qualifications in the relation to the activities to be contracted.

(2) There is an assessment of the risks associated with the provision of the contracted activities that has been agreed between the organisation under Part-IS and the contracted organisation.

(3) The organisation establishes and maintains an information security focal point with the contracted organisation.

GM1 IS.D.OR.235(a) Contracting of information security management activities

RISK ASSESSMENT ASSOCIATED WITH THE PROVISION OF THE CONTRACTED ACTIVITIES

The risk assessment should take into account the maturity level of the contracted organisation, and should consider the following:

(e) Identification and assessment of critical and sensitive information and assets that may be shared with, or provided by, external suppliers;

(f) Identification of the information security requirements of the organisation that are applicable to the contracted organisation;

(g) Evaluation, by means of a supplier assessment, of the ability of the contracted organisation (both existing and new contracted organisations) to meet the information security requirements of the contracting organisation;

(h) Assessment of risks that may be introduced by the contracted organisation.

This agreed risk assessment should also include the roles and responsibilities of the parties (i.e. contracting and contracted organisation).

GM2 IS.D.OR.235(a) Contracting of information security management activities

AUDIT OF CONTRACTED ORGANISATIONS

The following aspects should be considered by the organisation when auditing an supplier contracted to perform security management activities:

— the scope of the audit as well as the objective should be limited to processes, resources and data used for the execution of Part-IS contracted activities;

— compliance and/or implementation audits should be done at the contracting organisation's discretion;

— findings identified during an audit shall be addressed through a remediation plan with a timeframe to be validated by the contracting organisation.

AMC1 IS.D.OR.235(b) Contracting of information security management activities

In order to ensure access upon request to the contracted organisation, the organisation under Part-IS should include proper clauses and requirements in the contractual documents.

The competent authority's access to the contracted organisations should be at least equivalent to that granted to the contracting organisation and, in any case, sufficient to ensure the assessment of continued compliance with the requirements within the scope of the contracted activities.

GM1 IS.D.OR.235(b) Contracting of information security management activities

Access to the contracted organisation means to have visibility of evidence for compliance of the contracted activities (such as artefacts, documents, independent certifications).

Evidence of compliance could be achieved either by transfer of documents and/or access to information at the premises in accordance with the 'audit scope' as defined in the contract.

The opportunity to visit the premises should be evaluated considering different aspects such as the sensitivity of the related information or the practical accessibility to the contracted organisation (e.g. the contracted organisation is a service provider with distributed resources).

GM1 IS.D.OR.240 Personnel requirements

The objectives of the requirements contained in points (a) through (e) are:

(a) to ensure that an effective organisational structure is in place in order to comply with the requirements of this Regulation;

(b) to provide trust to other organisations with whom they share risks.

AMC1 IS.D.OR.240(a)(2) Personnel requirements

PROMOTION OF INFORMATION SECURITY POLICY

The accountable manager of the organisation or, in the case of design organisations, the head of the design organisation should make sure that the information security policy is known and easily accessible for all staff members.

AMC1 IS.D.OR.240(a)(3) Personnel requirements

BASIC UNDERSTANDING OF THE REGULATION

In order to demonstrate a basic understanding of this Regulation, the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation should have:

(c) the ability to explain the overarching objectives of the Regulation and its implications for the organisation;

(d) records of training on the content of the Regulation and the technical basis to comply with it, as well as documented work experience in areas of activities pertinent to this Regulation.

GM1 IS.D.OR.240(a)(3) Personnel requirements

BASIC UNDERSTANDING OF THE REGULATION

The training material should cover the overarching objectives of the Regulation, and the assessment should evaluate the understanding of these regulatory objectives.

AMC1 IS.D.OR.240(b)&(c) Personnel requirements

APPOINTMENT OF A PERSON OR GROUP OF PERSONS

The person or group of persons appointed under point IS.D.OR.240(b) with the responsibility to ensure compliance with the requirements of this Regulation should represent the management structure of the organisation.

The person or group of persons should be directly responsible to the accountable manager for providing guidance, direction and support for the planning, implementation and operation of the process and standards to comply with the Regulation. They should have direct access to keep the accountable manager properly informed on compliance and security matters (for instance, through meetings organised on a regularly basis).

Appointments should take into account the possibility that a person may not be able to carry out the organisational tasks assigned to them for a period of time, and thus also identify the necessary deputies.

These nominated persons should demonstrate a complete understanding of the requirements of this Regulation, to be able to ensure that the organisation's processes and standards accurately reflect the applicable requirements. It is their role to ensure that compliance is proactively managed, and that any early warning signs of non-compliance are documented and acted upon.

A description of the functions and the responsibilities of the appointed persons and deputies, including their names, should be contained in the ISMM (see point IS.D.OR.250).

GM1 IS.D.OR.240(b) Personnel requirements

A condition of a lengthy absence occurs when a person is unable to fulfil the assigned organisational duties and therefore a potential vulnerability may arise.

GM1 IS.D.OR.240(b)&(c) Personnel requirements

Appointments should be made by email, organisational chart, roles & responsibilities table, etc. usually in use by the organisation. The organisation may adopt any titles for the foregoing managerial positions, but it should identify to the competent authority the titles and the persons chosen to carry out these functions.

AMC1 IS.D.OR.240(d) Personnel requirements

COORDINATION

The criteria to establish a coordination that ensures an adequate integration of the information security management within the organisation are the following:

(e) the scope and boundaries of the organisations have been established and communicated to the common responsible person;

(f) the requirements of this Regulation have been communicated to and shared with the common responsible person;

(g) the common responsible person has direct access to the accountable manager;

(h) issues are proactively managed and any early warning signs of non-compliance are documented and acted upon.

GM1 IS.D.OR.240(e) Personnel requirements

COMMMON RESPONSIBLE PERSON

The common responsible person should be capable of managing the organisation's cybersecurity strategy and its implementation to ensure the achievement of the objectives described in Article 1. If this person is delegated by the accountable manager or, in the case of design organisations, by the head of the design organisation, for the activities under this Regulation, this person should also be given the appropriate delegation that is necessary to implement the provisions of IS.D.OR.200, including the authority and the financial means to mobilise and control the resources across the organisations, or parts of the organisation involved.

According to the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022, this person may be described, for instance, as (Chief) Information Security Officer, Cybersecurity Programme Director or Information Security Manager.

AMC1 IS.D.OR.240(f) Personnel requirements

PERSONNEL SUFFICIENCY

To determine the sufficiency of the personnel, the following elements should be taken into consideration:

— the organisational structures, policies, processes and procedures subject to information security management;

— the amount of coordination required with other organisations, contractors and suppliers;

— the level of risk associated with the activities performed by the organisation.

