European Union Aviation Safety Agency

Notice of Proposed Amendment 2025-101(B)

in accordance with Article 6 of MB Decision 01-2022

Proposed GM to Regulations (EU) 2023/203 and 2022/1645 (Part-IS regulatory package)

Table of contents

Proposed amendments 4

Amendments to the AMC and GM to the Articles of Commission Implementing Regulation (EU) 2023/203 4

GM1 Article 5(1) — Requirements arising from other Union legislation 4
GM1 Article 5(2) — Requirements arising from other Union legislation 4
GM1 Article 6(2) — Competent authority 5

Amendments to the AMC and GM to the Articles of Commission Delegated Regulation (EU) 2022/1645 6

GM1 Article 4(1) — Requirements arising from other Union legislation 6
GM1 Article 4(2) — Requirements arising from other Union legislation 6
GM1 Article 5(2) — Competent authority 6

Amendments to the AMC and GM to Part-IS.AR of Commission Implementing Regulation (EU) 2023/203 8

GM1 IS.AR.200 Information security management system (ISMS) 8
GM1 IS.AR.225(c) Personnel requirements 10
GM1 IS.AR.235 Continuous improvement 11

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~ 11

Appendix III — Examples of aviation services and interfaces 11

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences 11

Appendix V — Proportionality considerations related to indicators of complexity 11

Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF) 12

Amendments to the AMC and GM to Part-IS.I.OR of Commission Implementing Regulation (EU) 2023/203 12

GM1 IS.I.OR.200 Information security management system (ISMS) 12
GM1 IS.I.OR.200(d) Information security management system (ISMS) 14
GM1 IS.I.OR.200(e) Information security management system (ISMS) 15
GM1 IS.I.OR.210 Information security risk treatment 16
GM1 IS.I.OR.240(g) Personnel requirements 17
GM1 IS.I.OR.245 Record-keeping 18
GM2 IS.I.OR.255 Changes to the information security management system 18
GM1 IS.I.OR.260 Continuous improvement 18

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~ 19

Appendix III — Examples of aviation services and interfaces 19

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences 19

Appendix V — Proportionality considerations related to indicators of complexity. 19

Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF)...... 19

Amendments to the AMC and GM to Part-IS.D.OR of Commission Delegated Regulation (EU) 2022/1645.. 20

GM1 IS.D.OR.200 Information security management system (ISMS) 20
GM1 IS.D.OR.200(d) Information security management system (ISMS)..................... 22
GM1 IS.D.OR.200(e) Information security management system (ISMS)..................... 23
GM1 IS.D.OR.210 Information security risk treatment... 24
GM1 IS.D.OR.240(g) Personnel requirements... 25
GM1 IS.D.OR.245 Record-keeping.. 26
GM2 IS.D.OR.255 Changes to the information security management system 26
GM1 IS.D.OR.260 Continuous improvement.. 26

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~ 27

Appendix III — Examples of aviation services and interfaces 38

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences 43

Appendix V — Proportionality considerations related to indicators of complexity 70

Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF)...... 75

Proposed amendments

The amendments are arranged as follows to show deleted, new and unchanged text:

— deleted text is ~~struck through~~;

— new text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

Where necessary, the rationale is provided in *italics.*

Amendments to the AMC and GM to the Articles of Commission Implementing Regulation (EU) 2023/203

GM1 Article 5(1) — Requirements arising from other Union legislation

Pursuant to Article 44 of Directive (EU) 2022/2555 (the NIS 2 Directive), the previous Directive (EU) 2016/1148 (the NIS Directive) was repealed with effect from 18 October 2024. In accordance with the NIS 2 Directive, references to the repealed Directive shall be construed as references to Directive (EU) 2022/2555 and shall be read in accordance with the correlation table set out in Annex III.

In accordance with this table, references to Article 14 of Directive (EU) 2016/1148 shall be now read as references to Article 21 and Article 23 of Directive (EU) 2022/2555. For an exact correlation, please refer to Annex III to Directive (EU) 2022/2555.

For legal certainty, the equivalence of any requirements should be assessed against the requirements of the national legislation transposing Directive (EU) 2022/2555.

When assessing the equivalence established between the requirements laid down in Regulation (EU) 2023/203 and Directive (EU) 2022/2555, organisations should consider the following:

— The equivalence between Regulation (EU) 2023/203 and Directive (EU) 2022/2555 requirements should be assessed in terms of which requirements can be deemed as equivalent.

