UK Civil Aviation Authority

ISMS Regulation

Acceptable Means of Compliance (AMC)

and

Guidance Material (GM)

Proposed Wording for Consultation

Note from the editor

This document contains acceptable means of compliance and guidance material adopted by the UK CAA. The reference numbers indicate the section or paragraph in the corresponding regulation under consultation which is referred to as *ISMS Regulation*.

All references to other regulations are to the UK law bearing that title or number, being EU retained law as retained (and amended by UK domestic law) pursuant to the European Union (Withdrawal) Act 2018.

Contents

GM1 200 Information security management system (ISMS)

An **information security management system (ISMS)** is a systematic approach to establish, implement, operate, monitor, review, maintain and continuously improve the state of information security of an organisation. Its objective is to protect the information assets, such that the operational and safety objectives of an organisation can be reached in a risk-aware, effective and efficient manner.

Generally speaking, an ISMS establishes an information security risk management process, based upon the results of information security impact analyses, which basically determine its scope. If information security breaches may cause or contribute to aviation safety consequences, information security requirements need to limit their impact on levels of aviation safety, which are deemed acceptable. Hence, all roles, processes, or information systems, which may cause or contribute to aviation safety consequences, are within the scope of the ISMS regulation. The ISMS provides for means to decide on needed information security controls for all architectural layers (governance, business, application, technology, data) and domains (organisational, human, physical, technical). It further allows to manage the selection, implementation, and operation of information security controls. Finally, it allows to manage the governance, risk management and compliance (GRC) within the ISMS scope.

The risk management process is thus based on aviation safety risk assessments and derived information security risk acceptance levels, which are designed to effectively treat and manage information security risks with a potential impact on aviation safety caused by threats exploiting vulnerabilities of information assets in aeronautical systems. Interacting bow-ties allow for a higherlevel and non-exhaustive illustration of how different disciplines of risk assessment may need to collaborate to establish a common risk perspective, as depicted in Figure 1.

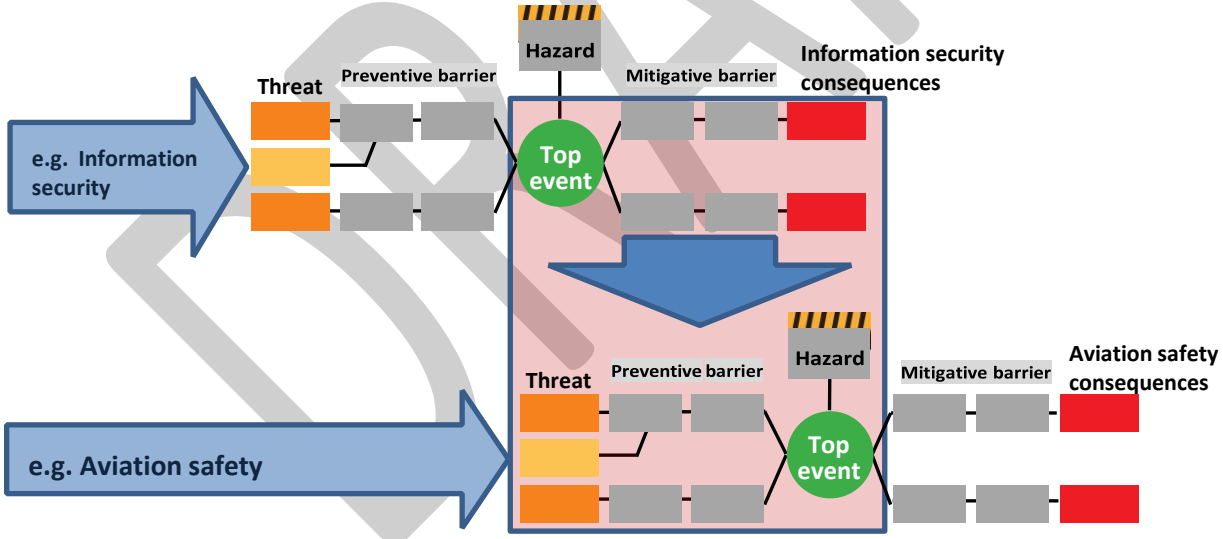

Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

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 defined in this Regulation, employs the perspectives of governance, risk and compliance, and an approach that combines the safety risk and performance dimensions to determine the information security

controls that are appropriate to and compliant with the specific context and can effectively provide the level of protection required to achieve the aviation safety objectives by:

— **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 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 and 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 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.

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

Based on these perspectives, we may identify the following processes or subject areas that have been shown to be relevant for the establishment of an effective ISMS. These ISMS processes and subject areas 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 to achieve a sufficient level of information security awareness and training of all involved 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, record-keeping, 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 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, if the functions do not perform as planned.

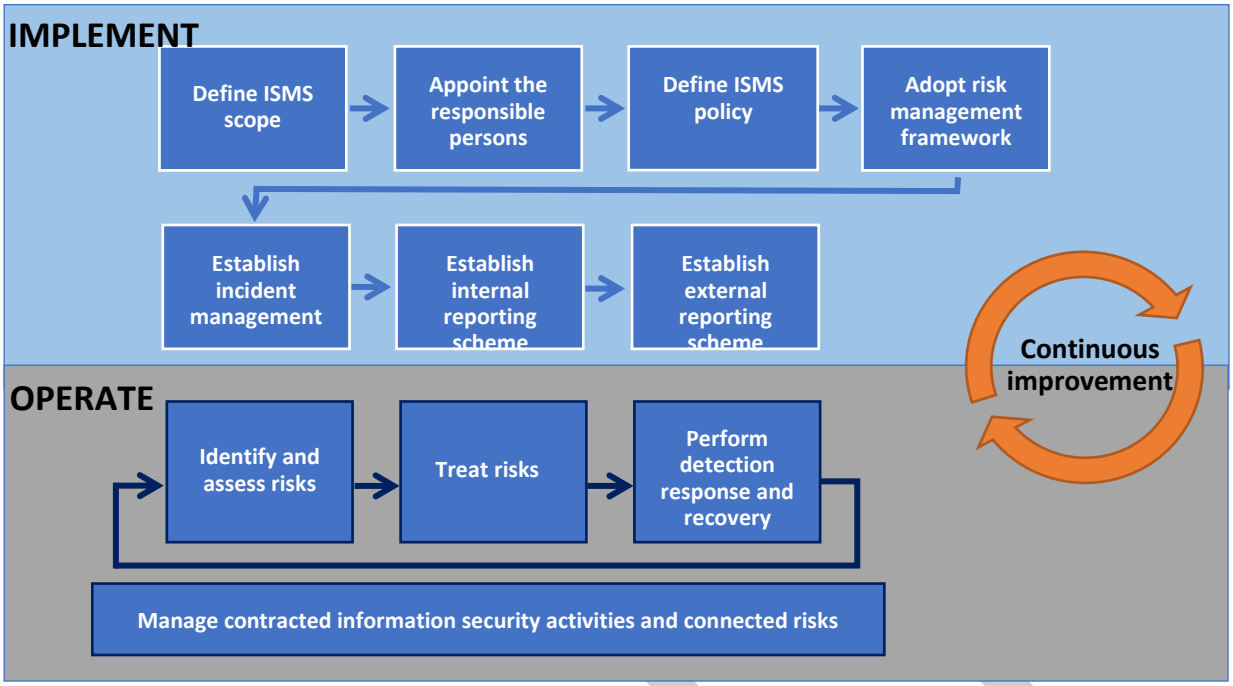

Figure 2: Representation of the requirements from an ISMS's life cycle perspective Plan-Do-Check-Act approach

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.

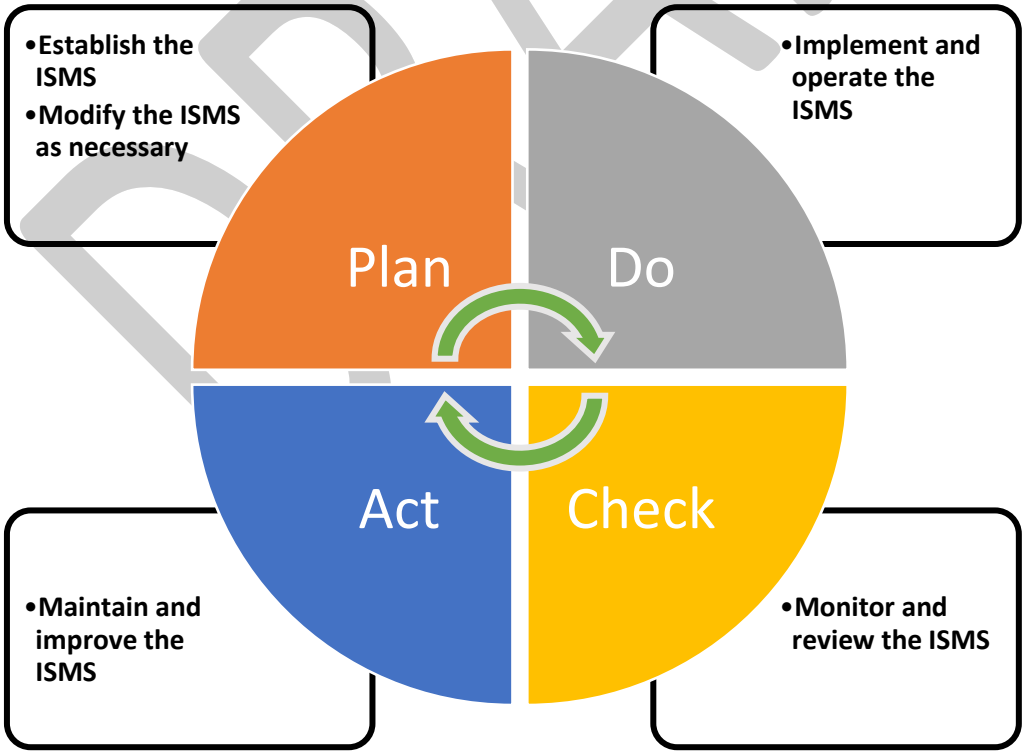

Figure 3: Plan-Do-Check-Act approach applied to an ISMS

Benefits of an ISMS

The benefits of a management system operating in a dynamic, uncertain or unpredictable risk environment are realised in 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 on 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 information security 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 information 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 information security strategy in times of digital transformation, increasing interconnectivity of systems, emerging information security threats and new technologies.