GM1 IS.D.OR.240(f) Personnel requirements

PERSONNEL SUFFICIENCY

For the purpose of this Regulation, personnel refers to the combination of the personnel directly employed by the organisation, as well as the personnel contracted as specified in IS.D.OR.235.

The activities reported in Appendix II 'Main tasks stemming from the implementation of the Part-IS Regulation' should be considered when establishing the organisational structure necessary to comply with the requirements of this Regulation.

AMC1 IS.D.OR.240 (g) Personnel requirements

PERSONNEL COMPETENCE

To determine the competence needed by the personnel performing the activities, the following elements should be taken into consideration:

— work roles and the associated tasks;

— required knowledge, skills and abilities.

As part of the process to ensure that personnel maintain the necessary competence, the organisation should:

— assess the personnel qualifications and experience with respect to the required competence for the assigned work roles to identify gaps;

— align the personnel qualifications and experience with the expected competence by either organising adequate learning programmes for existing personnel members, recruiting new resources, or a combination thereof.

GM1 IS.D.OR.240(g) Personnel requirements

TRAINING PROGRAMME

A training programme should start with the identification of the competence required by the staff for each role, followed by the identification of the gaps between the existing competence and the required one.

In order to develop the list of competencies an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the NICE (National Initiative for Cybersecurity Education) based on the NIST Cybersecurity Framework (NIST CF).

The competencies listed in Appendix II, stemming from the NIST CF, that are mapped to the main tasks of this Regulation may be used to establish a baseline to identify the aforementioned competence gaps.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the organisation's needs considering the size, scope, required competencies, and complexity of the organisation.
Finally, as information security/cybersecurity evolves due to the rise of new threats, the organisation should periodically review the adequacy of the training programme.

AMC1 IS.D.OR.240(h) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Regarding any assigned role and task, the organisation should specify all information security responsibilities an employee has in a clear and transparent manner.

As part of this, the employee should acknowledge, in a traceable and verifiable manner, understanding of the instructions received as well as the expected roles and responsibilities.

GM1 IS.D.OR.240(h) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

Acknowledgement of receipt such as a valid electronic or wet signature, confirmation email, etc., is a traceable proof of acknowledgement.

AMC1 IS.D.OR.240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

(a) The establishment of a person's identity should be determined on the basis of documentary evidence.

(b) Regarding the establishment of trustworthiness, a standard level of vetting, which includes the following verification of:

— employment, education and any gaps during at least the preceding 5 years;

— criminal records in all states of residence during at least the preceding 5 years,

should always be completed, taking also into account the relevant national laws and regulations.

(c) In case the information system and data to be accessed have been associated with a high severity of the safety consequences in accordance with GM1 IS.D.OR.205(c), an enhanced level of vetting should be performed for persons having administrator rights or unsupervised and unlimited access, or having been otherwise identified in the risk assessment in accordance with IS.D.OR.205.

(d) An enhanced level of vetting should include the verification, to be completed in accordance with relevant national laws and regulations, of:

— employment, education and any gaps during at least the preceding 5 years;

— criminal records in all states of residence during at least the preceding 5 years;

— intelligence and any other relevant information (e.g. available to the national competent authorities) that is considered to be relevant for the suitability of a person to work in a function which requires an enhanced level of vetting.

GM1 IS.D.OR.240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

Enhanced level of vetting may be used when already existing controls or mitigation measures for risk treatment identified during the risk analysis rely on organisational/operational procedures. Thus, enhanced level of vetting is needed for personnel who applies such measures — for instance, correct configuration and administration of information technologies, database operations, security monitoring, etc.

Intelligence and any other relevant information should be gathered by screening and analysing public sources such as social media and websites.

Standard and enhanced background check, as defined in Regulation (EU) 2015/1998, are suitable for the standard and enhanced level of vetting respectively. However, it should be noted that the standard and enhanced levels of vetting referred to in AMC1 IS.D.OR.240(i) do not constitute compliance with the provisions on background checks as defined in Regulation (EU) 2015/1998.

GM1 IS.D.OR.245 Record-keeping

Records are required to document results achieved or to provide evidence of activities performed. Records become factual when recorded and cannot be modified. Therefore, they are not subject to version control. Even when a new record is produced covering the same issue, the previous record remains valid.

The 'approval received' referred to in point (a)(1)(i) includes any 'certificate' received by the organisation when it is foreseen by the implementing rule for its domain.

AMC1 IS.D.OR.245(a)(1)(vi)&(a)(5) Record-keeping

When complying with the requirements under points (a)(1)(vi) and (a)(5), the organisation should establish a data retention policy defining procedures to:

(a) manage relevant security data files;

(b) establish the periodical assessment of their content; and

(c) define the criteria to allow deletion of events when the objective of the requirement under (a)(5) is no longer met.

GM1 IS.D.OR.245(a)(1)(vi)&(a)(5) Record-keeping

The objective of the requirement (a)(1)(vi) is to ensure detection of possible indication of compromise or vulnerabilities which are not obvious by normal operation (e.g. previously unknown situations), while the objective of the requirement under (a)(5) is to allow the necessary flexibility to control the volume of the stored security events.

Records of information security events include those events identified to be within the scope of the detection activities under IS.D.OR.220(a), as well as other security data produced by assets that have been identified under IS.D.OR.205.

A data retention policy clarifies what information should be stored or archived and for how long. Some guidance about data retention can be found in EUROCAE ED-206 Chapter 2.6.

Once a data set completes its retention period, it can be deleted or moved as permanent historical data to a secondary or tertiary storage.

AMC1 IS.D.OR.245(c)&(d) Record-keeping

When complying with the requirements under points (c) and (d) for all the records required by points IS.D.OR.245 (a) and (b), the organisation should consider the following:

(a) Records should be kept in paper form or in electronic format or a combination of both media. The records should remain accessible whenever needed within a reasonable time and usable

throughout the required retention period. The retention period starts when the record has been created.

(b) Records data integrity and availability should be protected in consistency with protection of corresponding operational data, and as such, should be within the scope of the ISMS.

(c) Backup/archiving systems should be protected against unauthorised access (i.e., data leakage attempts against personal data/modification of records) and thus should have security measures implemented in consistency with the level of cyber risk associated with them.

(d) Once records shall not be retained anymore, the destruction of records and decommissioning of assets used for their storage should be implemented appropriately.

GM1 IS.D.OR.245(c)&(d) Record-keeping

RECORDS ACCESSIBILITY THROUGHOUT THE RETENTION PERIOD

It is recommended to follow best practices for data retention and backup strategies, such as using automated backup tools, segregation or geographical separation of the backup storage location(s), and to consider offline backups to prevent ransomware risks. These criteria should be considered also when record-keeping is contracted to service providers with distributed resources.