— Possible differences in the perimeter of applicability of the rules, in particular as regards the elements that are within the scope under the two different frameworks.

GM1 Article 5(2) — Requirements arising from other Union legislation

Notwithstanding the equivalence between the provisions in Regulation (EU) 2023/203 and the cybersecurity requirements contained in point 1.7 of the Annex to Regulation (EU) 2015/1998, in order to ensure effective management of safety consequences by leveraging the requirements of Regulation

(EU) 2015/1998, organisations need to consider the differences in the scope of the rules in terms of which elements are covered under the two different regulatory frameworks.

GM1 Article 6(2) — Competent authority

The applicability of Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 to competent authorities is specified in Article 4(2) and called for under the authority requirements for a management system in the implementing or delegated acts for each domain. Therefore, the Part-IS.AR requirements apply to the competent authority under Article 6(1) irrespective of the allocation of roles and responsibilities to an independent and autonomous entity designated by the State under Article 6(2).

At the same time, this independent and autonomous entity designated by the State is not subject to the Part-IS.AR requirements; this entity has only to fulfil the responsibilities for certifying and overseeing organisations' compliance with Implementing Regulation (EU) 2023/203.

Amendments to the AMC and GM to the Articles of Commission Delegated Regulation (EU) 2022/1645

GM1 Article 4(1) — Requirements arising from other Union legislation

Pursuant to Article 44 of Directive (EU) 2022/2555 (the NIS 2 Directive), the previous Directive (EU) 2016/1148 (the NIS Directive) was repealed with effect from 18 October 2024. In accordance with the NIS2 Directive, references to the repealed Directive shall be construed as references to Directive (EU) 2022/2555 and shall be read in accordance with the correlation table set out in Annex III.

In accordance with this table, references to Article 14 of Directive (EU) 2016/1148 shall be now read as references to Article 21 and Article 23 of Directive (EU) 2022/2555. For an exact correlation, please refer to Annex III to Directive (EU) 2022/2555.

For legal certainty, the equivalence of any requirements should be assessed against the requirements of the national legislation transposing Directive (EU) 2022/2555.

When assessing the equivalency established between the requirements laid down in Regulation (EU) 2022/1645 and Directive (EU) 2022/2555, organisations should consider the following:

— The equivalence between Regulation (EU) 2022/1645 and Directive (EU) 2022/2555 requirements should be assessed in terms of which requirements can be deemed as equivalent.

— Possible differences in the perimeter of applicability of the rules, in particular as regards the elements that are within the scope under the two different frameworks.

GM1 Article 4(2) — Requirements arising from other Union legislation

Notwithstanding the equivalence between the provisions in Regulation (EU) 2022/1645 and the cybersecurity requirements contained in point 1.7 of the Annex to Regulation (EU) 2015/1998, in order to ensure effective management of safety consequences by leveraging the requirements of Regulation (EU) 2015/1998, organisations need to consider the differences in the scope of the rules in terms of which elements are covered under the two different regulatory frameworks.

GM1 Article 5(2) — Competent authority

The applicability of Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 to competent authorities is specified in its Article 4(2) and called for under the authority requirements for a management system in the implementing or delegated act for each domain. Therefore, the Part-IS.AR requirements apply to the competent authority under Article 5(1) irrespective of the allocation of roles and responsibilities to an independent and autonomous entity designated by the State under Article 5(2).

At the same time, this independent and autonomous entity designated by the State is not subject to the Part-IS.AR requirements; this entity has only to fulfil the responsibilities for certifying and overseeing organisations’ compliance with Implementing Regulation (EU) 2023/203.

Amendments to the AMC and GM to Part-IS.AR of Commission Implementing Regulation (EU) 2023/203