Relation to ISO/IEC 27001

The international standard ISO/IEC 27001 is a widely adopted standard for ISMS which specifies generic requirements for establishing, implementing, maintaining and continually improving an ISMS. It also includes requirements for the assessment and treatment of information security risks. The requirements are applicable to all entities, regardless of type, size or nature. The conformity of an ISMS with the ISO/IEC 27001 standard can be certified by an accredited certification body. ISO/IEC 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.

ISO/IEC 27001 allows entities to define their own scope of audit and their own organisational risk appetite. This, in turn, leads to information security requirements that provide the ISMS with criteria for the acceptability of information security risks in line with the entity's risk appetite (see Figure4).

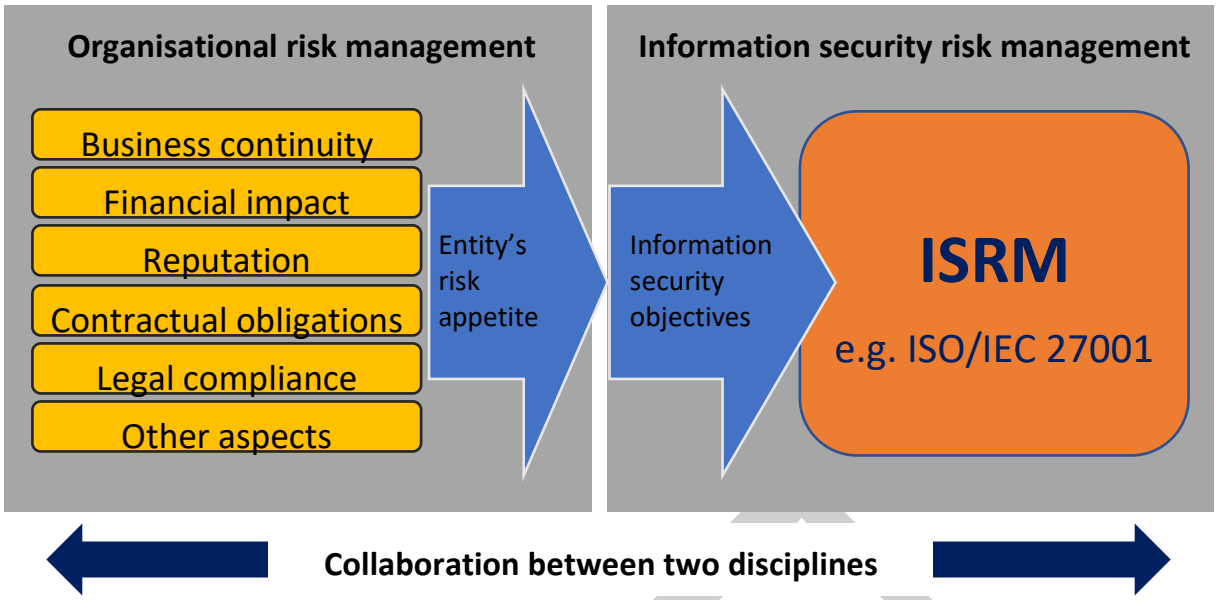

Figure 4: Relation between the entity's risk appetite and the information security objectives

The requirements for an ISMS specified by this Regulation are in most parts consistent and aligned with ISO/IEC 27001; however, this Regulation introduces provisions specific to the context of aviation safety. If an ISO/IEC 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. In order to take credit from ISO/IEC 27001 certifications to achieve compliance with the ISMS regulation, aviation safety needs to be included in the organisational risk management, with the relevant risk acceptance level determined by the applicable regulation (see Figure 5). Therefore, careful determination of the scope of the ISMS related to aviation safety risks is needed, as it might differ from the one related to the other organisational risks. To allow demonstration of compliance with the ISMS regulation, careful delineation between aspects of the ISMS related to aviation safety risks and other organisational risks may be required. This could have an influence upon the decision to integrate ISMSs.

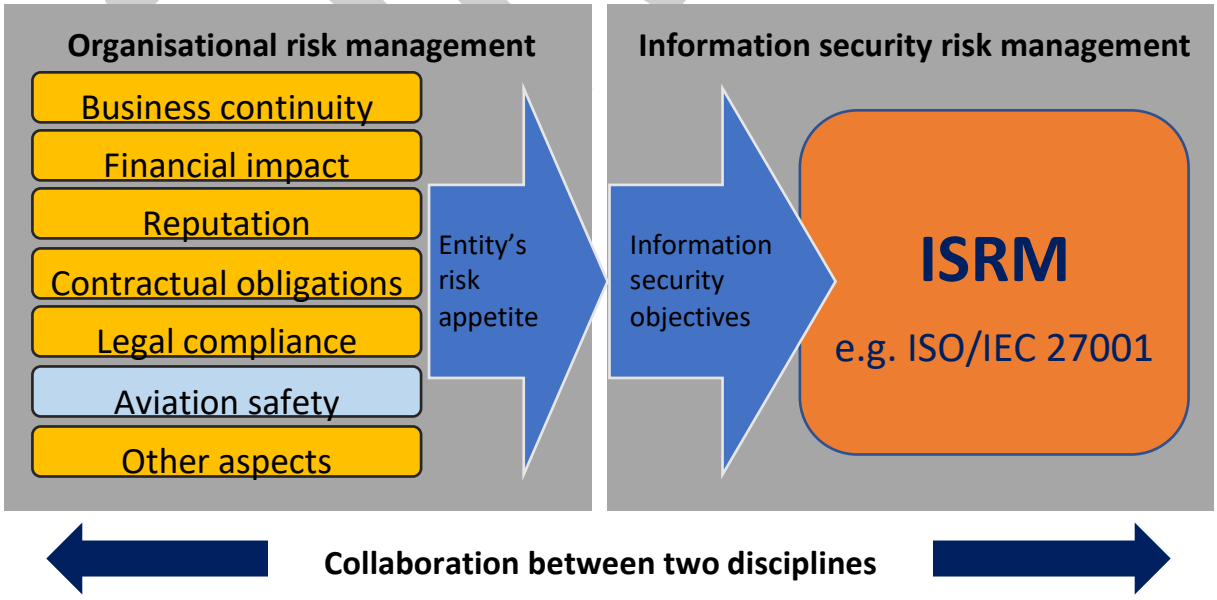

Figure 5: Introduction of aviation safety aspects in the entity's risk appetite

ISMS Regulation versus ISO/IEC 27001 cross reference table

For a mapping between the main tasks required under the ISMS regulation and the clauses and associated controls in ISO/IEC 27001, refer to Appendix II.

AMC1 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 be endorsed by the accountable manager and reviewed at planned intervals or if significant changes occur. Moreover, the policy should cover at least the following aspects with a potential impact on aviation safety by:

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

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

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

(d) committing to apply ISMS requirements into the processes of the organisation;

(e) committing to continually improve towards higher levels of information security process maturity as per 260;

(f) 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;

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

(h) committing to promote the information security policy through training or awareness sessions within the organisation to all personnel on a regular basis or upon modifications;

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

(j) committing to communicate the information security policy to all relevant parties, as appropriate.

Note: A significant change is a notable alteration or modification that has a meaningful impact on the organisation's operations, such as a structural change within the organisation due to reorganisations, a change in the business processes (e.g. working from home, use of personal devices), a technological evolution (e.g. distributed computing resources, artificial intelligence/machine learning) or an evolution in the threat landscape.

GM1 200(a)(1) Information security management system (ISMS)

INFORMATION SECURITY POLICY AND OBJECTIVES

The information security policy should suit the organisation's purpose and direct its own information security activities. Such policy should contain the needs for information security in the organisation's context, a high-level statement of direction and intent of the information security activities, the principles and most

important strategic and tactical objectives to be achieved by the ISMS, as well as the general information security objectives or a specification of a framework (who, how) for setting information security objectives. The information security policy should also contain a description of the established ISMS, including roles, responsibilities and references to topic-specific policies and standards.

The information security objectives should be:

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

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

— measurable if practicable (to be able to determine whether the objective has been met), aimed to be SMART (specific, measurable, attainable, realistic, timely) and aligned with all affected responsible persons.

When defining information security objectives, e.g., based on the overarching organisation's objectives, the information security requirements or the results of risk assessments, it should be determined how these objectives will be achieved. The degree to which information security objectives are achieved must be measurable. If possible, it should be measured by key performance indicators (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 information security objectives which are relevant for the organisation, more of a long-term nature and measurable with a reasonable effort relative to the delivered benefits.

AMC1 200(a)(12) Information security management system (ISMS)

COMPLIANCE MONITORING

When establishing compliance with the provisions under point 200(a)(12), the organisation should 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 mechanism of audit findings to the accountable manager or delegated person(s) to ensure implementation of corrective actions as necessary.

GM1 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 information security 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 approach and a decision-making process based on evidence. Moreover, when setting up an audit programme, the importance of the processes concerned, and definitions of the audit criteria and scope should be considered. Documented information should be retained evidencing the audit results, their reporting to the relevant management and the audit programme.

AMC1 200(a)(13) Information security management system (ISMS)

When establishing compliance with the provisions under points 200(a)(13), the organisation should implement and maintain information security controls that are sufficiently robust and effective to protect information and ensure the need-to-know principle (i.e. limiting access to information to only those who need it to perform their duties). It should protect the source of information in accordance with the relevant provisions established in UK Regulation (EU) 2018/1139. It should also comply with UK Regulation (EU) No 376/2014.

AMC1 200(c) Information security management system (ISMS)

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

(a) provide an outline of the structure of the specific information security personnel (internal and external), including their roles and responsibilities. This outline of the structure will be used to manage and maintain the elements included within the scope of the ISMS and will be approved by the accountable manager. The organisation should review the outline of the structure at planned intervals or if significant changes occur (see the Note in AMC1 200(a)(1));

(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 of this Regulation 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 of this Regulation;

(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 the documented information required by the ISMS to ensure that it is:

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

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

GM1 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 200(a), the recordkeeping requirements referred to in

245 and the information security management manual requirements referred to in 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 — see 200(a)(1);

(b) responsibilities and accountabilities for roles relevant to information security — see 250(a)(2), (3), (6) and (7) and the personnel requirements referred to in points 240(a), (b), (c), (d) and (f) and the related AMC and GM;

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

(d) information security risk management process — see the information security requirements referred to in points 205 and 210;

(e) archive of the risks identified in the information security risk assessment along with the associated risk treatment measures (often referred to as 'risk register' or 'risk ledger') — see 245;

(f) evidence of the competencies necessary for the personnel performing the activities required under this Regulation — see 240(g) and the related AMC and GM;

(g) evidence of the current competencies of the personnel performing the activities required under this Regulation — see 245(b)(1);

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

GM1 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 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.

