Acceptable Means of Compliance and Guidance Material to Annex I (Part-IS.AR) to Commission Implementing Regulation (EU) 2023/203

Issue 1

12 July 2023[1]

[1] For the date of entry into force of this Issue, kindly refer to ED Decision 2023/010/R at the Official Publication of EASA.

TABLE OF CONTENTS

AMC AND GM TO ANNEX I (PART-IS.AR) TO COMMISSION IMPLEMENTING REGULATION (EU) 2023/203

GM1 IS.AR.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 Regulation (EU) 2023/203. 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 higher-level 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.

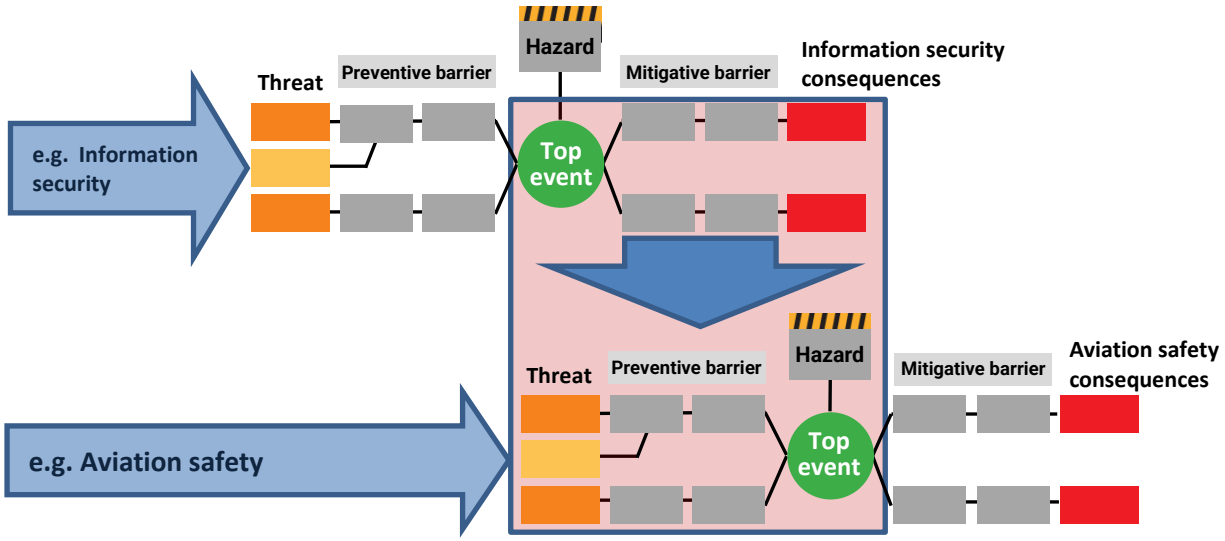

Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

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 and 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 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.

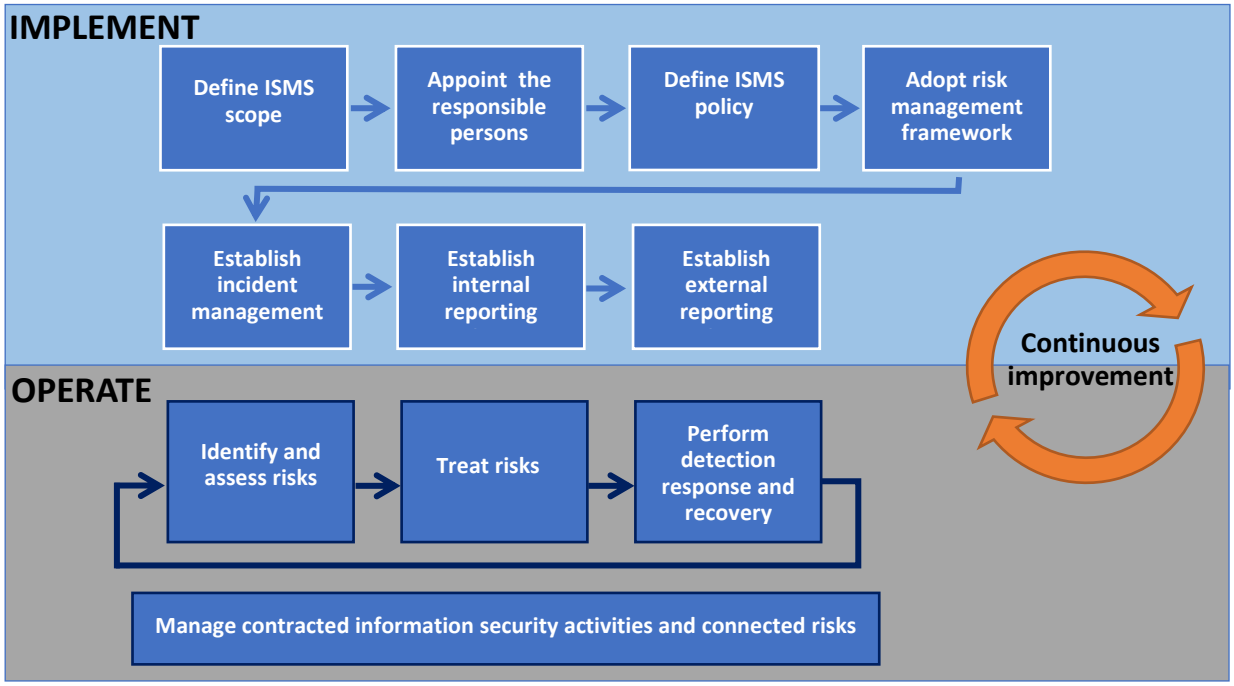

Figure 2: Representation of the Part-IS requirements from an ISMS's life cycle perspective