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

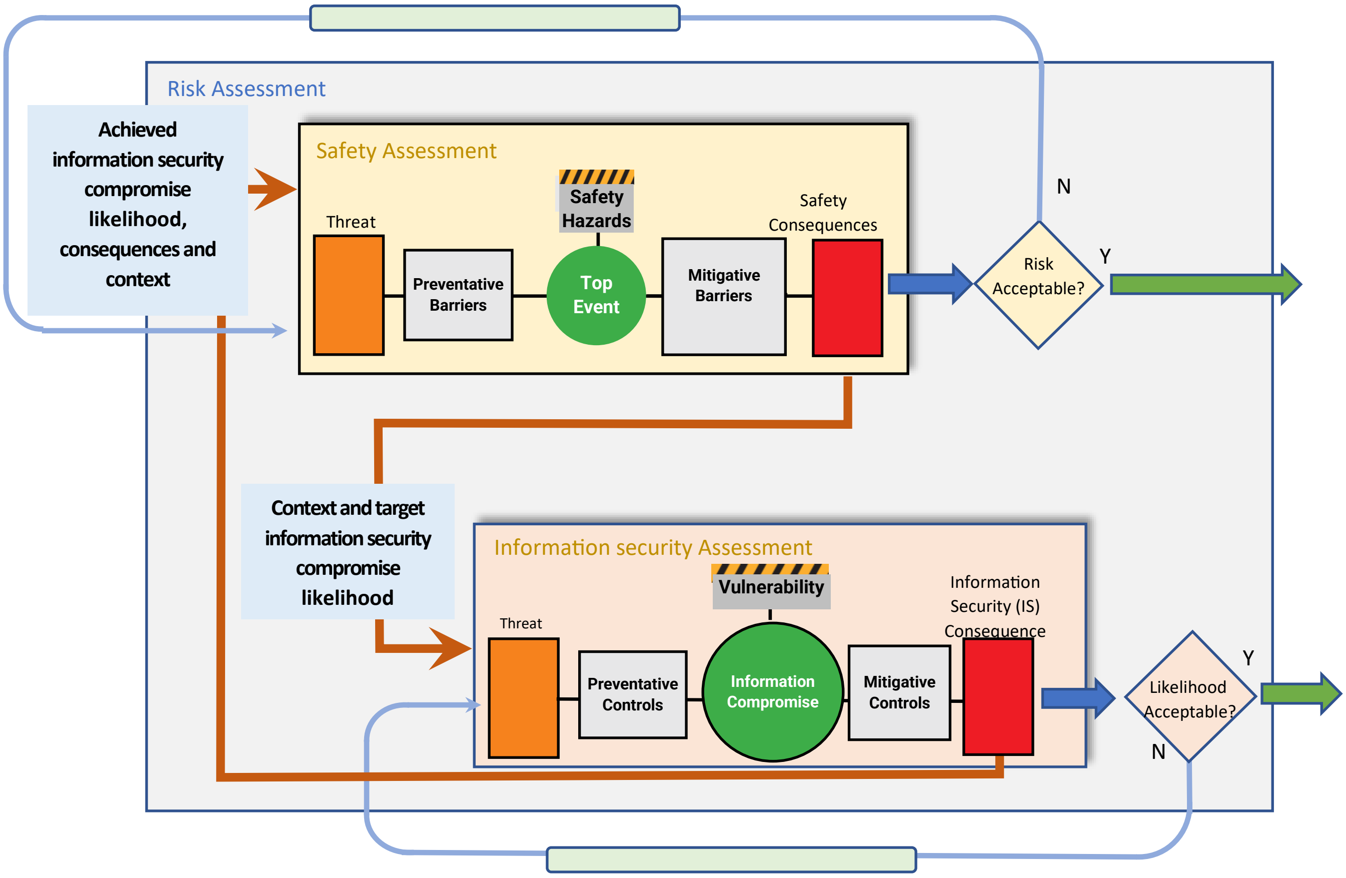
An **information security management system (ISMS)** is a systematic approach to establish, implement, operate, monitor, review, maintain and continuously improve the state of information security of an organisation. Its objective is to protect the information assets, such that the operational and safety 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~~ influence 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 overall risk assessment should consider safety consequences influenced by information security risks, which may emerge as threats, hazards, escalation factors weakening barriers, or direct triggers of existing hazards. When conducting this assessment, 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.

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. The below Figure 1 from ICAO Doc 10204 ‘Manual on Aviation Information Security’ illustrates these interactions.