Special attention should be paid to significant hardware and software changes, ensuring that stored digital records remain accessible and readable (e.g. file system, application file format, forward compatible database versions, etc.). Paper-based information needs to be archived in an adequate environment, in which records are protected against long-term degradation factors (e.g. heat, light, humidity).

RECORDS DATA INTEGRITY AND PROTECTION FROM UNAUTHORISED ACCESS

A commonly used method to achieve authenticity and integrity protection is the use of digital signatures at document level. Digital signatures can be added to the document's file (e.g. PDF) to ensure that a record has not been modified by someone other than its author (integrity) and that the author is who is expected to be (authenticity).

Moreover, to prevent unauthorised access, a record can be protected with a password at file level. Commercial applications feature built-in basic password protection functions for their file formats. Access protection can also be achieved by protecting the environment where the individual records are stored (e.g. access protection on databases, file shares, directories, etc.).

GM1 IS.D.OR.255 Changes to the information security management system

Rule point IS.D.OR.255 is structured as follows:

Point (a) introduces the possibility for the organisation to agree with the competent authority that changes to the ISMS can be implemented without prior approval as long as these changes are covered in a change procedure.

Point (b) introduces an obligation of prior approval (by the competent authority) for changes not covered by the procedure mentioned above, and also indicates how those changes should be handled.

The organisation should consider the establishment of a procedure in order to manage and notify changes to the competent authority as foreseen under IS.D.OR.255(a). In case of lack of any approved

procedure, the organisation will have, for any change, to apply for and obtain an approval as required under IS.D.OR.255(b). In any case, all changes should be notified to the competent authority upon implementation.

GM1 IS.D.OR.250(a) Information security management manual (ISMM)

The organisation may choose to document some of the information required under point IS.D.OR.250(a) in separate documents (e.g. procedures). In this case, it should ensure that the manual contains adequate references to any document kept separately. Any such documents are then to be considered an integral part of the organisation's information security management system manual.

AMC1 IS.D.OR.255 Changes to the information security management system

The procedure should cover the change management and the criteria for the notification of changes. The change management should explain how changes are managed, including the evidence that should be produced to describe a change and its impact.

With regard to prior approval of changes, the organisation may, upon valid justification in the developed procedure, propose changes that can be implemented without the need for such prior approval by the competent authority.

Without prejudice to the communication regarding changes as required under the implementing rule for the domain, the procedure should take into account the criticality of the changes when proposing how they will be managed. In particular, those changes that could have a significant impact on achieving or maintaining compliance with the provisions under Part-IS, or which could lead to an unacceptable level of risk (e.g. as per the guidance provided in GM1 IS.D.OR.205(c)), should be subjected to rigorous scrutiny.

When applying for prior approval for a change not covered under the approved procedure, at least the following information should be provided:

— the nature and purpose of the change;

— the implementation plan of the change;

— the verification plan of the change;

— the impact to aviation safety introduced by the change.

A significant deviation from the original plan during the change process should be considered as a new change to be communicated to the competent authority to obtain approval.

GM2 IS.D.OR.255 Changes to the information security management system

Changes within the following areas should be considered as potentially resulting in a significant impact on establishing or maintaining compliance with the provisions under Part-IS:

(e) changes in the scope of the ISMS, as per AMC1 IS.D.OR.200(a)(1), interfaces or related policies;

(f) changes in responsibilities and accountability as well as in the organisational structure involving the implementation and continuing monitoring of compliance with this Regulation;

(g) changes to the methodology used for risk management;

(h) changes to the incident management process.

GM3 IS.D.OR.255 Changes to the information security management system

RELATION BETWEEN CHANGES TO THE ISMS AND CONTINUOUS IMPROVEMENT

Changes stemming from the continuous improvement process established by the organisation (see IS.D.OR.260) should be handled as any other change according to the guidelines in AMC1 IS.D.OR.255 and GM2 IS.D.OR.255.

EXAMPLE SCENARIOS OF CHANGES WITH A SIGNIFICANT IMPACT ON ESTABLISHING OR MAINTAINING COMPLIANCE WITH THE PROVISIONS UNDER PART-IS, OR WHICH COULD LEAD TO AN UNACCEPTABLE LEVEL OF RISK

With reference to the GM2 IS.D.OR.255, below are some examples of changes that could have a significant impact on achieving or maintaining compliance with the provisions under Part-IS, or which could lead to an unacceptable level of risk:

(e) Changes to the scope of the ISMS, as per AMC1 IS.D.OR.200(a)(1), interfaces or related policies:

- The organisation expands its business functions, and integrates another company within its organisational structure.
- The organisation has identified non-conformities indicating an incorrect scope.
- The organisation amends its information security policy and/or information security objectives with a potential impact on aviation safety.
- Changes to the interfaces of the organisation resulting e.g. from modification in the insourced or outsourced activities.

(f) Changes in responsibilities and accountability as well as in the organisational structure involving the implementation and continuing monitoring of compliance with this Regulation:

- The accountable manager or, in the case of design organisations, the head of the design organisation, has delegated certain responsibilities under Part-IS to a person or a group of persons.
- The organisation contracts information security management activities as per IS.D.OR.235.

(g) Changes to the methodology used for risk management:

- The organisation changes the classification for likelihood or impact in their risk management methodology e.g. to obtain more granularity.
- The organisation implements changes to their risk treatment methodology.
- The organisation integrates its information security risk management into existing management systems.

(h) Changes to the incident management process:

- The organisation decides to contract incident management activities.

— The organisation changes the process to notify incidents and the criteria to escalate to higher management for a quicker resolution.

— The organisation changes its incident recovery procedure.

EXAMPLE SCENARIOS OF CHANGES WITHOUT A SIGNIFICANT IMPACT

— After a successfully detected security event which could have easily evolved to an incident, the organisation decides to roll out an extensive cyber security awareness campaign for all employees

— Update in the staff training programme and/or training content as a result of the continuous improvement processes established within the organisation

— The organisation replaces the software tool that it uses for encrypting sensitive files with another software solution.

— The organisation has decided to make an internal restructuring for business reasons, changing the names of departments or sections, without making any changes in the responsibilities and accountability (e.g. accountable manager) involving the ISMS of the organisation.

— The organisation decides to update an existing preventive control e.g. configuring a new firewall in its internal network.