Plan-Do-Check-Act approach

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

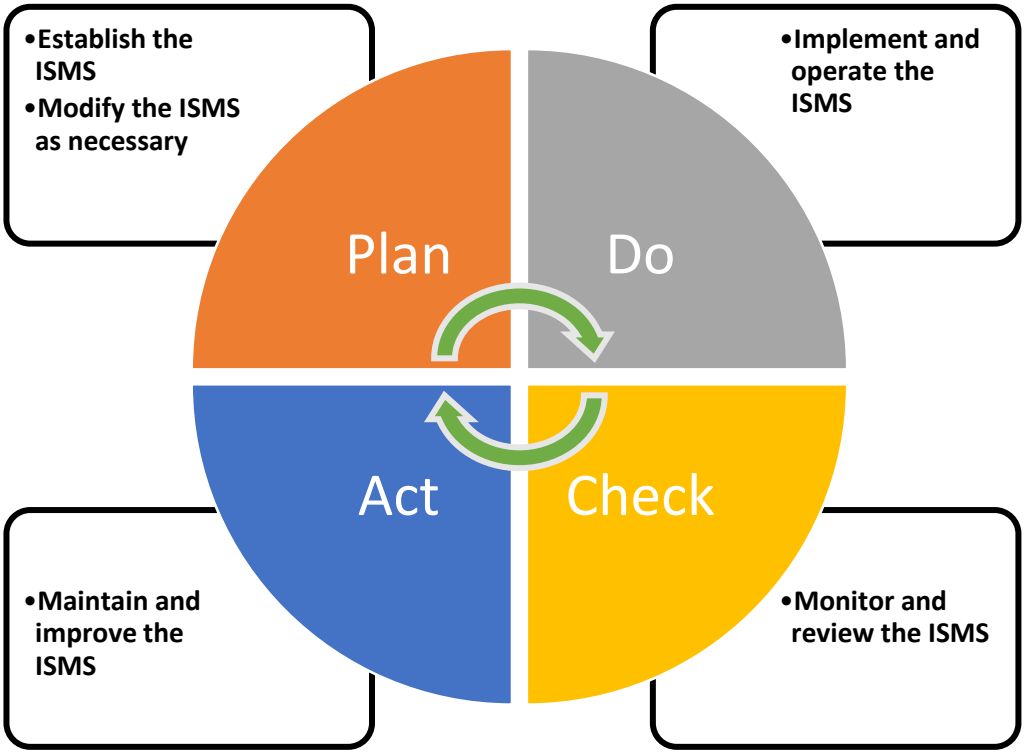

Figure 3: Plan-Do-Check-Act approach applied to an ISMS

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 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).

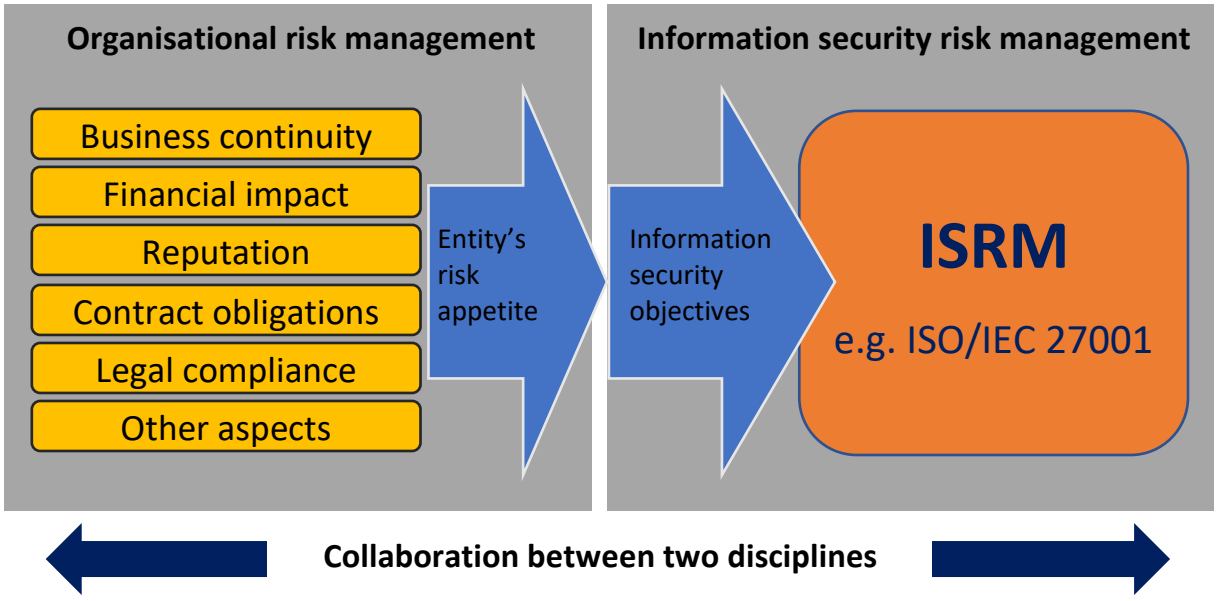

Figure 4: Relation between the entity's risk appetite and the information security objectives

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 Part-IS, 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 Regulation (EU) 2023/203, 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.