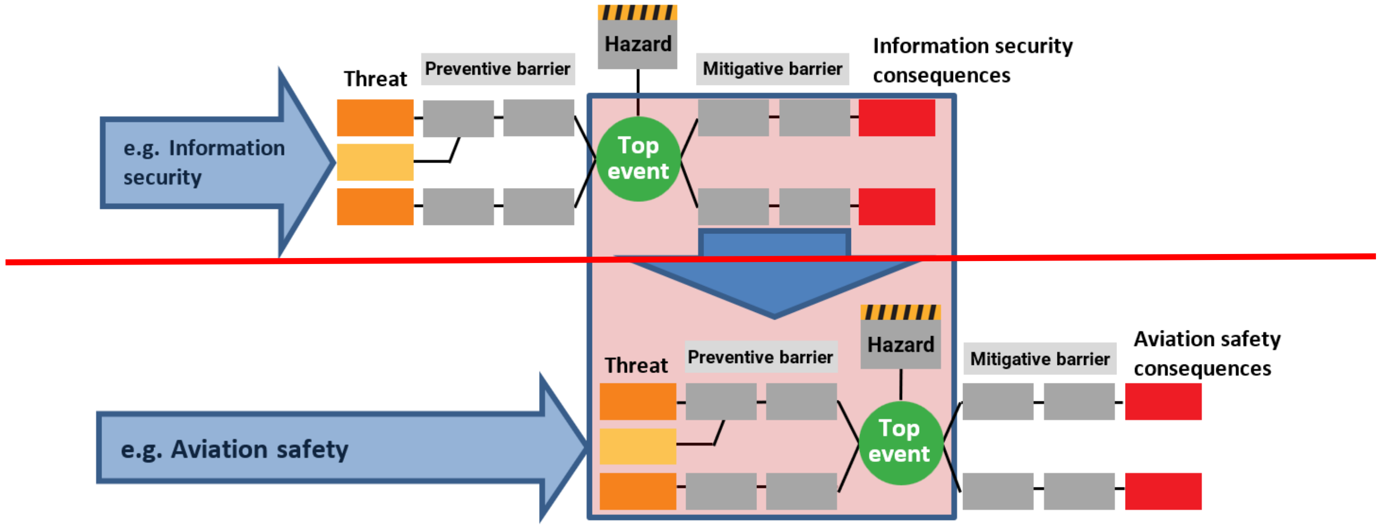


Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

Note: In the drawing, the term ‘context’ in the communication between the safety assessment process (SAP) and the information security assessment process (ISAP) carries slightly different notions, which need to be understood and distinguished.

In order to satisfy the safety requirements, the SAP will provide context information, such as the architecture and functional descriptions of the items within the scope, including those related to the barriers; all identified relevant safety hazards; the top events and their relations (e.g. triggers) to those hazards. In addition to context information, it provides target information security compromise likelihood. While this value is commensurate with the safety objectives related to the severity of the safety consequence, it needs to be amended by information about the level of uncertainty that is expected to be achieved in order to be able to adequately rely on the results of the ISAP.

In turn, the ISAP will return context information, such as modification to the architecture and functional descriptions of the items modified or added, whether those were safety barriers or other items; additional threats; potentially additional safety hazards; additional direct triggers of hazards; or additional escalating factures affecting barriers. In addition to context information, it provides achieved information security compromise likelihood. While this value is commensurate with the safety objectives as requested by the SAP, it shall be also amended by information about the level of uncertainty that has been achieved, as requested by the SAP.

[…]

PART-IS versus ISO/IEC 27001 cross reference table

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

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, an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the European e-Competence Framework (e-CF 4.0) or the NICE 2.0 (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 EU e-CF or, for ease of mapping, to the functions and categories of the NIST CSF. This mapping may be used to establish a baseline to identify the aforementioned competence gaps. However, it should be noticed that existing cybersecurity/information security competence frameworks ~~such as the NICE~~ typically focus primarily on the protection of standard information technologies; therefore, the proposed list of competencies may need to be adapted to the technologies or integrated with processes used in the organisation.

[…]

GM1 IS.AR.235 Continuous improvement

[…]

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

[…]

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~

See Appendix II in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix III — Examples of aviation services and interfaces

See Appendix III in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences

See Appendix IV in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix V — Proportionality considerations related to indicators of complexity

See Appendix V in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF)

See Appendix VI in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Amendments to the AMC and GM to Part-IS.I.OR of Commission Implementing Regulation (EU) 2023/203

GM1 IS.I.OR.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~~ influence 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 overall risk assessment should consider safety consequences influenced by information security risks, which may emerge as threats, hazards, escalation factors weakening barriers, or direct triggers of existing hazards. When conducting this assessment, 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.

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. The below Figure 1 from ICAO Doc 10204 'Manual on Aviation Information Security' illustrates these interactions.