SUPPORTED IMPLEMENTATION OF THE ISMS

In the context of the ISMS regulation, all organisations initiate the implementation of an ISMS with determining its scope, which in turn is based upon at least an assessment of aviation safety impacts for which information security incidents are a cause or a contributing factor. Organisations, irrespective of their size, may not have yet sufficient knowledge about their information security risks, and may consider seeking support by a service provider that can also provide additional personnel and expertise during this implementation phase of the ISMS. The same may apply to later phases of the ISMS implementation, and to this end organisations may want to consider the provision of 235 and related AMC. Outsourcing specific ISMS functions, such as information security monitoring or incident response to service providers, may help ensure that the organisation has access to experienced personnel and expertise. Similarly, organisations may want to be supported by a service provider in performing risk assessments.

Regarding the establishment of the appropriate personnel to implement and comply with the provisions of this Regulation, organisations should always refer to AMC1 240(f) and GM1 240(f), by considering that

multiple responsibilities may be assigned to one person, while always ensuring the independence of the compliance monitoring.

As an introduction to the nature of information security risks and their management, organisations may use, as initial guidance, the NIST Interagency Report (NISTIR 7621 Rev.1) '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 the ISMS with other management systems: an organisation may align the ISMS with other management systems, such as safety management systems (SMSs), 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 information security risks potentially leading to aviation safety risks.

— Reuse existing controls: an organisation may reuse existing controls, such as access controls or incident management process, to implement the information 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 200(e) Information security management system (ISMS)

DEROGATION

Organisations should follow the directions provided in AMC1 205(a) and AMC1 205(b) to perform a documented information security risk assessment to seek the approval by the CAA of a derogation under point 200(e). In order to justify the grounds for a derogation, the risk assessment is expected to provide explanations for the exclusion of all elements from the scope of the ISMS. It is up to the CAA to determine whether this assessment is deemed satisfactory for a derogation to be granted.

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

GM1 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 a derogation by the CAA following the procedure outlined in AMC1 200(e).

Some examples of organisations that may consider asking for a derogation might include:

— An air operator that performs non-high-risk commercial specialised operations (SPO) with noncomplex aircraft, if the nature of the operations justifies the grounds for a derogation.

— An air operator that operates ELA2 aircraft as defined in Article 1(2)(j) of UK Regulation (EU) No 748/2012 with the exception of one aircraft that is operated in predefined operational conditions or under certain operational limitations.

— A maintenance organisation approved under Part-145 dealing only with maintenance of components or maintenance activities that do not contribute to ensuring the structural integrity of the aircraft nor any major safety-related functionalities — for instance, undertaking activities such as washing, removing coatings, painting, 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 elements of an organisation from the scope of the ISMS.

GM1 205 Information security risk assessment

The ISMS regulation does not require the use of any specific information security framework, such as ISO, NIST or others to develop the risk assessment or in general to implement risk management. 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 need to consider aviation safety aspects.

Organisations whose information 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 (see GM1 200).

General guidance on risk management, including risk assessment, can be found in ISO/IEC 27005 and ISO/IEC 31000 as well as NIST SP 800-30. Aviation organisations may also wish to consider aviation specific guidance as defined in the risk management chapter of the latest version of EUROCAE ED201A and, as appropriate to the specific operating environment, in the chapters of EUROCAE ED-204A, EUROCAE ED-205A and EUROCAE ED-206 covering risk management.

AMC1 205(a) Information security risk assessment

When conducting an information security risk assessment, the organisation should ensure that all relevant aviation safety elements are identified and included in the ISMS scope as per 200 and related AMC.

A means to comply with the requirement in point 205(a) is to perform a preliminary high-level risk assessment or impact assessment, carried out in accordance with a documented methodology and following precise criteria for the inclusion in and exclusion from the ISMS scope of the elements listed in 205(a).

GM1 205(a) Information security risk assessment

SCOPE AND BOUNDARIES IDENTIFICATION

The organisation should develop clear and comprehensive understanding of its aviation activities and services, the related processes and associated information systems, and the relevant data flows and information exchanges that define the scope of the ISMS and the boundaries for risk assessment. Therefore,

the organisation should develop corresponding documentation on resources and dependencies related to computing, networking 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 may be considered for the identification of the aforementioned scope and boundaries. The level of detail of the analysis can be an iterative process, with the effort commensurate with the expected level of risk. As stated above, the purpose is to establish understanding of all relevant assets, resources and dependencies that are directly a part of the functions, services and capabilities through the following activities:

(a) Identification of operational inputs and outputs relevant to the functions, services and capabilities of the organisation; these can be related to:

— internal or external sources;

— internal or external leased or managed services, or other dependencies;

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

(c) Identification of the operating environments (e.g. office, public access area, access-controlled room, etc.) and locations for all relevant assets;

(d) For each asset included in the scope, identification of the specific methods, processes and resources that will be used to manage, operate and maintain each asset throughout its life cycle, including:

— internal or contracted resources;

— contracted companies remotely managing the assets (i.e. provider of managed services).

AMC1 205(b) Information security risk assessment

The organisation should, as part of the information security risk assessment, identify the interfaces it has with other parties such as service providers, supply chains and other third parties, based on the exchange of data and information and the assets used for that exchange, which could lead to a situation where information security risks, as a result of mutual exposure, may either:

— increase aviation safety risks faced by other parties; and/or —

increase aviation safety risks faced by the organisation.

GM1 205(b) Information security risk assessment

RISK INFORMATION SHARING

Interfacing organisations should share information with each other about the potential exposure to information security risks by following, for instance, the approach detailed in EUROCAE ED-201A, Appendix B — B.1, B.2 and B.3. The purpose of this exchange of information is to enable organisations to establish a matching mapping for the services identified under 205(a), including all information and data flows, 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 (i.e. hardware, software, network and computing resources) that will be used in the exchange;

(c) identify all functions, activities and processes, including their respective information and data, which will be created, transmitted, processed, 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.

TWO CATEGORIES OF INTERFACING ORGANISATIONS

There are two categories of interfacing organisations: those that are also subject to the ISMS regulation, and those that are not.

Where the organisation has interfaces with an organisation that is subject to the ISMS regulation, each entity:

— is responsible for the identification of the interfaces that its own organisation has with other organisations, and which could result in the mutual exposure to information security risks. The entity may benefit from the sharing of risk information as this exchange allows for a more accurate assessment of those risks;

— remains accountable for the proper management of the information security risks within the scope of its own ISMS.

In all other cases (including those where the organisation has interfaces with an organisation that is subject to EU implementing regulation 2023/203 or EU delegated regulation 2022/1645) the organisation is accountable for the proper management of the information security risks that may arise from its exposure to the interfacing entity. Where these risks need to be treated, the organisation always has the option of implementing mitigating measures and controls within its own boundaries. In the specific case where the interfacing entity is a supplier, the organisation may decide to manage the risks through contractual arrangements and require the supplier to implement mitigating measures and controls within its own organisation.

GM2 205(b) Information security risk assessment

EXAMPLES OF AVIATION SERVICES

Examples of aviation services that may be considered when determining the ISMS scope and interfaces are provided in Appendix III.

AMC1 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 assessment of risks which have a potential impact on aviation safety including the level of risks. The organisation should associate each risk with the relevant elements and interfaces identified under 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 carried out 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 results for similar inputs;

(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 valid, in particular:

  (1) the information that allows the determination of the safety consequences;

  (2) the information that allows the determination of the potential of occurrence of the threat scenario;

(d) iterative refinement over time allowing for more fine-grained threat scenarios as inputs to become available, with the aim of reducing uncertainty regarding threats, vulnerabilities, effectiveness of existing controls, and dependencies on external entities, in particular by:

  (1) refining initial high-level threat scenarios with greater detail and specificity as more data is gathered;

  (2) refining data on known vulnerabilities by continuously updating information about their exploitability and the associated consequences;

  (3) reviewing the effectiveness of existing controls, and consider newly available controls;

  (4) refining the understanding of the dependencies on external entities and their implications for the organisation's risk profile.

GM1 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, organisation-specific classification levels with an accurate qualitative or quantitative definition in terms of a range or interval of numerical values in order to enable a sufficiently calibrated, consistent estimation, evaluation and communication within the organisation or with the interfacing entities. 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.

Note 1: The phrase 'duration of the observation' refers to the time period during which a threat scenario is observed or monitored. It is essential in determining the likelihood of the threat scenario occurring, since the probability of occurrence may vary depending on the length of the observation period.

Note 2: EUROCAE ED-202A and EUROCAE ED-203A were originally developed for aircraft information security risk assessment, but the generic principles developed in those documents can be adapted to other frameworks when deemed useful by the organisation.

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 may 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 reported or detected vulnerabilities in a fast, risk-prioritised manner with high assurance in order to reduce the attack surface

— Reduction of the severity of a successful attack (i.e. through a redundant system that can maintain the continuity of service in case of a denial of service of a system critical for aviation safety)

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 computer emergency response teams (CERTs) / computer security incident response teams (CSIRTs), information sharing and analysis centres (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 unsafe condition where an unsafe condition 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 either 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.

Examples for high, moderate, and low severity can be found in EUROCAE ED-201A, Appendix B for products, ATM systems and airspace.

If the organisation cannot determine the safety effect, the assessment should identify assumptions from the risk-sharing information at interfaces with other organisations along the functional chain, leading up to the safety effect.

Some of those assumptions can be granted with the certification of products: where assets are subject to product certification from other aviation regulations addressing product information security, the organisation performing the risk assessment may consider the perimeter of the product certification as already covered. This should be acceptable under the condition that this certification is valid and that the instructions provided by the OEM to maintain the certification validity are implemented by the organisation.

Additional information can also be found in Regulation (EU) 2015/1018 on mandatory reporting of occurrences in civil aviation. Further examples of impact severity classifications 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 allowing also for the accountable manager or delegated person(s) 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. The risk management should consider the variability and consistency of threat likelihood, vulnerability, existing controls, external dependencies and safety impact. This is typically achieved when the organisation reaches a higher level of maturity that is representative of functionality and repeatability of information security risk management — see GM1 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: Example of a risk acceptance matrix for comparison purposes

* The potential of occurrence of the threat scenario is reassessed in a timely manner (refer to 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 delegated person(s) who may impose additional conditions for the risk retention, including risk treatment measure and the timeline for its implementation;

— 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: As detailed in NIST SP-800 Rev.1, repeatability refers to the ability to repeat the assessment in the future, in a manner that is consistent with and hence comparable to prior assessments — enabling the organisation to identify trends. Therefore, a risk assessment process can be classified as 'repeatable' when under similar conditions an entity or a person delivers consistent results.