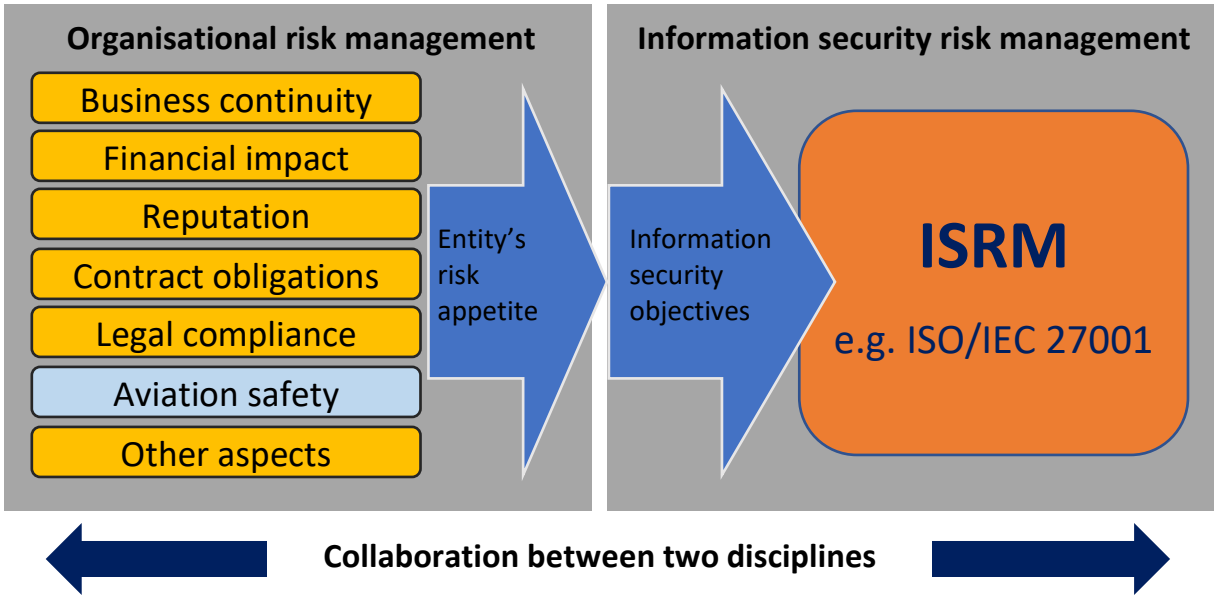

Figure 5: Introduction of aviation safety aspects in the entity's risk appetite

PART-IS versus ISO/IEC 27001 cross reference table

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

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

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

The information security policy should be endorsed by the person identified as per IS.AR.225(a) 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 competent authority to appropriately secure information and communication technology systems and data;

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

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

(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 competent authority 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 competent authority operations, such as a structural change within the authority 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 IS.AR.200(a)(1) Information security management system (ISMS)

INFORMATION SECURITY POLICY AND OBJECTIVES

The information security policy should suit the competent authority's purpose and direct its own information security activities. Such policy should contain the needs for information security in the competent authority'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 competent authority's objectives, and the results from the risk assessment and treatment (which, in turn, supports the implementation of the competent authority'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 competent authority'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 competent authority, more of a long-term nature and measurable with a reasonable effort relative to the delivered benefits.

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

COMPLIANCE MONITORING

When establishing compliance with the provisions under point IS.AR.200(a)(8), the competent authority 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. Compliance monitoring should include a feedback mechanism of audit findings to the person of the competent authority as identified in IS.AR.225(a) to ensure implementation of corrective actions as necessary.

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

COMPLIANCE MONITORING

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

— conformity of the ISMS to the requirements of this Regulation and the competent authority's own requirements either stated in the 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 scopes should be considered. Documented information should be retained evidencing the audit results, their reporting to the relevant management and the audit programme.

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

When establishing compliance with the provisions under points IS.AR.200(a)(9), the competent authority 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 Regulation (EU) 2018/1139. It should also comply with Regulation (EU) No 376/2014.

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

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

information needs to be shared and with whom.

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

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

(a) provide an outline of the structure of the specific information security personnel (internal and external), including their roles and responsibilities that will be used to manage and maintain the elements included within the scope of the ISMS and will be approved by the person identified in IS.AR.225(a). The competent authority should review the outline of the structure at planned intervals or if significant changes occur (see the Note in AMC1 IS.AR.200(a)(1));

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

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

(d) identify and document any other information that will be used to maintain compliance with the objectives 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 IS.AR.200(c) Information security management system (ISMS)

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

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

(b) responsibilities and accountabilities for roles relevant to information security — see the personnel requirements referred to in points IS.AR.225(a) and (b) and the related AMC and GM;

(c) scope of the ISMS and the interfaces with, and dependencies on, other parties — see

IS.AR.200(a)(2) and the information security requirements referred to in points IS.AR.205(a) and (b);

(d) information security risk management process — see the information security requirements referred to in points IS.AR.205 and IS.AR.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 IS.AR.230;

(f) evidence of the competencies necessary for the personnel performing the activities required under this Regulation — see IS.AR.225(c) and the related AMC and GM;

(g) evidence of the current competencies of the personnel performing the activities required under this Regulation — see IS.AR.230(b)(1);

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

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

PROPORTIONALITY IN ISMS IMPLEMENTATION

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

INTEGRATION OF ISMS UNDER THIS REGULATION WITH EXISTING MANAGEMENT SYSTEMS

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

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

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

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

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

GM1 IS.AR.205 Information security risk assessment

Part-IS 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 competent authority, and should be customised and tailored to meet the overall needs of a competent authority as well as the specific need to consider aviation safety aspects.

Competent authorities whose information security frameworks have achieved industry certifications can provide this information as supporting artefacts; however, these competent authorities should show the applicability of the industry certification to the scope of this Regulation (see GM1 IS.AR.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. Competent authorities may also wish to consider aviation-specific guidance as defined in the risk management chapter of the latest version of EUROCAE ED-201A 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 IS.AR.205(a) Information security risk assessment

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

A means to comply with the requirement in point IS.~~I~~.AR.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 IS.~~I~~AR.205(a).

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

SCOPE AND BOUNDARIES IDENTIFICATION

The competent authority 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 competent authority 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 authority; 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 IS.AR.205(b) Information security risk assessment

The competent authority 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 IS.AR.205(b) Information security risk assessment

RISK INFORMATION SHARING

Interfacing parties 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 the parties to establish a matching mapping for the services identified under IS.AR.205(a), including 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 subject to Regulation (EU) 2023/203 or Regulation (EU) 2022/1645, and those that are not.