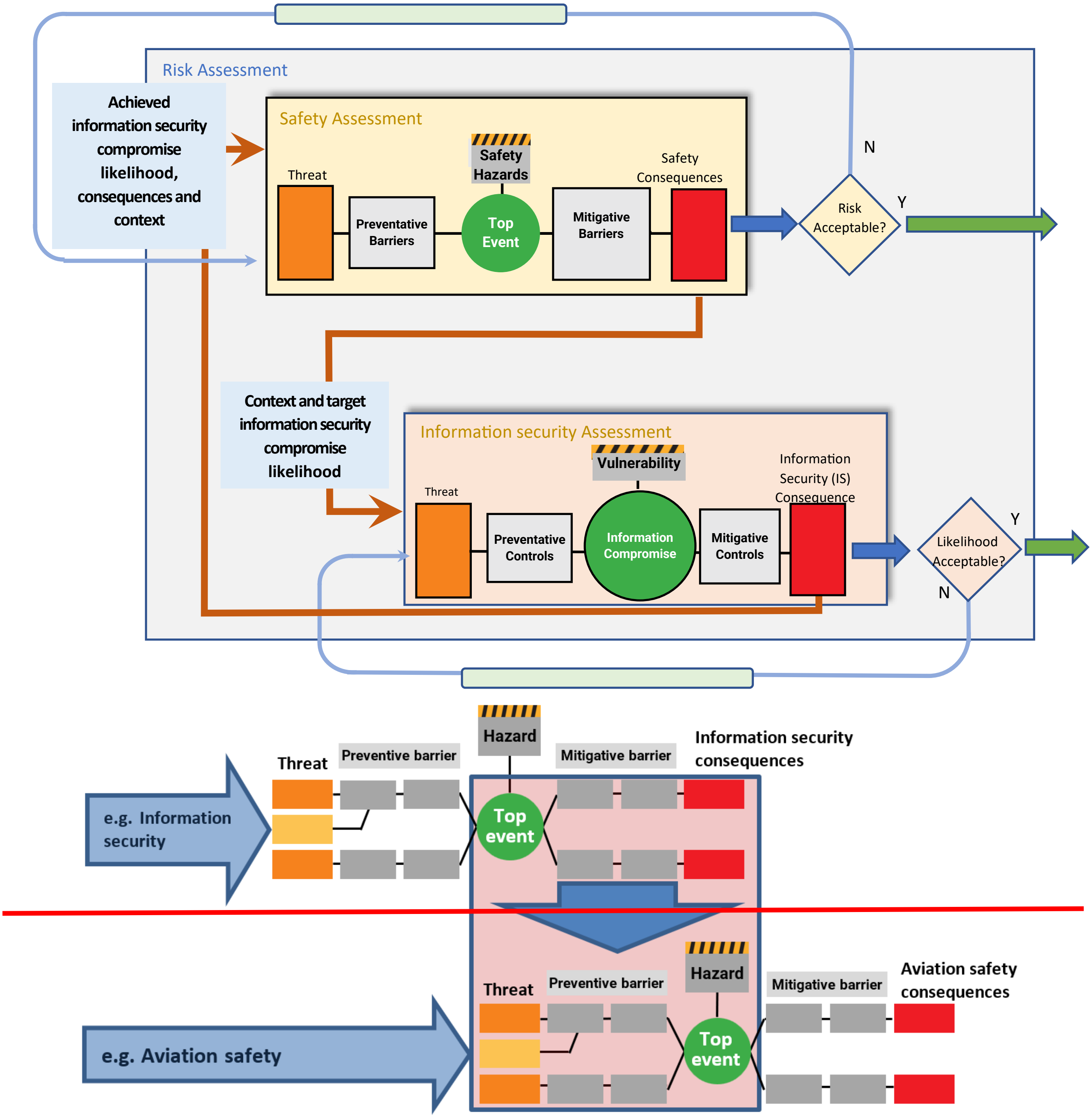


Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

Note: In the drawing, the term ‘context’ in the communication between the safety assessment process (SAP) and the information security assessment Process (ISAP) carries slightly different notions, which need to be understood and distinguished.

In order to satisfy the safety requirements, the SAP will provide context information, such as the architecture and functional descriptions of the items within the scope, including those related to the barriers; all identified relevant safety hazards; the top events and their relations (e.g. triggers) to those hazards. In addition to context information, it provides target information security compromise likelihood. While this value is commensurate with the safety objectives related to the severity of the safety consequence, it needs to be amended by information about the level of uncertainty that is expected to be achieved in order to be able to adequately rely on the results of the ISAP.