As detailed in NIST SP-800 Rev.1, reproducibility refers to the ability of different experts to produce the same results from the same data. Therefore, a risk assessment process can be classified as 'reproducible' when another entity or person, given the same inputs, assumptions, information security context and threat environment can replicate the same steps and reach the same conclusions.

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 information 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 EUROCAE 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 information security and safety aspects should be coordinated throughout the process to ensure mutual understanding of the threat preventive measures and mitigating measures 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.

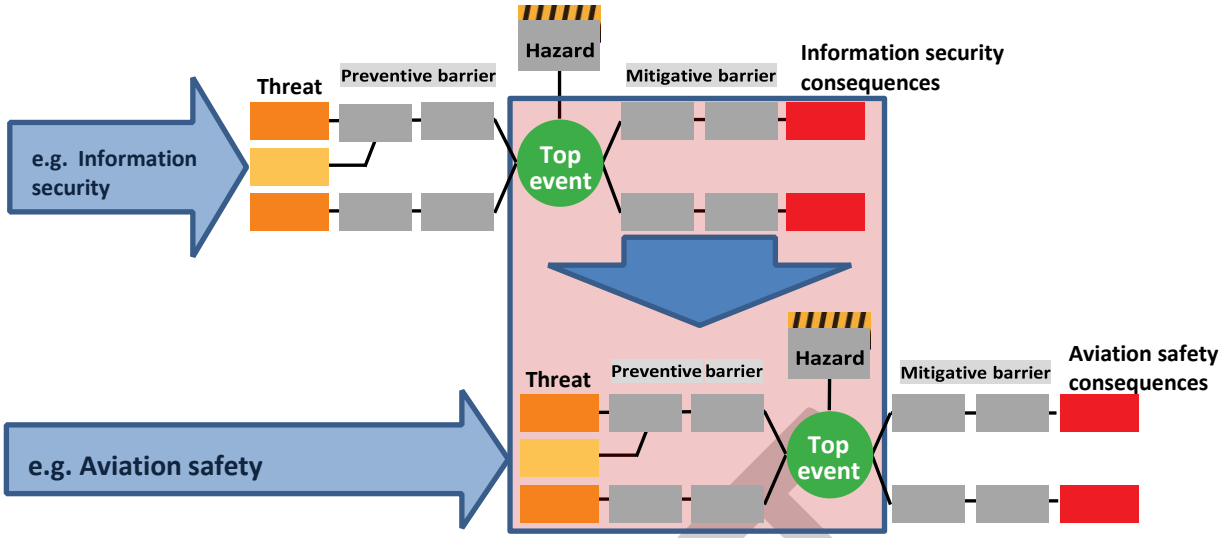

Figure 2: Interactions between information security and aviation safety risk management areas

Note: A preventive barrier or measure is a proactive action or control implemented to reduce the likelihood of a risk, hazard, or threat materialising, while a mitigating measure is an action or control designed to reduce the severity or impact of an undesired event, would it occur.

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 3-7 and 3-8 for the threat catalogues examples and other threat catalogue examples. 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 205(d) Information security risk assessment

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

(a) The risk assessment performed under points 205 (a), (b) and (c) should be reviewed at regular intervals to identify and account for relevant changes. The periodicity at which potential changes have to be evaluated should be determined by the organisation performing the assessment considering the criticality of the assets within the scope of the risk assessment, levels of residual risk of the assets within the scope of the risk assessment and any contractual 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 205(d) Information security risk assessment

The criteria to consider for the frequency of the risk assessment review may be the risk level as well as the criticality and complexity of the assets concerned. The objective of a risk assessment review is to trigger the revaluation of risks, their likelihood and impact in case of relevant changes. One possible way is to have a tiered approach to risk assessment, with a higher-level risk assessment being used for the identification of changes. The higher-level risk assessment could allow the identification of the detailed risks that should be reviewed in a next step. 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 mitigating measures in both their design and operation;

(c) review plans and actions for risk treatment;

(d) identify any organisational change which may require a review of the priorities as well as of the treatment of risks;

(e) maintain an overview of the complete risk picture; and (f) identify any emerging risks.

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

The periodicity of risk assessment reviews should also be documented by the organisation in information 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 in EUROCAE ED-205A, Chapter 3.2 (for ATMS/ANS).

GM2 205(d) Information security risk assessment

The following are examples of changes that should be identified during the risk assessment review as they may trigger an update of the risk assessments:

(a) there is a change in the elements subject to information security risks as identified in 205(a); a change in the elements will include:

— additions to, or removals from, the scope of the risk assessment of individual elements;

— changes to design or configuration of elements within the scope of the risk assessment 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;

(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 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 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 100 and therefore are not subject to the same requirements. Where this is the case, these organisations should be informed of their responsibility to report such changes as listed above through contractual arrangements 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 why and how incidents have occurred; and

— reviewing all types of incidents including those due to external factors, technical reasons, human errors (inadvertent behaviour). For human intentional acts, a distinction can be made between malign and benign actions.

AMC1 205(e) Information security risk assessment

SAFETY SUPPORT ASSESSMENT

Non-ATS providers should conduct a safety support assessment as it is described in UK 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 non-ATS provider should share with the ATS provider, in an appropriate form, information on the residual risk and the impact on the services it provides to that ATS provider .

The residual risk should be used to assess the potential impact on services and products that a nonATS provider offers to an ATS provider.

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 205(e) Information security risk assessment

SAFETY SUPPORT ASSESSMENT

Table 1 below shows the non-ATS providers which shall comply with Subpart C of Annex III to UK 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.

Table 1: Non-ATS providers which shall comply with Subpart C of Annex III to UK Regulation (EU) 2017/373

	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)
	Subpart A	Subpart B	Subpart C	Subpart D									
Air traffic services providers	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

GM1 210 Information security risk treatment

Unacceptable risks identified in accordance with point 205 require a risk treatment process that may lead to the introduction of information security measures, often referred to as information security controls.

For each identified risk, the organisation should define the specific risk treatment measures, 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 should be communicated to and accepted by the accountable manager of the 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, for risks that may lead to an unsafe condition. The updated risk treatment should be communicated to the CAA 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 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 CAA 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 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 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 235 and related AMC).

AMC1 210(a) Information security risk treatment

(a) The risk treatment process should reach at least one of the objectives listed under 210(a).

(b) When establishing compliance with the objectives under points 210(a)(1) and 210(a)(2), the organisation should take into account that:

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

(2) life cycle considerations should be identified and associated to ensure continuous effectiveness of the information security measures including exchange of data with other entities;

(3) it should review and update the risk assessment, according to 205(d), to evaluate whether the measures developed under these points introduce new unacceptable risks

or modify existing risks in a way that they become unacceptable.

(c) Risk treatment should be documented and recorded, for example, in a risk registry, even if the risk has been avoided.

AMC1 215(a)&(b) Information security internal reporting scheme

Organisations should use as a source the incidents detected during activities performed to show compliance with 220(a). Organisations should have a mechanism to collect notifications of events by personnel and by sources outside the company including suppliers, partners, customers, open-source software, and information 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 reportable and if so, what potential or actual impact on aviation safety has occurred. Information security events should be considered in

combination with other events to provide correlation to identify incidents or vulnerabilities with a potential impact on aviation safety.

The organisation should consider the outcome of the risk assessment and the exploitability of new vulnerabilities discovered during the detection activities conducted according to the measures required in 220(a).

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 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. Both internal and external reporting are necessary for a complete and effective reporting system. Internal reports should be assessed in a timely manner and where the potential impact on safety is an unsafe condition, organisations should initiate reporting of these internal reports according to 230.

GM2 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 information security operations in a security operations centre (SOC) and make use of an information 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 a joint SOC to review and act on these events. Organisations may choose to use a SOC for events relevant to the ISMS regulation in isolation or in combination with events not subject to the ISMS regulation but of interest to the organisation, such as events relating to business interests. Events can be automatically aggregated, correlated and analysed in order to detect abnormal behaviour leading to information security incidents.

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 collection and evaluation capabilities as well as detection and response times.

GM3 215(a)&(b) Information security internal reporting scheme

RELEVANT INFORMATION FOR INCIDENTS AND VULNERABILITIES

Understanding the causes of, and contributing factors to, information security incidents and vulnerabilities relevant to the ISMS regulation 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 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, Chapter 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 information 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 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 information security events.

GM1 215(d) Information security internal reporting scheme

The cooperation under point 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. Organisations may consider developing formal agreements (e.g. a memorandum of understanding) outlining roles and responsibilities for information security collaboration such as governance meetings, joint development activities, and real-time indicators of compromise (IoC) sharing.

Moreover, commitment to cooperate may also be achieved through the active participation of the organisation in information security sharing initiatives; for instance, ISAC(s). Additionally, for their own awareness, organisations may also subscribe to receive vulnerability and threat alerts, like those distributed by CERTs.

GM1 220 Information security incidents — detection, response and recovery

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 220(a) include vulnerability discovery; —

response activities under 220(b) include vulnerability management.

AMC1 220(a) Information security incidents — detection, response and recovery

DETECTION

When complying with the requirement in 220(a), the organisation should define and implement a strategy to detect information security incidents which may have a potential 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 205;

(b) identify, as a minimum, those assets that, if compromised, contribute to the scenario(s) that may materialise in an unsafe condition. For this identification of the assets, the measures introduced under 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 also 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 a functional chain and it is compromised, the effect should propagate and may be delayed.

GM1 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 the:

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

(b) expected information security baseline: engage in the identification of deviations from the expected information security operation of information 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 found in EUROCAE ED-206, Chapter 4.

AMC1 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 220(b) relative to incidents:

(1) Preparation of procedures and delineation of roles and responsibilities to respond in a timely, effective and orderly manner to any relevant information security incidents.

(2) The response procedure should:

(i) consider the warnings, unitary or combined, from 220(a)(2), and in collaboration with appropriate personnel assess their potential impact on aviation safety;

(ii) establish, in accordance with 220(b)(2), a containment strategy for each asset category considering the potential worst-case effect and the mission constraints, and provide criteria indicating when the incident is contained;

(iii) define, in accordance with 220(b)(3), the acceptable impact on safety and information 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 220(b) should be based on the response procedure referred to in the point (a)(2) and they should, in particular, consider the following:

(i) the maximum acceptable safety level degradation of the assets within the scope of incident;

(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).

(5) The response time and the measures should take into account the potential immediate negative impact on safety if the measure is taken before it has been fully verified that it would not cause additional immediate safety impacts.