Where the competent authority has interfaces with an organisation that is subject to Regulation (EU) 2023/203 or Regulation (EU) 2022/1645, 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, the competent authority 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 competent authority 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 competent authority may decide to manage the risks through contractual arrangements and require the supplier to implement mitigating measures and controls within its own organisation.

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

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

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

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

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

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

(c) the gathering of inputs that are relevant and 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 competent authority's risk profile.

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

RISK ASSESSMENT

The risk classification levels for potential of occurrence of the threat scenario and severity of the safety consequences listed below may be applied; however, this does not prevent the competent authority from developing additional intermediate categories if it deems this necessary for risk assessments. The competent authority should specify and document the applied, entity-specific classification levels with an accurate qualitative 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 competent authority 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 authority.

In order to facilitate the mutual comparability of risks assessment methodologies between interfacing entities, the competent authority may associate the assessment of the potential of occurrence of the threat scenario with one of the following categories:

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

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

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

The evaluation of the potential of occurrence of the threat scenario 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, tactics, techniques and procedures (TTPs) and success rate of attacks.

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

— High severity: those immediate or delayed scenarios that can cause or contribute to an 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 competent authority 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 up to date 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. 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 person identified in IS.AR.225(a) to accept risks above this level under defined circumstances and conditions.

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

— unacceptable risk;

— conditionally acceptable risk;

— acceptable risk.

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

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

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

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

Figure 1: 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 IS.AR.205(d)) and monitored to ensure that it remains low and that if the risk materialises, it is early detected and dealt with.

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

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

— a thorough review of those risks proposed to be conditionally acceptable that is performed by

the person identified in IS.AR.225(a) who may impose additional conditions for the risk retention, 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 competent authority 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.

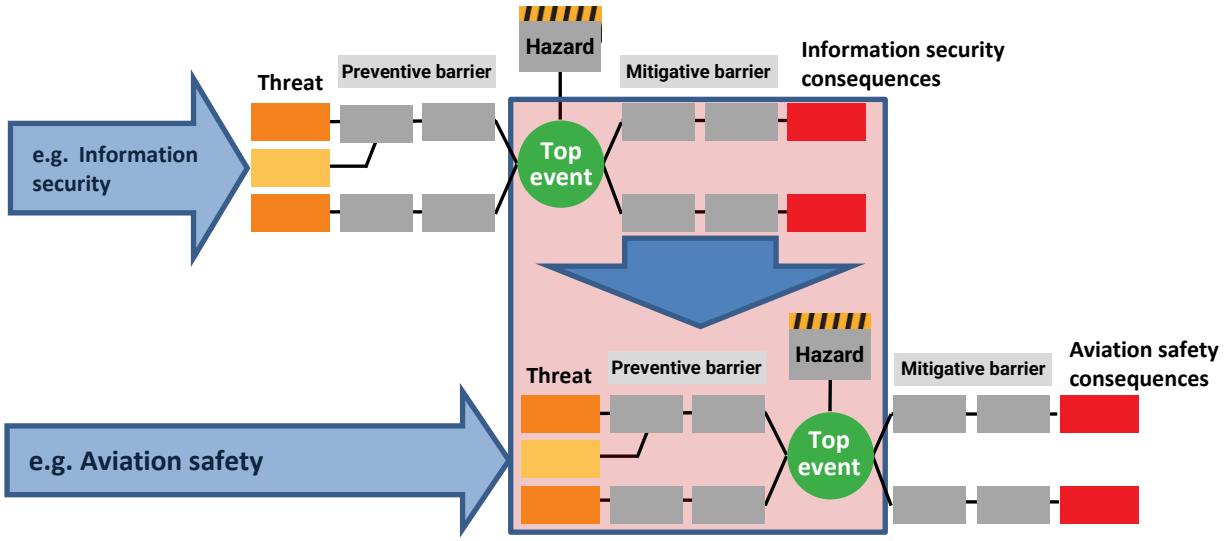

Figure 2: Interactions between information security and aviation safety risk management areas

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 catalogue examples and other threat catalogue examples as they are provided by EU institutions — for example, the ENISA threat taxonomy. However, this is not an exhaustive list of examples, and the identification of threat scenarios should therefore not be limited to those examples only. In addition, other relevant resources containing information on information security threats and the information security threat landscape should be consulted to support the risk assessment process with relevant inputs.

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

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

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

(a) The risk assessment performed under points IS.AR.205 (a), (b) and (c) should be reviewed at regular intervals to identify and account for relevant changes. The periodicity at which potential

changes have to be evaluated should be determined by the authority 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 competent authority and include the justification, date of approval and information about the risk owner.

GM1 IS.AR.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 registry.

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

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

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

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

- changes to threats and their values or addition of new threats that have not previously been assessed;
- changes to vulnerabilities or addition of new vulnerabilities that have not previously been assessed;
- changes in impacts or consequences of assessed threats or vulnerabilities;
- changes in aggregation of risks that may result in unacceptable levels of risks;
- changes or improvements in the risk management process, risk assessment approach and related activities;
- changes or improvements in the treatments of risks;

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

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

— understanding why and how incidents have occurred; and

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

GM1 IS.AR.210 Information security risk treatment

Unacceptable risks identified in accordance with point IS.I.OR.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 competent authority 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 by 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 person identified in IS.AR.225(a).

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 delay is also subject to the acceptance by the person identified in IS.AR.225(a). The identified person may condition such acceptance on the implementation or availability of compensating controls or reactive measures to monitor, early detect and timely respond to the materialisation of the risk in treatment. In order to timely respond, the incident response team may be informed to trigger their preparedness.

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

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

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

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

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

(b) When establishing compliance with the objectives under points IS.AR.210(a)(1) and IS.AR.210(a)(2), the competent authority 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 IS.AR.205(d), to evaluate whether the measures developed under these points introduce new unacceptable risks or modify existing risks into 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.