In turn, the ISAP will return context information, such as modification to the architecture and functional descriptions of the items modified or added, whether those were safety barriers or other items; additional threats; potentially additional safety hazards; additional direct triggers of hazards; or additional escalating factures affecting barriers. In addition to context information, it provides achieved information security compromise likelihood. While this value is commensurate with the safety objectives as requested by the SAP, it shall be also amended by information about the level of uncertainty that has been achieved, as requested by the SAP.

[...]

PART-IS versus ISO/IEC 27001 cross reference table

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

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

PROPORTIONALITY IN ISMS IMPLEMENTATION

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

As a general guide, the following indicators of information security complexity could be used. Each of them influences certain aspects of appropriate ISMS implementation:

(a) Where the organisation is placed in the functional chain and the number and safety relevance of the interfacing organisations/stakeholders.

(b) The complexity of the organisational structure and hierarchies (e.g. number of staff, departments, hierarchical layers, etc.)

(c) The complexity of the information and communication technology systems and data used by the organisation and their connection to external parties.

More details on the influence on the proportionate implementation of Part-IS for each complexity indicator are provided in Appendix V.

[...]

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

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority following the procedure outlined in AMC1 IS.I.OR.200(e).

Consideration of safety risks arising from information security threats can build on existing safety risk assessments; for example, those carried out as part of the SMS.

APPLICATION FOR A DEROGATION

In order to ensure a consistent approach by organisations when submitting a derogation request, the competent authority may have established an official derogation request application form.

The application for a derogation, based on the application form where one exists or in a format decided by the organisation, will need to be signed by the accountable manager of the applicant organisation and submitted to the appropriate competent authority for review and consideration.

The application for a derogation should contain preliminary information used for a pre-assessment by the competent authority, including:

- Company information and contact information;
- Affected approval(s);
- Detailed justification for the exclusion of the provisions;
- Overview of services that the organisation provides and receives;
- Architecture overview of information systems used for business operation;
- Summary of the initial information security risk assessment aligned with the above architecture;
- Methodology used to perform the information security risk assessment;
- List of people and roles involved in the information security risk assessment process;
- Date and signature.

EVALUATION OF THE REQUEST FOR A DEROGATION

The information security risk assessment and other supporting documentation is normally reviewed by the competent authority to assess whether:

- the documentation is sufficient for a proper analysis and assessment;
- the repository of digital systems, data flows and processes is comprehensive;
- the information security risk assessment has been conducted in accordance with the organisation’s methodology and with the appropriate diligence;
- the relevant stakeholders have been involved in the assessment process;
- the assessment has been performed by people with sufficient expertise in information security and aviation safety;

- the organisation has assigned and indicated a point of contact for enquiries.

EXPECTATIONS AND RECOMMENDATION AFTER DEROGATION APPROVAL

Once a derogation approval has been granted, the organisation is expected to undertake the following on a continuous basis:

- Comply with all provisions of the regulation which are not exempted, in particular:
  - IS.I.OR.200(a)(13) which should not be limited to only protection of the received information. When transmitting information with confidential nature, the organisation needs to have secure means in place as well;
  - IS.I.OR.205(d) as the risk picture may vary due to changes in the safety and security environment over time;
  - IS.I.OR.240(a)(3) because at least someone in the organisation needs to have a basic understanding of the Regulation.
- Continuously monitor any changes in the organisation's scope of work and identify those which may have a potential impact on the documented information, which supports the derogation approval. Where such changes are identified, the organisation should ensure that they are brought to the attention of the competent authority without delay and notified in accordance with the applicable implementing rule.
- Ensure that the accountable manager or the head of the design of the organisation can demonstrate an understanding of the derogation process and the terms on which the approval has been granted.
- Implement basic protection against information security risks according to industry best practices.
- To consult the respective national cybersecurity body for additional guidance.

[...]

GM1 IS.I.OR.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 organisation ~~should~~ can 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~~ includes 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~~ includes a prioritisation of risks, the corresponding information on the objectives and means for risk treatment to reach an acceptable level of risk, as well as agreed timelines specifying when responsible personnel should have implemented the risk treatment measures. The timelines for the implementation of a risk treatment measure ~~should be agreed~~ are subject to agreement by the personnel responsible for the implementation and ~~should be~~ are communicated to and accepted by the accountable manager of the organisation or delegated person(s).