(b) VULNERABILITIES

The organisation should take into account the following aspects when establishing compliance with the objectives contained in point 220(b) relative to vulnerabilities:

(1) Establishment of a vulnerability management strategy defining procedures, roles and responsibilities to respond in a timely, effective and orderly manner to any detected relevant vulnerabilities.

(2) The response measures implemented under point 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 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.

The term 'warning' as used in IS.220 should be understood as an alert that would require timely awareness and response from the information security events management team.

In the context of information security response, 'deception' refers to a range of techniques that aim to mislead potential attackers or malicious users, thereby protecting the system and its data. Deception techniques, such as honeypots or breadcrumb trails, are designed to confuse, slow down or divert attackers, increasing their cost and risk while providing defenders with valuable time and intelligence.

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.

AMC1 220(c) Information security incidents — detection, response and recovery

When complying with the requirement in 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, 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 220(b)&(c) Information security incidents — detection, response and recovery

RECOVERY OBJECTIVES AND TIMING

Point 220(b) addresses event conditions which may develop or have developed into information security incidents, that may have a potential impact on aviation safety, and require 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 level of operations drops, 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 an information security incident occurs. In this scenario, the safety level is first reduced by the incident and then it degrades as long as the time passes. The figure also shows the expected effect that mitigating measures 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.

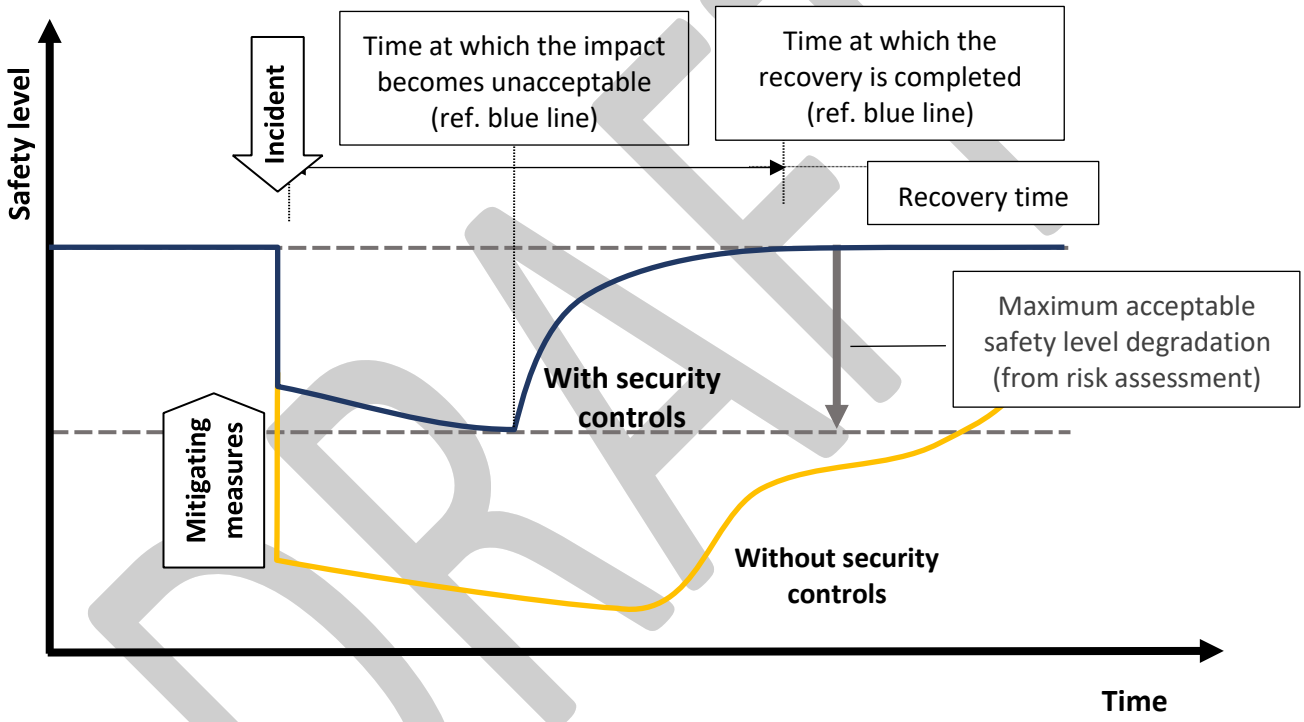

Figure 1: Conceptual framework for the definition of the response and recovery objectives

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, which is depicted in Figure 3.

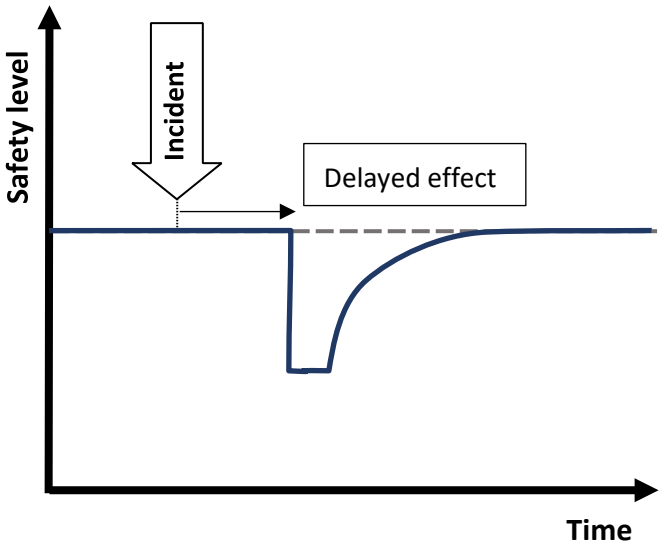

Figure 2: Incident with a delayed effect on safety

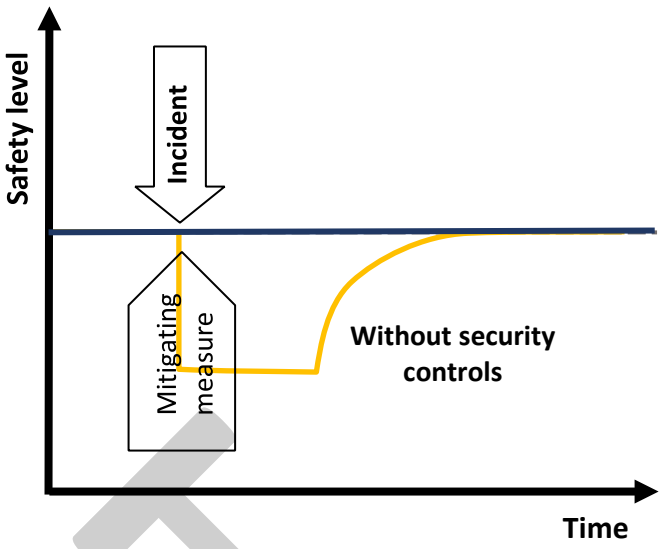

Figure 3: Incident with a fully mitigated effect on safety

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 referred to in AMC1 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 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 the recovery actions in a timely manner after an incident has occurred. Those resources may be internally available or provided by contracted organisations as provided for in 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 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 here 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 information 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 CAA is usually required.

AMC1 225 Response to findings notified by the CAA

The compliance with 225 should be managed as required for each organisation in the corresponding implementing regulation for the domain as identified in 100 concerning the response to findings notified by the CAA. The domain regulation may require the organisation to respond to the findings in accordance with their categorisation.

GM1 225 Response to findings notified by the CAA

The requirement for the categorisation of findings and the period within which the actions in 225(a) should be performed can be found in the corresponding implementing regulation for the domain, under the CAA requirements. For the opening of findings related to this Regulation, the CAA will follow the above-mentioned requirement.

GM1 230 Information security external reporting scheme

Organisations are required to report occurrences to the CAA.

EXAMPLES

Design organisations that are operating in the UK, but were previously approved by EASA, would now consider CAA as the competent authority for reporting requirements.

SPECIAL CASES

In a situation where an organisation has two air operator certificates (AOCs), one of which is in the UK, then that organisation must report occurrences to the CAA in addition to the EU state in which the other certificate is held, assuming that the issue affects the aircraft in both jurisdictions.

For design organisations holding multiple approvals, the reporting will be sent to the CAA as well as to the competent authority in the EU state in which the incident has occurred, or the vulnerability has been discovered.

For organisations holding an approval but operating outside the UK (e.g. Part-145), CAA is the competent authority and they have to report accordingly.

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 should be properly removed).

AMC1 230(a)&(b) Information security external reporting scheme

In order to comply with the provisions under 230 (a) and (b), the organisation should report:

(a) any occurrence covered by UK Regulation (EU) No 376/2014 that originated from intentional unauthorised electronic interactions;

(b) information security incidents having a potential significant risk to aviation safety not covered under UK Regulation (EU) No 376/2014;

(c) vulnerabilities that pose a significant risk to aviation safety and are not yet adequately mitigated in accordance with an approved vulnerability management strategy (see AMC1 220(b)).

GM1 230(a)&(b) Information security external reporting scheme

RELATION BETWEEN 230(b) AND UK REGULATION (EU) No 376/2014

UK Regulation (EU) No 376/2014 is UK retained legislation, originating from 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 230(b) does not exempt organisations from compliance with UK Regulation (EU) No 376/2014.

For each category of reporter, UK Regulation (EU) 2015/1018 defines the nature of items to be mandatorily reported. UK 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 UK Regulation (EU) No 376/2014 does not exempt organisations from compliance with point 230(b). However, this should not give rise to two parallel reporting systems, and point 230(b) and UK Regulation (EU) No 376/2014 should be seen as complementary in that respect.

In practice, this means that reporting obligations under point 230(b) on the one hand and reporting obligations under UK 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 UK Regulation (EU) No 376/2014 later identifies that the root cause of, or the contributing factor to, the occurrence was an intentional unauthorised electronic interaction, the organisation should update its notification to the CAA.

SIGNIFICANT RISK TO AVIATION SAFETY

In line with the definition of occurrence under Article 2(7) of UK Regulation (EU) No 376/2014, any information security incident or vulnerability, which may represent a significant risk to aviation safety, should be considered a reportable occurrence. 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: When assessing the possibility that the effects of an information security incident could lead to an unsafe condition, the organisation should consider the combination of effects if the incident involves multiple systems; indeed, some assumptions about system independence that may be valid for fortuitous occurrences may be violated by deliberate acts.