AMC1 IS.D.OR.260 Continuous improvement

The continuous improvement process (CIP), as required by IS.D.OR.200(b), should aim to continuously improve the effectiveness, suitability and adequacy of the ISMS. This should be achieved by a proactive and systematic assessment of the ISMS and all of its elements including its maturity. The assessment should take into account the outcomes and conclusions of other information security and assurance processes including audits, management reviews, evaluation of performance, effectiveness and maturity, as well as the outcomes of the derived corrective actions and corrections.

The steps to be performed should be at least the following:

(f) Identify improvement opportunities based on the outcomes of the assessment of the ISMS with respect to its suitability, effectiveness, adequacy and, if deemed necessary, efficiency, as well as any other suggestion for improvement. The assessment should consider performance indicators which reflect its processes and elements and the defined objectives for effectiveness and maturity.

(g) Evaluate the identified opportunities regarding cost benefit, absence or reduction of undesired effects and achievement of the targeted objectives and intended outcomes.

(h) Propose the evaluated improvement opportunities to the management, and recommend actions to support their review and decision-making.

(i) According to the decision taken under point (c), plan, develop and implement actions and changes to the ISMS, its processes or elements to achieve the improvements.

(j) Evaluate the effectiveness of the implemented actions and ISMS changes, and, as applicable, verify that the root cause of identified deficiencies has been eliminated.

The management should assess and review the outcomes of the CIP at planned intervals to ensure the continuing effectiveness, adequacy and suitability of the ISMS, to decide on the prioritisation of the implementation of actions and changes, as well as to revise or set new objectives or targets for continuous improvement.

GM1 IS.D.OR.260 Continuous improvement

Point IS.D.OR.260 covers assurance processes for the ISMS in a manner that can be considered equivalent to the safety assurance in ICAO Doc 9859 'Safety Management Manual (SMM), which includes performance monitoring and measurement, management of change and continuous improvement of the SMS.

In this Regulation:

— IS.D.OR.260(a) addresses, using adequate performance indicators, the effectiveness and maturity assessment of the ISMS;

— IS.D.OR.260(b) addresses the improvement measures, i.e. corrections and corrective actions, for the deficiencies detected in IS.AR.260(a) and the continuous improvement process.

Similar provisions for continuous improvement are foreseen in other information management systems such as ISO 27001 (see Appendix II to this document).

The context and risk environment of organisations are never static and therefore require a dynamic adaptation, evolution and change of the entity's objectives, architectures, organisational structures and processes to maintain the information security risks at an acceptable level. Consequently, the ISMS should be considered as an evolving and learning part/element of the entity which needs to be continuously monitored and improved to ensure alignment with the entity's safety objectives and effectiveness.

The CIP aims to continuously improve the effectiveness, suitability, adequacy and, if deemed necessary, the efficiency of the ISMS. An entity may integrate the Part-IS CIP in some other already operated CIP and may apply methods such as Plan-Do-Check-Act (PDCA) Cycle or Define-Measure-Analyse-Improve-Control (DMAIC) (see also GM1 IS.D.OR.200).

The CIP is based on a proactive and systematic assessment of the ISMS and all its elements including the information security processes and controls driven by the ISMS. The assessment should be carried out against organisational targets for desired levels of performance, effectiveness and maturity. These targets, besides ensuring the achievement of compliance with the requirements under this Regulation, may also aim to include objectives established by the entity's policy or standards and by management decisions.

The above-mentioned assessment is based on the outcome of performance evaluations, audits, risk and incident processes, as well as already applied corrections and corrective actions. Some factors that should be considered when performing the assessment are the following:

— **Adequacy** refers to whether the system uses industry standards for information security in a sufficient manner with regard to compliance with the requirements of this Regulation.

— **Effectiveness of the ISMS** and the effective implementation of processes and controls driven by the ISMS is assessed by analysing whether the:

- the information security risks are managed to achieve the safety objectives;
- the intended outcomes of the ISMS are achieved, and the requirements or objectives are met;
- all types of deficiencies are managed including failures to fulfil or correctly implement a requirement or control.

— **Efficiency** of the ISMS refers to the implementation of streamlined processes, however, efficiency improvements should not adversely impact effectiveness.

Identification of improvement opportunities

Improvement opportunities may be identified from the results of the CIP assessment or may be introduced as suggestions from other sources. The identification often involves deviations or corrective actions as well as ineffective processes or controls which are not remediated.

Suggestions for improvements stem from sources including:

— Risk management: results of regular risk analysis and subsequent risk treatment are a primary factor in improving the ISMS, where the risk treatment process involves monitoring of the implemented security measures and evaluating their effectiveness.

— Performance & effectiveness evaluation: conclusions from (key) performance Indicators, their measurement, analysis and continued monitoring as well as the result of the assessment of the effectiveness including the outcomes of the subsequently applied corrections and corrective actions

— Evaluation of maturity including the results of the subsequent corrections and corrective actions

— Lessons learned from the security incident detection, handling and response process and from a potential treatment of a root cause

— Results of (internal) audits may be used to verify whether the ISMS and controls within the audit scope meet the entity's requirements, and to determine where there are potential areas for improvement.

— Review and evaluation by management, review of the current action plan, setting or revision of the objectives or decision on improvement opportunities and actions.

— Entity's suggestion programme (suggestions for improvement), reviews, surveys or assessments with employees or feedback from suppliers or interfacing parties

Any outcome of this process should be documented. The resulting actions may be integrated into an overarching action plan which is centrally consolidated and periodically reviewed according to the relevant policies. The resulting action plan may be further divided into a tactical, short-/mid-term action plan and a strategic, long-term action plan.

AMC1 IS.D.OR.260(a) Continuous improvement

(a) **ISMS EFFECTIVENESS EVALUATION**

When complying with IS.D.OR.260(a), the organisation should have a process in place to monitor, measure, evaluate and review the effectiveness of its ISMS that defines:

(1) who monitors, measures, analyses and evaluates the results and takes accountable decisions;

(2) when the above steps should be performed;

(3) which methods for monitoring, measurement, analysis and evaluation are applied to ensure comparable and reproducible results.

The frequency of the assessments should be commensurate with the level of risk established under IS.D.OR.205.

The process to monitor, measure, evaluate and review the effectiveness of its ISMS referred to under AMC1 IS.D.OR.260(a) should include as a minimum:

(1) the gathering and retention of metrics of the activities, and additional information that could be useful for monitoring purposes,

(2) the analysis of the metrics in order to identify trends and deviations from predefined performance targets.

(b) **ISMS MATURITY EVALUATION**

The organisation should assess the maturity of its ISMS using a suitable maturity model in order to identify areas for improvement to the ISMS. To do so, the organisation should:

(1) define or adopt a maturity model which represents a set of important and relevant processes and capabilities that are expected to be implemented and maintained;

(2) for each assessed process or capability, define in the model criteria against which specific aspects, characteristics and effectiveness should be assessed and evaluated when determining a maturity level;

(3) define for each assessed process or capability its desired target maturity level.