Any subsequent implementation delay, together with its cause, reason, rationale or necessity, ~~should be~~ is documented in the risk treatment plan, for risks that may lead to an unsafe condition. ~~The updated risk treatment should be communicated to the competent authority in case the materialisation of risk would lead to an unsafe condition.~~

[…]

GM1 IS.I.OR.240(g) Personnel requirements

NECESSARY COMPETENCE AND TRAINING PROGRAMME

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

In order to develop the list of competencies, an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the European e-Competence Framework (e-CF 4.0) or the NICE 2.0 (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 EU e-CF or, for ease of mapping, to the functions and categories of the NIST CSF. This mapping may be used to establish a baseline to identify the aforementioned competence gaps. However, it should be noticed that existing cybersecurity/information security competence frameworks ~~such as the NICE~~ typically focus primarily on the protection of standard information technologies; therefore, the proposed list of competencies may need to be adapted to the technologies or integrated with processes used in the organisation.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the organisation’s needs considering the size, scope, required competencies, and complexity of the organisation.

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

ROLE-BASED COMPETENCE FRAMEWORK

Although under this Regulation there are no provisions for specific roles, besides the optional nomination of a CRP, for organisations characterised by a large number of staff members and hierarchical layers, it may be convenient to identify some roles and the related required competencies. To this end, EASA has developed an adaptation of the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022 that can be found in the Appendix VI.

GM1 IS.I.OR.245 Record-keeping

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

The 'approval received' referred to in point (a)(1)(i) refers to any derogation that has been granted by the competent authority under IS.I.OR.200(e). ~~includes any 'certificate' received by the organisation when it is provided for by the implementing rule for its domain.~~

GM2 IS.I.OR.255 Changes to the information security management system

[…]

(c) Changes to ~~the methodology used for~~ risk management:

— The organisation changes the classification for likelihood or impact in their risk management methodology e.g. to obtain more granularity.

— The organisation implements changes to their risk treatment methodology.

— The organisation delays the implementation of risk treatment measures which may potentially lead to an unsafe condition and documents this in their risk treatment plan.

— The organisation integrates its information security risk management into existing management systems.

GM1 IS.I.OR.260 Continuous improvement

[...]

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

[...]

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~

See Appendix II in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix III — Examples of aviation services and interfaces

See Appendix III in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences

See Appendix IV in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix V — Proportionality considerations related to indicators of complexity.

See Appendix V in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF)

See Appendix VI in the following amendment to the AMC & GM to Commission Delegated Regulation (EU) 2022/1645

Amendments to the AMC and GM to Part-IS.D.OR of Commission Delegated Regulation (EU) 2022/1645

GM1 IS.D.OR.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~~ influence 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) 2022/1645. 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 overall risk assessment should consider safety consequences influenced by information security risks, which may emerge as threats, hazards, escalation factors weakening barriers, or direct triggers of existing hazards. When conducting this assessment, 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.

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. The below Figure 1 from ICAO Doc 10204 ‘Manual on Aviation Information Security’ illustrates these interactions.