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

Without prejudice to the definition of 'information security event' in Article 3 of Regulation (EU) 2023/203, those events that indicate the potential materialisation of unacceptable risks include both occurrences (i.e. anything that causes harm or has the potential to cause harm) and discovery of vulnerabilities. In fact, information security risks are associated with the potential that threats will exploit vulnerabilities, therefore the discovery of an exploitable vulnerability is an information security event.

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

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

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

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

DETECTION

When complying with the requirement in IS.AR.215(a), the competent authority should define and implement a strategy to detect information security 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 an unacceptable consequence.

DETECTION STRATEGY

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

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

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

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

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

DETECTION STRATEGY

When developing the detection strategy, for those items within the scope of event detection, the competent authority should define the conditions that trigger a process that, for example, would require personnel intervention and further analysis. These conditions on the items may be defined using elements from 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 IS.AR.215(b) Information security incidents — detection, response and recovery

(a) INCIDENTS

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

(1) Preparation of procedures and delineation of roles and responsibilities to 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 IS.AR.215(a)(2), and assess their potential impacts on aviation safety;

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

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

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

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

(i) the maximum acceptable safety level degradation of the assets within the scope of the 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 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 competent authority should take into account the following aspects when establishing compliance with the objectives contained in point IS.AR.215(b) relative to vulnerabilities:

(1) Establishment of a vulnerability management 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 IS.AR.215(b) should be based on the maximum acceptable risk of the items within the scope of the vulnerability, considering the worst-case scenario of the vulnerability being exploited.

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

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

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

The term 'warning' as used in IS.AR.215 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 IS.AR.215(c) Information security incidents — detection, response and recovery

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

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

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

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

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

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

RECOVERY OBJECTIVES AND TIMING

Point IS.AR.215(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 became unreliable, the safety of flights is reduced too.

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

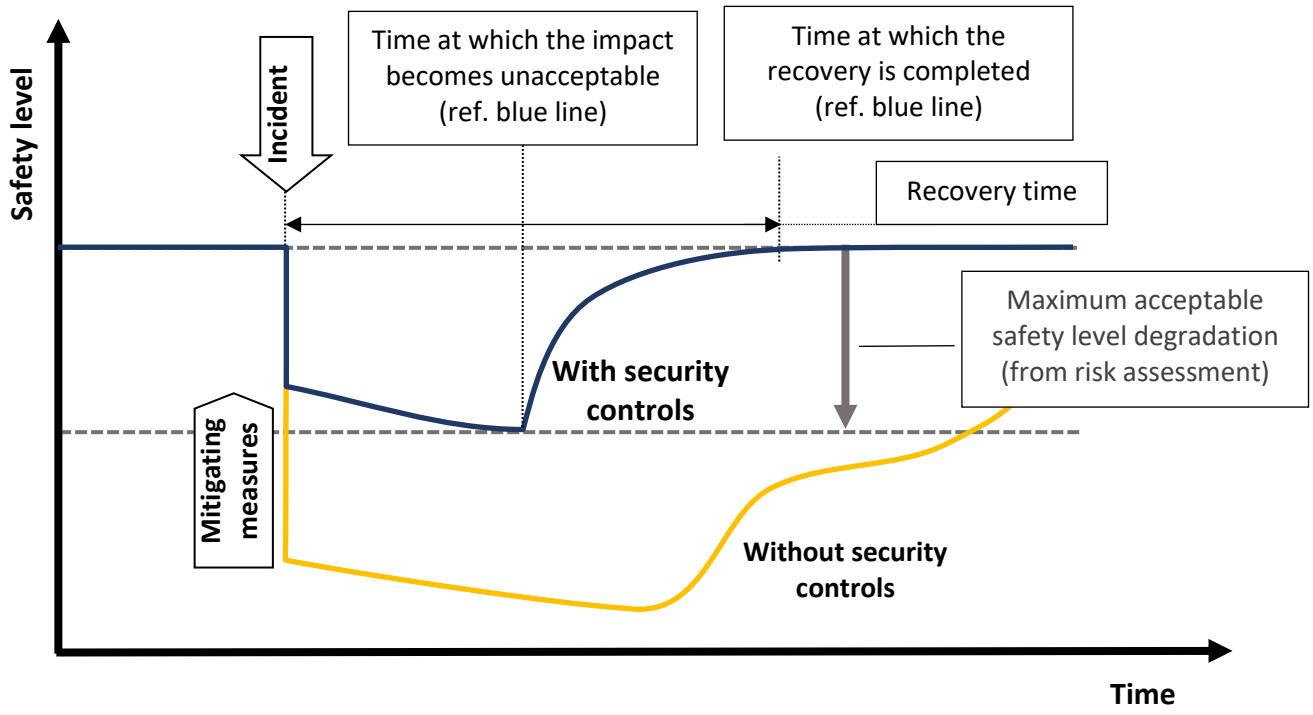

Figure 1: Conceptual framework for the definition of the response and recovery objectives

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.