(c) For each assessed security process or capability contained in the maturity model, the organisation should:

(1) evaluate and justify the current maturity level;

(2) identify any area for improvement it should make to reach the targeted maturity level;

(3) collect and record the evidence regarding strengths and weaknesses of the implemented ISMS and its evaluated maturity.

GM1 IS.D.OR.260(a) Continuous improvement

(a) As general guidance, the elements of the ISMS that should be monitored, measured and evaluated should be, as a minimum:

(1) the risk assessment and treatment process (including risks at the interfaces with other

organisations);

(2) the management of non-conformities and corrective actions;

(3) the incident and vulnerability management;

(4) the personnel competence management.

(b) Existing maturity models for ISMS maturity evaluation

As general guidance for the definition or the adoption of a maturity model (MM), the following existing models may be considered:

— Cybersecurity Capability Maturity Model (C2M2), version 1.1: this model was published by the US Department of Energy in 2014. It introduces the notion of Maturity Indicator Levels (MIL) ranging from 0 to 3, and addresses not only performance levels but also performance practices (under Approach Objectives and approach progression) as well as assurance practices (under Management Objectives and institutionalization progression).

— Systems Security Engineering – Capability Maturity Model (SSE-CMM): published by ISO as ISO 21827 in 2008. It focuses on engineering practices, much less on operational practices that are split in 11 'Security Base Practices', and 11 'Project and Organizational Base Practices'. It introduces the notion of five Capability Levels, from 'Performed Informally' to 'Continuously Improving'.

— NIST Cybersecurity Framework (NIST CF), version 1.1: published by NIST in April 2018. Although it is not proposed as a MM, the framework defines four 'Implementation Tiers', from 'Partial' to 'Adaptive', which are a qualitative measure of organisational cybersecurity risk management practices. It focuses on the functionality and repeatability of cybersecurity risk management.

— ATM Cybersecurity Maturity Model, edition 1: published in February 2019 by the EUROCONTROL NM for organisations in the ATM domain. Whilst not being designed for wider application, it can be adapted as necessary. It defines five maturity levels, ranging from 'Non-existent' to 'Adaptive' inspired by the 'Tier' terminology from the NIST CSF. In fact, the model is founded on NIST CSF, together with some elements of ISO 27001.

The following Table 1 maps the MM mentioned above to a hypothetical five-level MM.

Mapping with a five levels MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial	MIL 0	Non-Existent	Performed Informally	
Defined	MIL 1 (Initial)	Partial	Planned & Tracked	Partial
Implemented	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved		Adaptive	Continuously Improving	Adaptive

Table 1: Mapping matrix of an existing MM to a hypothetical five-level MM

AMC1 IS.D.OR.260(b) Continuous improvement

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

Based on an evaluation of the impact and extent of the deficiency and the potential consequences on the ISMS, the process should include as criteria for compliance:

(f) deciding on corrections and their implementation without undue delay in order to limit the impact of the deficiency and deal with its consequences as well as, as applicable, to control or eliminate it;

(g) deciding on the need for, and the implementation of, corrective actions to eliminate the cause and contributing factors of the deficiency based on a root cause analysis and an evaluation of actions remediating the cause aimed at being proportionate to the consequences and impact of the deficiency;

(h) verifying the implemented actions:

— to be effective and to result in acceptable residual risks,

— not to have unintended side effects leading to other deficiencies, new risks, or an ISMS not aligned with the applicable requirements, as well as

— for corrective actions, to effectively remediate or eliminate the root cause;

(i) reporting to and reviewing the identified deficiencies, action plan and results of the action taken with the accountable manager of the organisation or, in the case of design organisations, the head of the design organisation or delegated person(s) and, as necessary, with other involved or affected roles and parties;

(j) documenting as evidence the detected deficiencies, the planned and implemented corrections and/or corrective actions with deadlines and responsible persons, the management feedback, the outcomes of the process under point (c) above and, if necessary, the change decisions made

for the ISMS itself.

GM1 IS.D.OR.260(b) Continuous improvement

The 'necessary improvement measures' referred to in IS.D.OR.260(b) refer to correction or corrective actions to eliminate deficiencies or actions aimed at improving the effectiveness as well as the maturity of the ISMS.

A process satisfying the criteria defined in the AMC1 IS.D.OR.260 should include the following aspects:

(h) identifying the extent, impact, context and triggers of the deficiency, evaluating it according to some established criteria, analysing potential consequences on the ISMS including a potential existence in other areas;

(i) deciding on corrections and their implementation to immediately limit the impact and manage the consequences of the deficiency as well as, as applicable, to control or eliminate it;

(j) deciding on corrective actions required to eliminate the (root) cause(s) of the deficiency that are proportionate to the consequences;

(k) reassessing the elements of the ISMS which may be affected by the implemented actions to ensure that no further risk is introduced;

(l) verifying the implemented actions (see point (c) of AMC1 IS.D.OR.260(b));

(m) reporting to and reviewing the outcomes of the process steps with the management (see point (d) of AMC1 IS.D.OR.260(b);

(n) documenting and evidencing the result of the process steps above (see point (e) of AMC1 IS.D.OR.260(b)).

APPENDIX I

Examples of threat scenarios with a potential harmful impact on safety

The following is a non-exhaustive list of examples of information security threat scenarios with a potential harmful impact on safety that may be considered by authorities and organisations.

Example 1: Aircraft cockpit communications used for air traffic control (ATC) and aircraft pilot voice and datalink communications

— Threat vector assets/domain
  — ATC voice and ground automation systems
  — ground communications providers
  — air-ground/ground-air RF communications service providers
  — aircraft and the assets used for voice and datalink communications

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety.

— Non-exhaustive summary of potential threats
  — threat (availability): jamming
  — threat (integrity): man-in-the-middle or injection attacks
  — threat (confidentiality): insider threat

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety
  — Disruption of services prevent ATC communication with a single or multiple aircraft and/or ATC ground system
  — The manipulation of data through a man-in-the-middle attack would present false information to the pilot and/or ATC system with the potential of creating a safety hazard or injection of data to the aircraft or ground systems to disrupt the service and capability.
  — There are no specific requirements for encryption of data or voice for datalink communications; however, for confidentiality purposes, the assets used to provide and deliver the services should be controlled and limited to only those resources that require access to ensure that the services cannot be disrupted and manipulated in any way.