RELATION BETWEEN 230(b)(1) AND OTHER REPORTING REQUIREMENTS OF INFORMATION SECURITY OCCURRENCES RELATED TO AVIATION PRODUCTS OR PARTS

For organisations subject to reporting requirements of information security occurrences related to aviation products or parts, compliance with the specific provisions in the implementing regulation for their domain is considered sufficient to achieve compliance with the requirement in point 230(b)(1).

For example, for organisations subject to UK Regulation (EU) No 748/2012, the reporting can be done in accordance with point 21.A.3A of Annex I (Part 21) to that Regulation.

AMC1 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 the safety impact judged to have resulted from the information security incident or discovered vulnerability. Where an occurrence is judged by the person identifying the possible unsafe condition to have resulted in an immediate and particularly significant hazard, the CAA expects to be advised immediately and by the fastest possible means (telephone, fax, email, telex, etc.) of whatever details are available at that time.

GM1 230(c) Information security external reporting scheme

Guidance regarding the reporting of information 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 UK 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 215 and related 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 235 Contracting of information security management activities

Organisations may decide to outsource certain activities to suppliers, both for their own operational needs and for the purpose of complying with this Regulation (information security management activities). Activities contracted for operational needs may fall within the scope of the ISMS regulation and therefore the relevant information security risks have to be managed in accordance with the requirements in points 205 and 210. Instead, information security management activities are subject to the specific provisions of 235 because matters relating to these activities can have a major impact on the organisation.

Therefore the objectives of point 235 are:

(a) to protect critical and sensitive information and assets when being handled by organisations contracted for the provision of information security management activities (including organisations in the supply chain) at either their facilities or the 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 235 Contracting of information security management activities

(a) 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 responsible for the oversight of the contracted organisation(s) and accountable for compliance with this Regulation.

(b) A contract could take the form of a written agreement, letter of agreement, service letter agreement, memorandum of understanding, etc. as appropriate for the contracted activities.

GM3 235 Contracting of information security management activities

EXAMPLES

The following Table 1 provides some examples of information security management activities that may be contracted in relation to the provisions referred to as in 200.

Table 1: Examples of information security management activities that may be contracted

200 points related to activities	Example of contracted activity
(a)(1): establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;	Information security policy drafting and consultancy
(a)(2): identifies and reviews information security risks in accordance with point 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.

200 points related to activities	Example of contracted activity
(a)(3): defines and implements information security risk treatment measures in accordance with point 210;	Define, develop and implement measures. Verify the initial and the continued effectiveness of the implemented measures (e.g. redteam/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 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 220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point 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 CAA as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;	Implement immediate reaction measures to an information security incident or vulnerability as notified by the CAA.
(a)(7): takes appropriate action, in accordance with point 225, to address findings notified by the CAA;	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 230 in order to enable the CAA 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 CAA and when required to the design approval holder or the organisation responsible for the design.
(a)(9): complies with the requirements contained in point 235 when contracting any part of the activities described in point 200 to other organisations;	Not applicable
200 points related to activities	**Example of contracted activity**

(a)(10): complies with the personnel requirements laid down in point 240;	Activities of the accountable manager in the frame of the provisions for a 'cyber security responsible manager' as referred to in 240 Compliance monitoring as foreseen by 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 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 to ensure effective implementation of corrective actions;	Compliance monitoring (as foreseen by 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 requirements of the regulation, the organisation shall implement a continuous improvement process in accordance with point 260.	Execute independent effectiveness and maturity assessments. Define, develop and implement the necessary improvement measures.
(c): The organisation shall document, in accordance with point 250, all key processes, procedures, roles and responsibilities required to comply with point 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 255.	Production of documentation to detail all key processes, procedures, roles and responsibilities required to comply with point 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 235(a) Contracting of information security management activities

(a) OVERSIGHT OF THE CONTRACTED ORGANISATION

In order to exercise oversight of the contracted organisation, the organisation under the ISMS regulation 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 of the roles and responsibilities of the parties (i.e. contracting and contracted organisation);

(iii) definition and review of KPIs;

(iv) reaction to deviation from contractual obligations;

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

(vi) provision of feedback on the result of the compliance audits both within the organisation and to the contracted organisation, and response to findings. The feedback on the outcome of the compliance audits within the contracting organisation should reach the accountable manager or delegated person(s) to ensure proper monitoring of the response to findings (i.e. implementation of corrective actions) or, if deemed necessary, termination of the contract.

Note: The right of the organisation to conduct compliance audits of the contracted organisation should be included in the contract between the parties.

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

In order to properly manage 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 information 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 the ISMS regulation and the contracted organisation.

(3) The organisation establishes and maintains appropriate information security communication channels with the contracted organisation.

GM1 235(a) Contracting of information security management activities

PRIOR ASSESSMENT

The purpose of the prior assessment is to evaluate suppliers' competencies, sustainability as well as qualifications in relation to the information security activities to be contracted. This prior assessment

may need to be carried out taking into account other legal requirements or procurement procedures that apply to the organisation, and may therefore be carried out in different ways, such as:

(a) in case of public bids, inclusion of eligibility requirements in the procurement documents for the potential suppliers;

(b) review of the information security certifications granted by external and impartial auditors to the potential suppliers;

(c) review of self-assessment questionnaires compiled by the potential suppliers.

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 consider the roles and responsibilities of the contracting and contracted organisation as well as their interfaces.

GM2 235(a) Contracting of information security management activities

AUDIT OF CONTRACTED ORGANISATIONS

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

— the scope of the audit as well as the objective should be limited to processes, resources (i.e. contracted organisation personnel, systems/equipment, networks) and data used for the execution of the ISMS regulation contracted activities;

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

— findings identified during an audit should be addressed through a remediation plan within a time frame to be validated by the contracting organisation.

AMC1 235(b) Contracting of information security management activities

In order to ensure access by the CAA to the contracted organisation upon request, the organisation under the ISMS regulation should ensure that such a requirement or clause is included in the contractual documentation.

The CAA'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 of the contracted activities with the applicable requirements.

GM1 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.

In those cases where the organisation would use commercial off-the-shelf services with standard contractual clauses as part of the contracted information security management activities, the organisation should consider whether these clauses provide sufficient access to the required information.

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 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 240(a)(2) Personnel requirements

PROMOTION OF INFORMATION SECURITY POLICY

The accountable manager of the organisation should make sure that the information security policy is known and easily accessible for staff members as appropriate to their duties.

AMC1 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 should have the ability to explain the overarching objectives of the Regulation and its implications for the organisation.

GM1 240(a)(3) Personnel requirements

BASIC UNDERSTANDING OF THE REGULATION

In the event that the accountable manager has no previous experience in the areas of activity pertinent to the ISMS regulation, he or she may gain the necessary understanding by attending a training covering the content the Regulation and the technical basis for compliance. In particular, the training

material should cover the overarching objectives of the ISMS regulation, and the assessment should evaluate the understanding of these regulatory objectives.

AMC1 240(b) Personnel requirements

APPOINTMENT OF A PERSON OR GROUP OF PERSONS

The person or group of persons appointed under point 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 has direct access to the accountable manager (or the cyber security responsible manager, if appointed) to provide 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 (or the cyber security responsible manager) properly informed on compliance and information security matters (for instance, through meetings organised on a regular 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 appointed 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 250(a)(2)).

GM1 240(b) Personnel requirements

A condition of a lengthy absence of an appointed person occurs when that person is unable to perform the assigned organisational duties. For example, if an information security management activity is required to be carried out by appointed persons at a specified interval, an absence is considered lengthy when it exceeds this interval and therefore a vulnerability in the management activity may arise.

GM1 240(b)&(c) Personnel requirements

Appointments may 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 information security management positions, but it should identify to the CAA the titles and the persons chosen to carry out these functions.

GM1 240(c) Personnel requirements

COMPLIANCE MONITORING FUNCTION

The person appointed under point 240(c) with the responsibility to manage the compliance monitoring function required under point 200(a)(12) may be the same person as, or report to, the person

responsible for the compliance monitoring function required under the implementing regulation for the domain.

AMC1 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 cyber security responsible manager;

(b) the requirements of this Regulation have been communicated to and shared with the cyber security responsible manager;

(c) the cyber security responsible manager 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 240(e) Personnel requirements

Cyber Security Responsible Manager

If a Cyber Security Responsible Manager (CSRM) is delegated by the accountable manager for the activities under this Regulation, this person should also be given the appropriate delegation that is necessary to implement the provisions of 200, including the authority and the financial means to mobilise and control the resources across the organisations, or parts of the organisation involved. This delegation may also include the appointment of the person or group of persons referred to in 240(b) and (c) and, in general, the CSRM may be assisted in the performance of his or her duties by additional personnel.

The possibility of delegating a CSRM applies to an organisation that shares information security organisational structures, policies, processes and procedures with other organisations or with parts of its own organisation that are not part of the authorisation or declaration, and therefore this CSRM is expected to have information security responsibilities and competencies. In particular, the CSRM should be capable of managing the organisation's information security strategy and its implementation to ensure the achievement of the objectives described in the ISMS regulation requirements.

Where an entity holds multiple authorisations or declarations, the relevant accountable managers may delegate to the same CSRM, who will therefore be responsible for implementing the provisions of 200 for a functional cluster sharing information security structures, policies, processes and procedures.

AMC1 240(f) Personnel requirements

SUFFICIENT PERSONNEL

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

(a) the organisational structures, policies, processes and procedures subject to information security management;

(b) the amount of coordination required with other organisations, contractors and suppliers; (c)

the level of risk associated with the activities performed by the organisation.

GM1 240(f) Personnel requirements

SUFFICIENT PERSONNEL

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 235.

The activities reported in Appendix II, on the main tasks stemming from the implementation of PartIS, should be considered when establishing the organisational structure necessary to comply with the requirements of this Regulation.

AMC1 240(g) Personnel requirements

NECESSARY COMPETENCE

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

(1) work roles and the associated tasks;

(2) required knowledge, skills and abilities.

(b) As part of the process to ensure that personnel maintain the necessary competence, the organisation should:

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

(2) align the personnel qualifications and experience with the competence expected to fulfil their roles by organising adequate learning programmes for existing members of personnel, by recruiting new resources, or by a combination thereof;

(3) maintain the personnel competence during the time they are assigned to the work role.

GM1 240(g) Personnel requirements

NECESSARY COMPETENCE AND 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 CSF).

In Appendix II, the main tasks of this Regulation are listed and mapped to the competencies derived from the NIST CSF. This mapping may be used to establish a baseline to identify the aforementioned competence gaps. However, it should be noticed that existing cybersecurity/information security competence frameworks such as the NICE typically focus primarily on the protection of standard information technologies; therefore, the proposed list of competencies may need to be adapted to the technologies or integrated with processes used in the organisation.