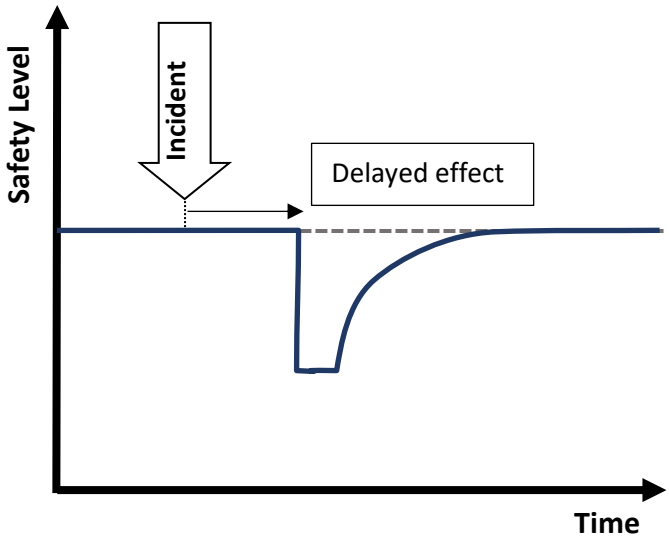

Figure 2: Incident with a delayed effect on safety

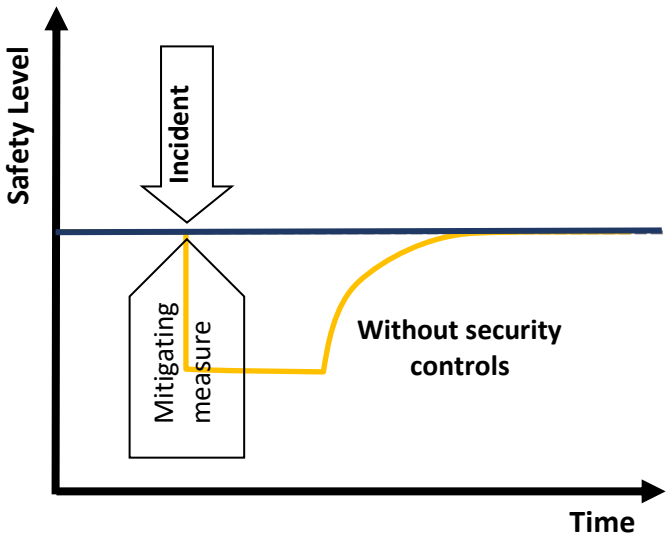

Figure 3: Incident with a fully mitigated effect on safety

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 under AMC1 IS.AR.215(c) may be expressed as a list of resources and services to be restored by order of priority, within the scope of the recovery. Guidance about objectives for recovery time can be found in EUROCAE ED-206, Chapter 7.3.5.

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

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

The resources required to apply the recovery measures should be available in order to implement 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 IS.AR.220. The contracting of recovery activities should be established before an incident occurs (proactive) and the contract should include provisions for the contracted party to react in a timely manner.

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

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

In such context the authority may not have a process or a recovery plan covering the specific occurrence. Therefore, the definition from the authority of a specific recovery plan is usually required.

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

Competent authorities 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 Part-IS and therefore the relevant information security risks have to be managed in accordance with the requirements in points IS.AR.205 and IS.AR.210. Instead, information security management activities are subject to the specific provisions of IS.AR.220 because matters relating to these activities can have a major impact on the competent authority.

Therefore the objectives of point IS.AR.220 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 competent authority facilities, or when being transmitted between the competent authority 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 competent authority, in the frame of the provision of information security management activities;

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

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

(a) The contracting of information security management activities is a means to allocate tasks from the competent authority to third parties (contracted organisations). The competent authority 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 IS.AR.220 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 IS.AR.200.

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

IS.AR.200 points related to activities	Example of contracted activity
(a)(1): establishes a policy on information security setting out the overall principles of the competent authority 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 IS.AR.205;	Identify activities, facilities and resources. Identify interfaces with other organisations which could be exposed to information security risks. Perform risk analysis or part of it, e.g. identify and classify information security risks.
(a)(3): defines and implements information security risk treatment measures in accordance with point IS.AR.210;	Define, develop and implement measures. Verify the initial and the continued effectiveness of the implemented measures (e.g. red-team/blue-team exercises, penetration testing, vulnerability scanning, etc.). Communicate to the involved stakeholders the outcome of the risk assessment and their responsibilities as part of the risk treatment process.
(a)(4): defines and implements, in accordance with point IS.AR.215, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety, and responds to, and recovers from, those information security incidents;	Define, develop and implement measures to detect events. Define, develop and implement measures to respond to any event conditions. Define, develop and implement measures aimed at recovering from information security incidents.
(a)(5): complies with the requirements contained in point IS.AR.220 when contracting any part of the activities described in point IS.AR.200 to other organisations;	Not applicable
(a)(6): complies with the personnel requirements contained in point IS.AR.225;	Contracted organisation to ensure that sufficient personnel is on duty to perform the activities related to this Regulation Define, develop and deliver adequate training to achieve the competencies required by the staff. Perform pre-employment checks.
(a)(7): complies with the record-keeping requirements contained in point IS.AR.230;	Define, develop and implement secured archiving. Provision of secure data centre (as a service) Provision of records updates

IS.AR.200 points related to activities	Example of contracted activity
(a)(8): monitors compliance of its own organisation with the requirements of this Regulation and provides feedback on findings to the person referred to in point IS.AR.225(a) to ensure effective implementation of corrective actions;	Compliance monitoring activities including the planning and the execution of independent audits
(a)(9): protects the confidentiality of any information that the competent authority may have related to organisations subject to its oversight and the information received through the organisation's external reporting schemes established in accordance with point IS.I.OR.230 of Annex II (Part-IS.I.OR) to this Regulation and point IS.D.OR.230 of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645;	Define, develop and implement solutions to protect the confidentiality of any information.
(a)(10): notifies the Agency of changes that affect the capacity of the competent authority to perform its tasks and discharge its responsibilities as defined in this Regulation;	Not applicable
(a)(11): defines and implements procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other competent authorities and agencies, as well as organisations subject to this Regulation, to conduct effective information security risk assessments relating to their activities.	Not applicable
(b): In order to continuously meet the requirements referred to in Article 1, the competent authority shall implement a continuous improvement process in accordance with point IS.AR.235.	Execute independent effectiveness and maturity assessments. Define, develop and implement the necessary improvement measures.
(c): The competent authority shall document all key processes, procedures, roles and responsibilities required to comply with point IS.AR.200(a) and establish a process for amending this documentation.	Production of documentation to detail all key processes, procedures, roles and responsibilities required to comply with point IS.AR.200(a) (e.g. information security policies, general description of the staff, procedures to specify compliance). Define, develop and implement processes for approving amendments and changes.