  *NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Example 2: Use of GPS for navigation by aircraft and ATM ground systems

— Non-exhaustive summary of potential threats

  — threat (availability): jamming, system (hardware/software) vulnerability exploitation

  — threat (integrity): spoofing (GPS signal), man-in-the-middle or injection attacks (PNT data)

  — threat (confidentiality): insider threat

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety

  — Disruption of services prevents effective aircraft navigation by the aircraft pilot and crew and ATC

  — Disruption of GPS or manipulation of a GPS signal used for ATC ground-based navigation devices and automation systems that rely on GPS for ATC synchronisation affects the ability of ANSPs to provide a single or multiple aircraft with services.

  — The manipulation of data through a man-in-the-middle attack presents false information to the pilot and/or ATC system with the potential of creating a safety hazard or injection of data to the aircraft or ground systems and thus disrupts the service and capability.

  — Uncontrolled access to navigation systems and the assets used to provide navigation services allows manipulation and disruption of services.

  *NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Application of bow-tie analysis to this example

Two coordinated bow-tie analyses of different risk dimensions are combined, as the ultimate interest lies only in the aviation safety consequence.

Information security bow-tie analysis element	Aviation safety bow-tie analysis element
Information security threats 1) jamming of GPS spectrum 2) system vulnerability exploitation 3) man-in-the-middle attack 4) insider intentional interaction	
Information security preventive barriers	
Information security hazards & top events 1) disturbed GPS spectrum (hazard) → *unreliable GPS position* 2) system integrity compromised (hazard) → *system function unpredictable* 3) manipulation of information during communication (hazard) → *undetectable falsification of information* 4) access to resources not adequately controlled (hazard) → *insider gets access to system resources*	**Safety threats** 1) unreliable GPS navigation function 2) unpredictable system function 3) undetectable falsification of information 4) insider gets access to system resources
Information security mitigative barriers	**Safety preventive barriers** 1) provision of different navigation systems (dissimilarity) 2) etc.
Information security consequences 1) loss of GPS availability (= in case of sole navigation function) 2) loss of system function integrity (= some system function inoperative) 3) loss of information integrity (= some information is incorrect)	**Safety hazards & top events** 1) loss of GPS signal (hazard) → unavailability of GPS information on the aircraft 2) loss of individual system function (hazard) → degraded aircraft system performance

4) loss of availability, integrity, or confidentiality (= all types of compromise possible)	3) loss of information integrity (hazard) → presentation of incorrect information to pilots or systems 4) loss of availability, integrity, or confidentiality (hazard) → unreliable system performance
	Safety mitigative barriers 1) Use of dissimilar navigation means 2) etc.
	Safety consequences 1) loss of airspace separation (disruption of services that prevent effective aircraft navigation by the aircraft pilot and crew and ATC) 2) disruption of ATC function or manipulation of information impacts the ability to provide services to aircraft 3) loss of airspace separation, disruption of ATC functions and services 4) disruption of ATC function or manipulation of information impacts the ability to provide services to aircraft

Example 3: Aircraft operator and aircraft maintenance organisations' software supply chain and ground infrastructure used to support aircraft management and operations

— Threat vector assets/domain

  — Aircraft operator or maintenance ground supply chain for aircraft parts, hardware and software

  — Aircraft operator or maintenance ground internal infrastructure used to manage aircraft operations (hardware/software) and other information technology assets

  — Aircraft operator information technology assets used to update systems on an aircraft (software/hardware) used for maintenance operations

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety.

— Non-exhaustive summary of potential threats

  — threat (availability): hardware/software vulnerability exploitation, system disruption

  — threat (integrity): vulnerability exploitation, compromised hardware/software/system

  — threat (confidentiality): vulnerability exploitation, compromised hardware/software/system

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety.

— Summary of threats and their potential harmful impacts on safety

  — threat (availability): disruption of production systems

  — threat (integrity): vulnerability exploit, compromised hardware/software/system of production systems

— threat (confidentiality): vulnerability exploit, compromised hardware/software/system of production systems

*NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Application of bow-tie analysis to this example

Two coordinated bow-tie analyses of different risk dimensions are combined, as the ultimate interest lies only in the aviation safety consequence.

Information security bow-tie analysis element	Aviation safety bow-tie analysis element
Information security threats 1) hardware/software vulnerability exploitation: disturbed system function 2) hardware/software vulnerability exploitation: system integrity compromised 3) hardware/software vulnerability exploitation: confidentiality of information processed by system(s) compromised	
Information security preventive barriers	
Information security hazards & top events 1) disturbed system functionality (hazard) → disrupted/unreliable system functionality 2) system integrity compromised (hazard) → system function unpredictable 3) information disclosable (hazard) → undetectable information exfiltration	**Safety threats** 1) disrupted/unreliable system functionality 2) system function unpredictable 3) undetectable information exfiltration
Information security mitigative barriers	**Safety preventive barriers** 1) Use of access controls for system administration 2) etc.
Information security consequences	**Safety hazards & top events**:

1) loss of system function (= production system down) 2) loss of system function integrity (= some system function wrong/inoperative) 3) loss of confidentiality of information (= some information can leak)	1) loss of system function (hazard) →*in operational maintenance system* 2) loss of system function integrity (hazard) → *systems operate with wrong information* 3) loss of information confidentiality (hazard) → *confidential maintenance information leaks*
	Safety mitigative barriers 1) use of back-up procedures to prevent faulty maintenance actions 2) etc.
	Safety consequences 1) faulty maintenance actions 2) incorrectly completed maintenance actions 3) exfiltration of information allows for identification of vulnerabilities

Example 4: Design and production organisations' software, supply chain, design and manufacturing ground infrastructure

— Threat vector assets/domain

  — Design and production organisations' supply chain for parts, hardware and software

  — Design and production organisations' ground internal infrastructure used to manage software/hardware used in the manufacturing and development of products that will be used by aircraft manufacturers, operators or ATM/ANS ground automation systems (hardware/software) information technology assets

  — Design and production organisations' information technology assets used by their customers to updated systems on an aircraft (software/hardware) used for maintenance operations or ATM/ANS ground automation systems

  *NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Non-exhaustive summary of potential threats

  — threat (availability): systems used to store, transmit and exchange information are rendered unavailable for essential operations through denial of service attacks.

  — threat (integrity): systems used to store, transmit and exchange information are compromised through man-in-the middle attacks.

  — threat (confidentiality): systems used to store, transmit and exchange information are accessed by insider or external threats.