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 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, all personnel performing the activities required under this Regulation should acknowledge, in a traceable and verifiable manner, understanding of the assigned roles and the associated information security responsibilities.

GM1 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 240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

For the personnel who have access to information systems and data subject to the requirements of the ISMS regulation, the identity should be determined on the basis of documentary evidence.

To establish the trustworthiness of such personnel, the organisation should have a documented process and appropriate criteria to ensure that individuals can be trusted to perform their role.

GM1 240(i) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

(a) Trustworthiness may be established, for example, by:

(1) prior to employment, a background check carried out in accordance with the applicable rules of Union and national law. This check may include verification of:

(i) education, previous employment and any gaps in the previous years;

(ii) absence of criminal record;

(iii) any other relevant information or intelligence considered relevant to the suitability of a person to work in the expected role;

(2) during employment, monitoring the employee's commitment and conduct.

(b) Furthermore, the process and criteria to establish personnel's trustworthiness may have to consider whether:

(1) the information systems and data to be accessed have been associated with a high severity of the safety consequences with the risk assessment process under 205;

(2) controls or mitigating measures for risk treatment identified during the risk analysis rely on organisational/operational procedures — for instance, correct configuration and administration of information technologies, database operations, information security monitoring, etc.

In such cases, the personnel who have administrator rights or unsupervised and unlimited access to the systems and data mentioned in (a)(1), or the personnel who applies the measures under above point (b)(2), may be subject to more stringent criteria.

(c) Intelligence and any other relevant information may be gathered by screening and analysing public sources such as social media and websites, within the limits set by relevant national laws and regulations.

(d) Some organisations subject to the ISMS regulation may also be subject to the Single Consolidated Direction (Aviation) 2/2023 that requires successful completion of background checks for personnel in certain roles, as well as a mechanism for the ongoing review of these checks. In such cases the organisation may consider suitable for the establishment of the personnel's identity and trustworthiness required under the ISMS regulation, in relation to their role, the process and the relevant criteria defined in SCD 2/2023 for standard and enhanced background checks. However, it should be noted that compliance with the provisions for the establishment of identity and trustworthiness under the ISMS regulation does not constitute compliance with the provisions on background checks as defined in SCD 2/2023.

GM1 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 provided for by the implementing rule for its domain.

AMC1 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 records of information security events when the objective of the requirement under (a)(5) has been met.

GM1 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 information security incidents 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 information security events.

Records of information security events include those events identified to be within the scope of the detection activities under 220(a), as well as other information security data produced by assets that have been identified under 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 245(c)&(d) Record-keeping

When complying with the requirements under points (c) and (d) for all the records required by points 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, availability and authenticity should be protected in consistency with protection of corresponding operational data, and as such, should be within the scope of the ISMS.

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

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

GM1 245(c)&(d) Record-keeping

RECORDS ACCESSIBILITY THROUGHOUT THE RETENTION PERIOD

It is recommended to follow best practices for data retention and, for data that may need to be restored, backup strategies, such as the use of automated backup tools, segregation or geographic separation of backup storage location(s), and to consider offline backups to prevent ransomware risks. These practices 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 degradation factors (e.g. excessive heat, light or 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, records can be protected, for example, by implementing a role-based access control (RBAC) approach, or certain records can be password protected at the 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 250(a) Information security management manual (ISMM)

The organisation may choose to document some of the information required under point 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.

In the event where an entity holds multiple authorisations or declarations, the ISMM may apply to one or more organisations at a time based on a common ISMS. This ISMM should include at least an approval document of each organisation and should formally be approved by each organisation's accountable manager or responsible person. A Cyber Security Responsible person may be appointed as per 240(d) and the guidelines of GM1 240(e).

To ensure that all parties involved can fulfil their responsibilities, all manuals, procedures, and communication between them are advised to be, at least, in one common language, e.g. English. Those parties involved include the competent authorities with which that common language should be agreed upon.

AMC1 255 Changes to the information security management system

Without prejudice to the communication of changes as required for each organisation in the corresponding implementing regulation for the domain as listed in 100, the procedure referred to in

255(a)(1) should take into account the criticality of the changes when proposing how they will be managed. In particular, those changes that could have an impact on the achievement or maintenance of compliance with the provisions under the ISMS regulation, or which could lead to an unacceptable level of risk (e.g. as per the guidance provided in GM1 205(c)), should be subjected to scrutiny. Upon establishment of this procedure, any further changes to it should be subject to approval by the CAA.

Where prior approval is sought from the CAA for a change not covered by an approved procedure, or where no such approved procedure exists, the organisation should provide at least the following information:

— the nature and purpose of the change;

— the implementation plan of the change;

— the verification plan of the change;

— the potential impact on aviation safety introduced by the change.

A significant deviation from the original implementation plan during the change process is an event that should be reported to the CAA as this deviation may require reconsidering the change impact.

GM1 255 Changes to the information security management system

Point 255 is structured as follows:

Point (a) introduces the possibility for the organisation to agree with the CAA 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 CAA) for changes not covered by the procedure mentioned above, and 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 CAA as provided for under 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 255(b). In any case, all changes should be notified to the CAA upon implementation.

GM2 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 260) should be handled as any other change according to the guidelines in AMC1 255 and GM1 255.

EXAMPLE OF CHANGES THAT MAY HAVE AN IMPACT ON THE ISMS

Below are some examples of changes that may have an impact on the ISMS, or which could lead to an unacceptable level of risk and therefore should be subject to scrutiny by the CAA according to the provisions established under 255:

(a) Changes to the scope of the ISMS, 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 has delegated certain responsibilities under the ISMS regulation to a person or a group of persons.

— The organisation contracts information security management activities as per 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 security event management process:

— The organisation decides to contract security event management activities.

— The organisation changes the process to notify security events and the criteria to escalate to higher management for a quicker resolution.

— The organisation changes its policy for mitigating vulnerabilities.

— The organisation changes its incident recovery procedure.

EXAMPLE OF CHANGES THAT DO NOT HAVE AN IMPACT ON THE ISMS

Not all operational changes related to information security have an impact on the ISMS, therefore not all changes are required to be reported to the CAA, following the provisions established under 255. The following scenarios may be representative of such changes:

— 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 260 Continuous improvement

The continuous improvement process (CIP), as required by 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 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 on 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), planning, development and implementation of actions and changes to the ISMS, its processes or elements to achieve the improvements.

(e) Evaluation the effectiveness of the implemented actions and ISMS changes, and, as applicable, verification 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 260 Continuous improvement

Point 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:

— 260(a) addresses, using adequate performance indicators, the effectiveness and maturity assessment of the ISMS;

— 260(b) addresses the improvement measures, i.e. corrections and corrective actions, for the deficiencies detected in 260(a) and the continuous improvement process.

Similar provisions for continuous improvement are provided for in other information management systems such as ISO/IEC 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 organisation'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 organisation which needs to be continuously monitored and improved to ensure alignment with the organisation'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 organisation may integrate the ISMS 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 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 organisation'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 establishes the disciplines needed to manage information security, e.g. by using broadly accepted industry standards, 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 organisation's requirements, and to determine where there are potential areas for improvement.
- Review and evaluation by management of the current action plan, setting or revision of the objectives or decision on improvement opportunities and actions
- Organisation'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 260(a) Continuous improvement

(a) **ISMS EFFECTIVENESS EVALUATION**

When complying with 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 calendar basis of the assessments should be commensurate with the maximum level of risk established under 205.

The process to monitor, measure, evaluate and review the effectiveness of the organisation's ISMS referred to under AMC1 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 ASSESSMENT**

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, ensure that the model defines 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 information 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 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 CSF), 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/IEC 27001.

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

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

Mapping to 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

No specific maturity level is required. However, if and when compliance is achieved, organisations will determine which requirements of which models have already been met (mandatory) and can opt to reach a level that is beneficial to the organisation (voluntary). In the longer term, achieving higher maturity levels may increase the confidence of oversight authorities, which can have an impact upon the level of oversight activities regarding such organisation.

AMC1 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 for 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(s) of, and contributing factors to, 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:

(1) to be effective and to result in acceptable residual risks,

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

(3) 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 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 260(b) Continuous improvement

The 'necessary improvement measures' referred to in 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 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 for 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 260(b);

(f) reporting to and reviewing the outcomes of the process steps with the management (see point (d) of AMC1 260(b));

(g) documenting and evidencing the result of the process steps above (see point (e) of AMC1 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 to ATC digital 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

Non-exhaustive summary of potential threats

- threat (availability): exceeding system performance, saturation of communication channel
- threat (integrity): man-in-the-middle or injection attacks
- threat (confidentiality): passive listening to communication, spying on hardware device

Summary of threats scenarios and their potential harmful impacts on safety

- Disruption of services prevents ATC communication with a single or multiple aircraft and/or ATC ground system.
- 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 regulatory 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.

Example 2: Tampered air traffic data

Threat vector assets/domain

- Internet service provider (ISP)
- ATM services network(s)
- surveillance data
- ATC systems

Non-exhaustive summary of potential threats

- ISP compromise (confidentiality): An attacker gains unauthorised access to the systems or infrastructure of the ISP providing network services to ATM system.

- data tampering (integrity): Once the ISP is compromised, an attacker could manipulate data in transit. This could involve injecting false data or removing/modifying legitimate data.
- denial of service (availability): an attacker could also potentially disrupt the communication of data entirely, resulting in a denial of service (DoS) to the ATM system.
- malware injection (integrity/availability): An attacker could potentially use the compromised ISP as a launching pad to inject malware into the systems, causing further disruptions or enabling additional attacks.

Summary of threats scenarios and their potential harmful impacts on safety

- ISP compromise: interception and/or manipulation of sensitive data, impacting the safe management of air traffic.
- data tampering: incorrect situational awareness, potentially resulting in reduced separation between aircrafts, and incorrect air traffic control decisions.
- denial of service: reduction of the ATC's ability to ensure separation leading to the activation of contingency procedures, including capacity reduction, with the eventual possibility of large areas of airspace being closed.