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

(a) OVERSIGHT OF THE CONTRACTED ORGANISATION

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

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

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

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

(ii) definition of the roles and responsibilities of the parties (i.e. competent authority and contracted organisation);

(iii) definition and review of KPIs;

(iv) reaction to deviation from contractual obligations;

(v) performance of compliance audits, according to 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 competent authority and to the contracted organisation, and response to findings. The feedback on the outcome of the compliance audits within the competent authority should reach the person of the competent authority as identified in IS.AR.225(a) 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 competent authority 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 competent authority 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 competent authority and the contracted organisation.

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

GM1 IS.AR.220 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 competent authority, 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 authority that are applicable to the contracted organisation;

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

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

This agreed risk assessment should also consider the roles and responsibilities of the parties (i.e. competent authority and contracted organisation) as well as their interfaces.

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

AUDIT OF CONTRACTED ORGANISATIONS

The following aspects should be considered by the authority when auditing a supplier contracted to perform 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 Part-IS contracted activities;

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

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

GM1 IS.AR.225 Personnel requirements

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

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

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

AMC1 IS.AR.225(a) Personnel requirements

The person referred to in point IS.AR.225(a) is normally intended to be a manager in the authority who, by virtue of his or her position, has overall responsibility for information security management and has sufficient authority to plan and allocate the relevant budgetary resources and initiatives in

accordance with the financial control model of the Member State. This person is not necessarily required to be knowledgeable on technical matters; however, he or she should be aware of the overarching objectives of this Regulation and its implications for the authority. The authority should make sure that this person has direct access to the highest-ranking executive in the authority and has the necessary funding allocation for the activities under this Regulation.

GM1 IS.AR.225(a) Personnel requirements

The person referred to in point IS.AR.225 (a) should be capable of managing the authority's information security strategy and its implementation to ensure the achievement of the objectives described in Article 1. According to the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022, this person may be described for instance as: (Chief) Information Security Officer, Cybersecurity Programme Director or Information Security Manager. However, it should be noticed that these descriptions and the related skills do not consider the aviation safety perspective that is required in Article 1.

AMC1 IS.AR.225(b) 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 authority.

GM1 IS.AR.225(b) Personnel requirements

SUFFICIENT PERSONNEL

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

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

AMC1 IS.AR.225(c) Personnel requirements

NECESSARY COMPETENCE

(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

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

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

(2) align the personnel qualifications and experience to the expected competence 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 IS.AR.225(c) Personnel requirements

NECESSARY COMPETENCE AND TRAINING PROGRAMME

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

In order to develop the list of competencies, a competent authority 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 and 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 authority's needs considering the size, scope, required competencies, and complexity of the organisation.

The competent authority may also identify professional certification schemes that cover a number of necessary competencies; therefore, it may decide to recognise these certifications as sufficient to cover the establishment of proper qualifications and experience for the certified personnel.

Finally, as information security/cybersecurity evolves due to the rise of new threats, the authority should periodically review the adequacy of the training programme.

AMC1 IS.AR.225(d) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

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

As part of this, 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 IS.AR.225(d) Personnel requirements

ACKNOWLEDGEMENT OF RESPONSIBILITIES

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

AMC1 IS.AR.225(e) Personnel requirements

IDENTITY AND TRUSTWORTHINESS

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

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

GM1 IS.AR.225(e) 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.

Note: The absence of criminal record may be verified by means of a certificate issued by the responsible authority in the Member State in accordance with Regulation (EU) 2016/1191. In the case of prospective foreign employees, the above checks may be carried out on the basis of equivalent certificates issued by the country of origin, such as a 'certificate of good 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 IS.AR.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 above 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) Competent authorities may also be subject to Regulation (EU) 2015/1998 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 considered suitable for the establishment of the personnel's identity and trustworthiness required under Part-IS, in relation to their role, the process and the relevant criteria defined in Regulation (EU) 2015/1998 for standard and enhanced background checks. However, it should be noted that compliance with the provisions for the establishment of identity and trustworthiness under Part-IS does not constitute compliance with the provisions on background checks as defined in Regulation (EU) 2015/1998.

GM1 IS.AR.230 Record-keeping

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

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

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

(a) manage relevant information 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 requirement (a)(4) has been met.

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

The objective of the requirement (a)(1)(iv) is to ensure detection of possible indication of 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)(4) 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 within the scope of the detection activities under IS.AR.215(a), as well as other information security data produced by assets that have been identified under IS.AR.205.

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

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

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

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

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

(b) Records data integrity, 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 IS.AR.230(c)&(d) Record-keeping

RECORDS ACCESSIBILITY THROUGHOUT THE RETENTION PERIOD

It is recommended to follow best practices for data retention, 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.).

AMC1 IS.AR.235 Continuous improvement

The continuous improvement process (CIP), as required by IS.AR.200(b), should aim to continuously improve the effectiveness, suitability and adequacy of the ISMS. This should be achieved by a proactive and systematic assessment of the ISMS and all 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) above, planning, development and implementation of actions and changes to the ISMS, its processes or elements to achieve the improvements.

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

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

GM1 IS.AR.235 Continuous improvement

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

In this Regulation:

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

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

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

The context and risk environment of competent authorities are never static and therefore require a dynamic adaptation, evolution and change of the competent authority'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 competent authority which needs to be continuously monitored and improved to ensure alignment with the competent authority'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 competent authority may integrate the Part-IS CIP in some other already operated CIP and may apply methods such as Plan-Do-Check-Act (PDCA) Cycle or Define-Measure-Analyse-Improve-Control (DMAIC) (see also GM1 IS.AR.200).