  *NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Summary of threats and their potential harmful impacts on safety

— Disruption of systems used to store, transmit and exchange information in a manner that would prevent the proper management of the aircraft and its systems and adversely affect the operations of the aircraft

— Systems used to store, transmit and exchange information can no longer be considered trusted. If they are not maintained at a level to ensure that all information exchange, data and software can be considered trusted, both ground and aircraft operations are disrupted.

— Uncontrolled access to systems used to store, transmit and exchange information (including information that is received and exchanged with the supply chain) can provide technical details that could be used to craft more sophisticated attacks targeting safety-critical systems.

*NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

Example 5: Training system

— Threat vector assets/domain

— Supply chain of all software and hardware that will be used in the training systems or training devices (including flight simulators) used to train pilot or ATM/ANS ground systems personnel.

— Internal infrastructure used in of all software and hardware that will be used in the design, manufacturing or production of products (hardware or software) that will be used in aircraft or ATM/ANS ground systems.

— Management of internal operating domains and system of all software and hardware that will be used in the design, manufacturing or production of products (hardware or software) that will be used in aircraft or ATM/ANS ground systems.

*NOTE: Organisations must document all threat vectors that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Non-exhaustive summary of potential threats

— threat (availability): training systems or training devices are rendered unavailable by means of denial of service attacks when they are needed to be used.

— threat (integrity): training systems or training devices are compromised through man-in-the middle attacks.

— threat (confidentiality): functional models, information and data that are embedded in training systems or training devices are accessed by insider or external threats.

*NOTE: Organisations must document all threats that have a potential harmful impact on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

— Summary of threats and their potential harmful impacts on safety

— Disruption of training systems (hardware and software) will have an impact on the organisations' ability to maintain qualified staff. It would also prevent the aircraft and its systems from being properly operated and affect maintenance operations for ATM/ANS ground systems.

— The training model or the failure modes and associated emergency conditions differ from the real aviation system behaviour and therefore induce inappropriate responses. If the training systems cannot be trusted, this will affect the ability of organisations to maintain sufficiently qualified staff for their operations (pilots, maintenance or ATM/ANS ground personnel who have been exposed to improper training should be re-qualified).

— Lack of control and access to training systems affects the ability of organisations to maintain a training system that is known to be in a trusted state. In addition, uncontrolled access to training systems that embed functional models, information and data can provide technical details that could be used to craft more sophisticated attacks on the training system itself or on the real-world safety-critical system.

*NOTE: For each threat, organisations must document and define the potential harmful impact of each threat on aviation safety. This includes systems used for any design, manufacturing and production of hardware and software.

Threat and risk mitigation considerations

The organisation being evaluated can only be evaluated for the unique domain they are responsible for management and operation. For each threat vector and threat identified, the organisation must define the methods used to mitigate all risks and threats identified and be prepared to provide supporting evidence and artefacts if requested by the authority. Of special note, the organisation should include in its considerations the following:

— The evaluation of risk comprises any interface where an interconnection between organisations exists and where information is exchanged through external interfaces.

— The sharing of risk assessment information ensures as much as practical for each scenario that any shared risks between directly interconnected parties are identified and mutually mitigated at an acceptable level by the organisation responsible for ensuring that any information security risks with the potential of harmful impacts on safety are effectively managed.

— Access to resources should be controlled and limited to ensure that the services cannot be disrupted and manipulated in any way.

APPENDIX II

Main tasks stemming from the implementation of the Part-IS Regulation, including references to NIST CF 1.1 and ISO/IEC 27001:2013

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Establish and operate an information security management system (ISMS)	Management	IS.D.OR.200(a)	IDENTIFY	ID.RM	4 6.1.1	
Establish the scope of the ISMS according to Part-IS requirements	Management		IDENTIFY		4.3	
Implement and maintain a security policy	Management	IS.D.OR.200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1
Identify and review information security risks	Management	IS.D.OR.200(a)(2) IS.D.OR.205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2	
Implement security risk treatment measures	Management	IS.D.OR.200(a)(3) IS.D.OR.210	PROTECT	PR.PT	6.1.3 8.1 8.3	
Implement measures to detect security events and identify those related to aviation safety	Management	IS.D.OR.200(a)(5) IS.D.OR.215	DETECT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7
Implement measures that have been notified by the competent authority	Operational	IS.D.OR.200(a)(6)			10.1	A6.1.3
Take appropriate remedial actions to address findings notified by the competent authority (non-compliances)	Both	IS.D.OR.200(a)(7)			10.1	A6.1.3
Implement an external information security reporting scheme	Management	IS.D.OR.200(a)(8) IS.D.OR.230	RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	7.4	A6.1.3 A16.1.2 A16.1.3

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Monitor compliance with this Regulation and report findings to top management	Operational	IS.D.OR.200(a)(12)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2
Protect confidentiality of exchanged information	Operational	IS.D.OR.200(a)(13)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.D.OR.200(b) IS.D.OR.260	IDENTIFY	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1
			PROTECT	PR.IP-7 PR.IP-10		
			DETECT	DE.DP-5		
			RESPOND	RS.MI-3 RS.IM-2		
			RECOVER	RC.IM-2		
Document and maintain all key processes, procedures, roles and responsibilities	Management	IS.D.OR.200(c)	IDENTIFY	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1
			PROTECT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12		
			DETECT	DE.DP-1		
			RESPOND	RS.CO-1 RS.AN-5		
Identify all elements which could be exposed to information security risks	Management	IS.D.OR.205(a)	IDENTIFY	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	
Identify the interfaces with other organisations which could result in exposure to information security risks	Management	IS.D.OR.205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3	

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Identify information security risks and assign a risk level	Management	IS.D.OR.205(c)	IDENTIFY	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2	
Review and update the risk assessment based on certain criteria	Operational	IS.D.OR.205(d)	IDENTIFY	ID.RM	8.2	
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.D.OR.210(a)	PROTECT	PR.IP PR.PT	6.1.3 8.3	
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.D.OR.210(b)	IDENTIFY	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1	
			PROTECT	PR.IP-7		
Establish an internal information security reporting scheme to enable the collection and evaluation of information security events from personnel	Management	IS.D.OR.200(a)(4) IS.D.OR.215(a) IS.D.OR.215(e)	IDENTIFY	ID.AM-3	7.4	A16.1.1 A16.1.2
Ensure that contracted organisations report information security events	Management	IS.D.OR.215(c)	RESPOND	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Operational	IS.D.OR.215(b)(1)-(b)(3)	IDENTIFY	ID.RA-1		A12.6.1 A16.1.1 A16.1.4
			DETECT	DE.AE-2 DE.AE-3 DE.AE-5		