Example 3: Software supply chain and infrastructure

Aircraft operators', CAMOs' and aircraft maintenance organisations' software supply chain and ground infrastructure, including equipment used to support aircraft management, operations and maintenance

Threat vector assets/domain

- aircraft operators', CAMOs' and maintenance organisations' supply chain
- aircraft operator or maintenance internal ground infrastructure used to manage aircraft and operations (hardware/software) and other information technology assets
- information technology assets used to update systems on an aircraft (software and hardware) used for maintenance activities

Non-exhaustive summary of potential threats

- threat (availability): hardware/software/system disruption
- threat (integrity): compromised hardware/software/system
- threat (confidentiality): compromised hardware/software/system

Summary of threats scenarios and their potential harmful impacts on safety

- Disruption to the dissemination of meteorological information while the aircraft is airborne, may reduce the ability of the flight crew to avoid potentially hazardous meteorological conditions (e.g. severe storms/fog at night).
- Manipulation of navigation data/database will have the effect that flight plans and navigation displays cannot be trusted.
- Lack of control and access to information such as fleet maintenance programme or flight crew planning affects the ability of organisations to maintain safe operations.

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 mitigating 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 and aircraft internals information leaks*
Information security bow-tie analysis element	**Aviation safety bow-tie analysis element**
	Safety mitigating barriers 1) use of back-up procedures to prevent faulty maintenance actions 2) use of procedures to secure aircraft software integrity

	Safety consequences 1) faulty maintenance actions 2) incorrectly completed maintenance actions 3) exfiltration of information allows for identification of vulnerabilities 4) disruption of aircraft systems, unpredictable system function, loss of major aircraft systems (such as engine control)

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 update systems on an aircraft (software/hardware) used for maintenance operations or ATM/ANS ground automation systems

Non-exhaustive summary of potential threats

- threat (availability): systems used to store, transmit and exchange information are rendered unavailable for essential operations through DoS 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

Summary of threats scenarios 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 safetycritical systems.

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

Non-exhaustive summary of potential threats

- threat (availability): training systems or training devices are rendered unavailable by means of DoS attacks when they are needed to be used
- threat (integrity): training systems or training devices are compromised through man-inthe 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

Summary of threats scenarios 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.

Example 6: Airport's fuel delivery system and associated infrastructure

Threat vector assets/domain

- ground fuel storage and distribution infrastructure
- digital systems used to control fuel pumping and metering
- supply chain for fuel delivery, including third-party fuel suppliers
- airport information technology assets used for fuel inventory management and scheduling deliveries

Non-exhaustive summary of potential threats

- threat (availability): disruption of fuel supply or delivery systems
- threat (integrity): tampering with fuel control systems or measurement devices

- threat (confidentiality): unauthorised access to fuel supply and delivery data

Summary of threats scenarios and their potential harmful impacts on safety

- Disruption to fuel delivery can lead to flight delays or cancellations, causing operational disruptions and potential safety issues if fuel reserves become critically low.
- Tampering with fuel control systems or measurement devices could lead to incorrect fuel loads being delivered to aircraft, impacting aircraft weight and balance calculations, and potentially causing fuel exhaustion incidents.
- Unauthorised access to fuel supply data could allow threat actors to manipulate fuel scheduling or inventory data, potentially causing disruptions to airport operations and fuel availability for aircraft.

Example 7: The NOTAM system and associated infrastructure in the UK

Threat vector assets/domain

- National NOTAM system infrastructure and digital interface
- Supply chain for NOTAM system maintenance and updates
- IT assets used for NOTAM creation, distribution, and storage

Non-exhaustive summary of potential threats

- threat (availability): disruption of the NOTAM system or its access
- threat (integrity): tampering with NOTAM data or unauthorised NOTAM creation
- threat (confidentiality): unauthorised access to NOTAM data

Summary of threats scenarios and their potential harmful impacts on safety

- Disruption to the NOTAM system could prevent the dissemination of critical aeronautical information to pilots and air traffic controllers, potentially leading to safety issues.
- Tampering with NOTAM data or unauthorised creation of NOTAMs could lead to incorrect information being disseminated, potentially resulting in pilots making decisions based on false or misleading data.
- Unauthorised access to NOTAM data could lead to information leakage, potentially revealing sensitive operational information.

Example 8: CAA's airworthiness directive (AD) system and associated infrastructure

Threat vector assets/domain

- CAA AD system infrastructure and digital interface
- supply chain for AD system maintenance and updates
- CAA IT assets used for AD creation, distribution, and storage

Non-exhaustive summary of potential threats

- threat (availability): Disruption of the AD system or its access
- threat (integrity): tampering with AD data or unauthorised AD creation
- threat (confidentiality): unauthorised access to AD data

Summary of threats and their potential harmful impacts on safety

- Disruption to the AD system could prevent the dissemination of critical airworthiness information to aircraft operators and maintenance organisations, potentially leading to safety issues.
- Tampering with AD data or unauthorised creation of ADs could lead to incorrect information being disseminated, potentially resulting in aircraft operators and maintenance organisations making decisions based on false or misleading data.
- Unauthorised access to AD data could lead to information leakage, potentially revealing sensitive operational information.

Appendix II - Main tasks stemming from the implementation of ISMS, including mapping to NIST CSF 1.1 competencies and ISO/IEC 27001 clauses and controls

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Establish and operate an information security management system (ISMS)	Management	200(a)	IDENTIFY	ID.RM	4 6.1.1		
Establish the scope of the ISMS according to the regulation requirements	Management	205(a)	IDENTIFY	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implement and maintain an information security policy	Management	200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1	A5.1
Identify and review information security risks	Management	200(a)(2) 205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implement information security risk treatment measures	Management	200(a)(3) 210	PROTECT	PR.PT	6.1.3 8.1 8.3		
Implement measures to detect information security events and identify those related to aviation safety	Management	200(a)(5) 220	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	A7.2 A8.15 A5.28
Implement measures that have been notified by the CAA	Operational	200(a)(6)			10.1	A6.1.3	A5.5
Take appropriate remedial actions to address findings notified by the CAA (noncompliances)	Both	200(a)(7) 225			10.1	A6.1.3	A5.5
Implement an external information security reporting scheme	Management	200(a)(8) 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	A5.5 A6.8

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Monitor compliance with this Regulation and report findings to top management	Operational	200(a)(12)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Protect confidentiality of exchanged information	Operational	200(a)(13)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	200(b) 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	A5.1 A5.28 A5.29 A5.35
			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	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	A5.1 A5.2
			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	205(a)	IDENTIFY	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	A8.1.1	A5.9
Identify the interfaces with other organisations which could result in exposure to information security risks	Management	205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Identify information security risks and assign a risk level	Management	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	205(d)	IDENTIFY	ID.RM	8.2		A5.7
Organisations under Subpart C of Annex III (Part-ATM/ANS.OR) to UK Regulation (EU) 2017/373 share the safety support assessment	Operational	205(e)					
Develop and implement measures to address risks and verify their effectiveness	Operational	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	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	200(a)(4) 215(a) 215(e)	IDENTIFY	ID.AM-3	7.4	A16.1.1 A16.1.2	A5.28 A6.8
Ensure that contracted organisations report information security events	Management	215(c)	RESPOND	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2	A5.19 A6.8
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Operational	215(b)(1)(b)(3)	IDENTIFY	ID.RA -1		A12.6.1 A16.1.1 A16.1.4	A8.8 A5.24 A5.25

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
			DETECT	DE.AE-2 DE.AE-3 DE.AE-5			
Implement measures to detect in processes and operations information security events which may have a potential impact on aviation safety	Operational	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	A7.2 A8.8 A8.15 A8.16 A5.24 A5.25 A5.26 A6.8
			PROTECT	PR.PT-1			
Implement measures to respond to information security events that may cause an information security incident	Operational	220(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5	A5.26
Cooperate on investigations with other organisations that contribute to the information security of its own activities	Management	215(d)	RESPOND	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7	A5.20 A5.21 A5.28
Implement measures to recover from information security incidents	Operational	220(c)	RECOVER	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6	A5.26 A5.27
Manage risks associated with contracted activities with regard to the management of information security	Management	235	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	240(f)	IDENTIFY	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Create and maintain a process to ensure that the personnel have the	Management	240(g)	IDENTIFY	ID.AM-5 ID.AM-6	7.2	A7.2.2	A6.3

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
necessary competence for activities regarding information security management			PROTECT	PR.AT-1			
Create and maintain a process to ensure that the personnel acknowledge the responsibilities associated with the assigned roles and tasks	Management	240(h)	IDENTIFY	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2
Verify the identity and trustworthiness of personnel who have access to information systems	Management	240(i)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
Archive, protect and retain records and ensure they are traceable for a specified time	Operational	245	IDENTIFY	ID.RA-4	7.5	A8.2.2 A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3	A5.10 A5.13 A7.3 A7.5 A8.6 A8.10 A8.13 A8.15
			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 CAA within the period agreed with the CAA	Operational	225			10.1	A18.1.1 A18.2	A5.31 A5.35 A5.36
Implement an information security reporting system in accordance with UK Regulation (EU) No 376/2014	Management	230(a)					
	Operational	230(b) 230(c)	DETECT	DE.DP-3	7.4	A16.1.1	

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Report information security incidents or vulnerabilities to the CAA and, under certain conditions, to others			RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5		A16.1.2 A16.1.3	A5.24 A6.8
			RECOVER	RC.CO-3			
Regularly assess the effectiveness and maturity of the ISMS	Operational	260(a)			9	A5.1.2 A12.7.1 A16.1.6	A5.1 A5.27 A8.34
Take actions to improve the ISMS if required. Reassess the ISMS elements affected by the implemented measures.	Operational	260(b)			10	A5.1.2	A5.1
Ensure accessibility of the CAA to the contracted organisation	Management	235(b)			9.3	A6.1.3 A15.1 A15.2	A5.5 A5.20 A5.22
Top management ensures that all necessary resources are available to comply with the Regulation	Management	240(a)(1)	IDENTIFY	ID.AM-5 ID.AM-6	7.1	A6.1.1	A5.2
Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Management	240(a)(2) &(a)(3)	IDENTIFY	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2	A5.1 A5.4 A6.3
			PROTECT	PR.AT-1 PR.AT-4			
Appoint a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Management	240(b) 240(c) 240(d)	IDENTIFY	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2	A5.2 A5.4 A6.3
			PROTECT	PR.AT-1 PR.AT-4			
Create and maintain an information security management manual (ISMM)	Management	250			7.5.1	A6.1.3 A12.1.1	A5.5 A5.37

ISMS main task	Activity type	Reference					
	Management, Operational	ISMS Regulation	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Develop a procedure on how to notify the CAA upon changes to the ISMS	Management	255(a)	IDENTIFY	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14
Manage changes to the ISMS and notify the CAA and/or request for approval of changes	Management	255(a) 255(b)	IDENTIFY	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14

Appendix III - Examples of aviation services

The following is a non-exhaustive and non-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)