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

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

— **Adequacy** refers to whether the system 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, including failures, are managed to fulfil or correctly implement a requirement or control.

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

Identification of improvement opportunities

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

Suggestions for improvements stem from sources including:

— Risk management: the results of regularly conducted risk analyses and the subsequent risk treatment are a primary factor in improving the ISMS, 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 information security incident detection, handling and response process and a potential treatment of a root cause

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

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

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

Any outcome of this process should be documented. The resulting actions may be integrated into an overarching action plan which is centrally consolidated and periodically reviewed according to the relevant policies. The resulting action plan may be further divided into a tactical, short-/mid-term action plan and a strategic, long-term action plan.

AMC1 IS.AR.235(a) Continuous improvement

(a) **ISMS EFFECTIVENESS EVALUATION**

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

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

(2) when the above steps should be performed;

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

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

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

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

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

performance targets.

(b) **ISMS MATURITY ASSESSMENT**

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

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

(2) for each assessed process or capability, ensure that the model defines criteria 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 competent authority should:

(1) evaluate and justify the current maturity level;

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

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

GM1 IS.AR.235(a) Continuous improvement

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

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

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

(3) the incident and vulnerability management;

(4) the personnel competence management.

(b) Existing maturity models for ISMS maturity evaluation

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

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

— Systems Security Engineering – Capability Maturity Model (SSE-CMM): published by ISO as ISO 21827 in 2008. It focuses on engineering practices, much less on operational practices that are split in 11 ‘Security Base Practices’, and 11 ‘Project and Organizational

Base Practices'. It introduces the notion of five Capability Levels, from 'Performed Informally' to 'Continuously Improving'.

— NIST Cybersecurity Framework (NIST 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, entities will determine which requirements of which models have already been met (mandatory) and can opt to reach a level that is beneficial to the competent authority (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 competent authority.

AMC1 IS.AR.235(b) Continuous improvement

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

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

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

(b) deciding on the need for, and the implementation of, corrective actions to eliminate the cause(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 person identified in IS.AR.225(a) and, as necessary, with other involved or affected roles and parties;

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

GM1 IS.AR.235(b) Continuous improvement

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

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

(a) identifying the extent, impact, context and triggers of the deficiency, evaluating it according to some established criteria, analysing potential consequences 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 AMC1 IS.AR.235(b);

(f) reporting to and reviewing the outcomes of the process steps with the management (see point (d) of AMC1 IS.AR.235(b));

(g) documenting and evidencing the result of the process steps above (see point (e) of AMC1 IS.AR.235(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 prevent 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: Aircraft operator, 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 safety-critical 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-in-the middle attacks

— threat (confidentiality): functional models, information and data that are embedded in training systems or training devices are accessed by insider or external threats

— **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: National competent authority's NOTAM system and associated infrastructure

- **Threat vector assets/domain**
  - National NOTAM system infrastructure and digital interface
  - Supply chain for NOTAM system maintenance and updates
  - National competent authority's 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: Aviation authority's airworthiness directive (AD) system and associated infrastructure

— **Threat vector assets/domain**

— EASA AD system infrastructure and digital interface

— supply chain for AD system maintenance and updates

— EASA 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 Part-IS, including mapping to NIST CSF 1.1 competencies and ISO/IEC 27001 clauses and controls

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	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	IS.AR.200(a)	IDENTIFY	ID.RM	4 6.1.1		
Establish the scope of the ISMS according to Part-IS requirements	Management	IS.AR.205(a)	IDENTIFY	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implement and maintain an information security policy	Management	IS.AR.200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1	A5.1
Identify and review information security risks	Management	IS.AR.200(a)(2) IS.AR.205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implement security risk treatment measures	Management	IS.AR.200(a)(3) IS.AR.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	IS.AR.200(a)(4) IS.AR.215	DETECT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7	A7.2 A8.15 A5.28
Monitor compliance with this Regulation and report findings to top management	Operational	IS.AR.200(a)(8)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Protect confidentiality of exchanged information	Operational	IS.AR.200(a)(9)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14
Communicate to the Agency changes regarding capability and responsibilities	Operational	IS.AR.200(a)(10)				A6.1.3	A5.5
Share information to assist other competent	Operational	IS.AR.200(a)(11)	IDENTIFY	ID.RA-2 ID.BE-2		A6.1.4	A5.6

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
authorities, agencies and organisations			PROTECT	PR.IP-8			
			RESPOND	RS.CO-3 RS.CO-5			
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.AR.200(b) IS.AR.235	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	IS.AR.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	IS.AR.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	IS.AR.205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		
Identify information security risks and assign a risk level	Management	IS.AR.205(c)	IDENTIFY	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2		
Review and update the risk assessment based on certain criteria	Operational	IS.AR.205(d)	IDENTIFY	ID.RM	8.2		A5.7

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.AR.210(a)	PROTECT	PR.IP PR.PT	6.1.3 8.3		
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.AR.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			
			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	IS.AR.215(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 a security incident	Operational	IS.AR.215(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5	A5.26
Implement measures to recover from information security incidents	Operational	IS.AR.215(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	IS.AR.220	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Define a person with the authority to establish and maintain the organisational structures, policies, processes, and procedures necessary to implement this Regulation	Management	IS.AR.225(a)	IDENTIFY	ID.AM-6	7.1	A6.1.1	A5.2

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.AR.225(b)	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 necessary competence for activities regarding information security management	Management	IS.AR.225(c)	IDENTIFY	ID.AM-5 ID.AM-6	7.2	A7.2.2	A6.3
			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	IS.AR.225(d)	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	IS.AR.225(e)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
Archive, protect and retain records traceability for a specified time	Operational	IS.AR.230	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			
			RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5			
			RECOVER	RC.CO-3			

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.AR.235(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 implemented measures of the ISMS elements.	Operational	IS.AR.235(b)			10	A5.1.2	A5.1

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)