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Implement measures to detect in processes and operations security events which may have a potential impact on aviation safety	Operational	IS.D.OR.220(a)	DETECT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5
			PROTECT	PR.PT-1		
Implement measures to respond to security events that may cause a security incident	Operational	IS.D.OR.220(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5
Cooperate on investigations with other organisations that contribute to information security of its own activities	Management	IS.D.OR.215(d)	RESPOND	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7
Implement measures to recover from information security incidents	Operational	IS.D.OR.220(c)	RECOVER	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6
Manage risks associated with contracted activities with regard to the management of information security	Management	IS.D.OR.235	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.D.OR.240(f)	IDENTIFY	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding information security management	Management	IS.D.OR.240(g)	IDENTIFY	ID.AM-5 ID.AM-6	7.2	A7.1.5
			PROTECT	PR.AT-1		
Create and maintain a process to ensure that the personnel acknowledge the responsibilities with the assigned roles and tasks	Management	IS.D.OR.240(h)	IDENTIFY	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Verify identity and trustworthiness of personnel who have access to information systems	Management	IS.D.OR.240(i)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1
Archive, protect and retain records traceability for a specified time	Operational	IS.D.OR.245	IDENTIFY PROTECT	ID.RA-4 PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1	7.5	A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3
Correct non-compliance findings upon notification by the competent authority	Operational	IS.D.OR.225(a) IS.D.OR.225(b)			10.1	A18.1 A18.2
Implement an information security reporting system in accordance with Regulation (EU) No 376/2014	Management	IS.D.OR.230(a)				
Report information security incidents or vulnerabilities to the competent authority and under certain conditions to others	Operational	IS.D.OR.230(b) IS.D.OR.230(c)	DETECT RESPOND RECOVER	DE.DP-3 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RC.CO-3	7.4	A16.1.1 A16.1.2 A16.1.3
Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.D.OR.260(a)			9	A5.1.2 A12.7.1 A16.1.6
Take actions to improve the ISMS if required. Re-assess the implemented measures of the ISMS elements.	Operational	detection strategy IS.D.OR.260(b)			10	A5.1.2
Ensure accessibility of the competent authority to the contracted organisation	Management	IS.D.OR.235(b)			9.3	A6.1.3 A15.1 A15.2
Ensure that all necessary resources are available to comply with the Regulation	Management	IS.D.OR.240(a)(1)	IDENTIFY	ID.AM-5 ID.AM-6	7.1	A6.1.1

Part-IS main task	Activity type	Reference			Reference	
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001:2013	
			Function	Category	Paragraph Clause	Annex A Control
Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Management	IS.D.OR.240(a)(2)&(a)(3)	IDENTIFY	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2
			PROTECT	PR.AT-1 PR.AT-4		
Nominate a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Management	IS.D.OR.240(b) IS.D.OR.240(c) IS.D.OR.240(d)	IDENTIFY	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2
			PROTECT	PR.AT-1 PR.AT-4		
Create and maintain an Information security management manual ISMM	Management	IS.D.OR.250			7.5.1	A6.1.3
Develop a procedure on how to notify the competent authority upon changes to the ISMS	Management	IS.D.OR.255(a)	IDENTIFY	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2
Manage changes to the ISMS and notify the competent authority and/or request for approval of changes	Management	IS.D.OR.255(a) IS.D.OR.255(b)	IDENTIFY	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2

APPENDIX III

Examples of aviation services

The following is a non-exhaustive and not complete list of aviation services that can be used as a basis to identify the scope of risk assessment for the organisation.

Aerodrome ATM- MET services provider
Aeronautical digital map service
AIM (external)
Airport
APP ACC
ATC (external)
ATC superior
ATM
ATM-MET services provider
Civil AU operations centre
Communication infrastructure
ER ACC
FIS/TIS data integrator
National AIM
Navigation infrastructure — ground-based
Navigation infrastructure — satellite-based
Non-ATM MET services provider
Non-aviation users (External)
Regional AIM
Regional ASM
Regional ATFCM
State AU operations centre
Static aeronautical data service
Sub-regional DCB common service provision
Sub-regional/local ATFCM
Sub-regional/national ASM
Surveillance infrastructure airport
Surveillance infrastructure en-route
Surveillance infrastructure TMA
Time reference (external)
Tower (TWR)

Annex III

1. Proposed amendments

The amendment(s) is (are) arranged as follows to show deleted, new, and unchanged:

— deleted text is ~~struck through~~;

— new text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

Where necessary, the rationale is provided in *italics.*

7.1. Draft acceptable means of compliance and guidance material

'AMC and GM to Part-ARA — Issue 1, Amendment 11'

AMC1 ARA.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 ARA.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:

— Traffic Light Protocol (TLP): with whom the received information can be shared.

— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part 21 — Issue 2, Amendment 13'

AMC1 21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.
— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part-ARO — Issue 3, Amendment 13'

The following AMC and GM are inserted:

AMC1 ARO.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 ARO.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.

— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part-ADR.AR — Issue 1, Amendment 7'

The following AMC and GM are inserted:

AMC1 ADR.AR.A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 ADR.AR.A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.

— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part-145 — Issue 2, Amendment 5'

The following AMC and GM are inserted:

AMC1 145.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 145.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.
— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part-CAMO — Issue 1, Amendment 3'

The following AMC and GM are inserted:

AMC1 CAMO.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 CAMO.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.
— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to Part ATCO.AR — Issue 1, Amendment 1'

The following AMC and GM are inserted:

AMC1 ATCO.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 ATCO.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.

— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.

'AMC and GM to ATM/ANS.AR — Issue 1, Amendment 3'

The following AMC and GM are inserted:

AMC1 ATM/ANS.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

The reporting of security-sensitive information should be made by means that ensure the necessary confidentiality and the selection of the appropriate recipient(s). This should be implemented to prevent the content of a report being exploited to the detriment of aviation safety, by revealing, for instance, uncorrected vulnerabilities.

GM1 ATM/ANS.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

When deemed necessary, a two-step mechanism could be used: a report alerting about the occurrence and the availability of information-security-sensitive data. This report should only alert recipients of the urgency and the necessity for organisations and competent authorities to establish further communication through secure means.
Therefore, the report should consist of two parts, one limited to mostly public information and one containing the sensitive data that should be restricted to the recipients who need to know. These parts of the report should be labelled according to an agreed information exchange protocol.
Examples of protocols for the distribution of sensitive information are the following:
— Traffic Light Protocol (TLP): with whom the received information can be shared.

— Permissible Action Protocol (PAP): complementary to TLP — 'what one is allowed to do with the received information'.

Further information about the usage of TLP can be found in the ICAO 'Guidance on Traffic Light Protocol'.

Wherever possible, reports should be based on an agreed taxonomy.