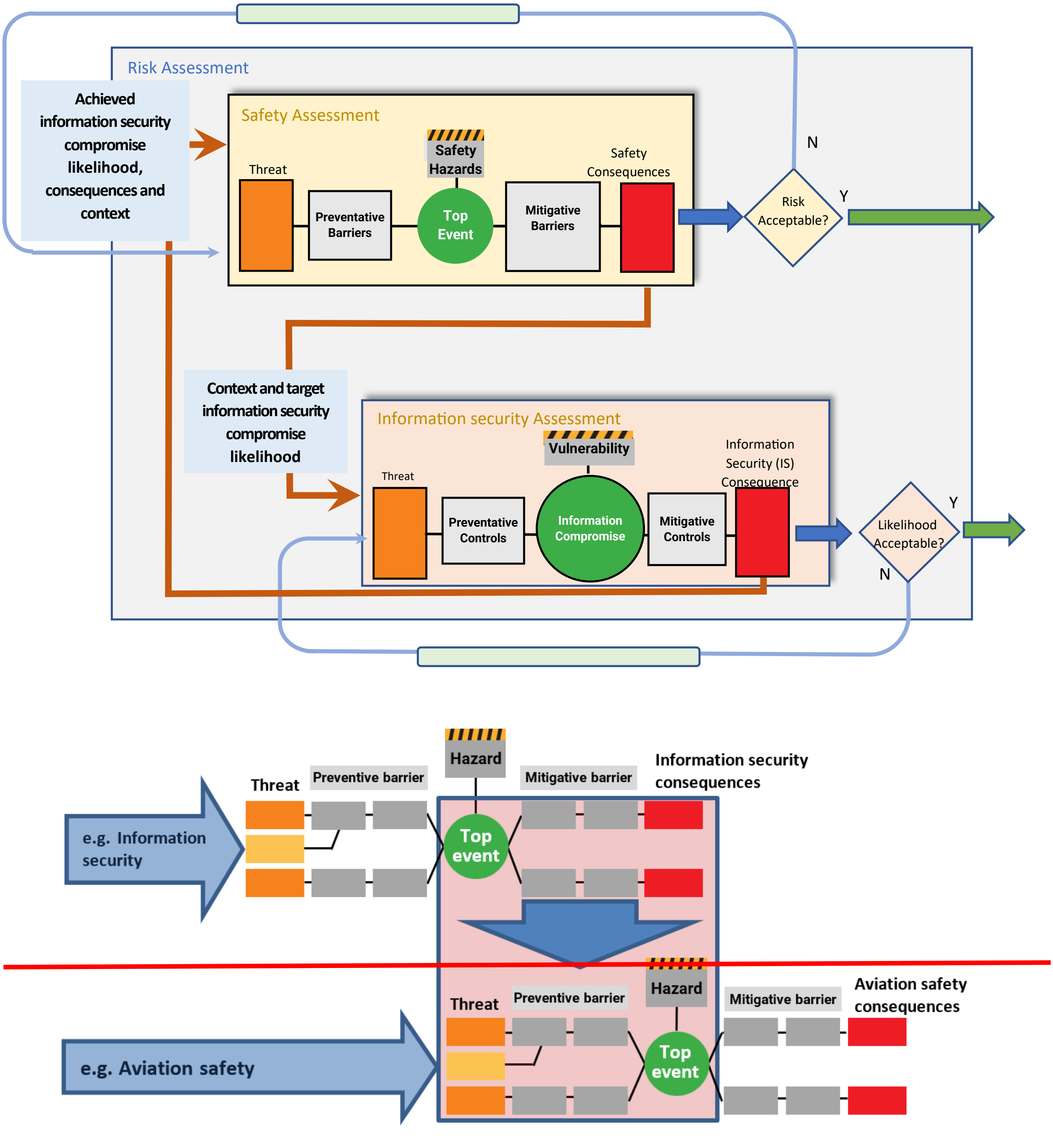


Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

Note: In the drawing, the term ‘context’ in the communication between the safety assessment process (SAP) and the information Security assessment process (ISAP) carries slightly different notions, which need to be understood and distinguished.

In order to satisfy the safety requirements, the SAP will provide context information, such as the architecture and functional descriptions of the items within the scope, including those related to the barriers; all identified relevant safety hazards; the top events and their relations (e.g. triggers) to those hazards. In addition to context information, it provides target information security compromise likelihood. While this value is commensurate with the safety objectives related to the severity of the safety consequence, it needs to be amended by information about the level of uncertainty that is expected to be achieved in order to be able to adequately rely on the results of the ISAP.

In turn, the ISAP will return context information, such as modification to the architecture and functional descriptions of the items modified or added, whether those were safety barriers or other items; additional threats; potentially additional safety hazards; additional direct triggers of hazards; or additional escalating factures affecting barriers. In addition to context information, it provides achieved information security compromise likelihood. While this value is commensurate with the safety objectives as requested by the SAP, it shall be also amended by information about the level of uncertainty that has been achieved, as requested by the SAP.

[...]

PART-IS versus ISO/IEC 27001 cross reference table

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

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

PROPORTIONALITY IN ISMS IMPLEMENTATION

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

As a general guide, the following indicators of information security complexity could be used. Each of them influences certain aspects of appropriate ISMS implementation:

(a) Where the organisation is placed in the functional chain and the number and safety relevance of the interfacing organisations/stakeholders.

(b) The complexity of the organisational structure and hierarchies (e.g. number of staff, departments, hierarchical layers, etc.)

(c) The complexity of the information and communication technology systems and data used by the organisation and their connection to external parties.

More details on the influence on the proportionate implementation of Part-IS for each complexity indicator are provided in Appendix V.

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

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority following the procedure outlined in AMC1 IS.D.OR.200(e).

Consideration of safety risks arising from information security threats can build on existing safety risk assessments; for example, those carried out as part of the SMS.

APPLICATION FOR A DEROGATION

In order to ensure a consistent approach by organisations when submitting a derogation request, the competent authority may have established an official derogation request application form.

The application for a derogation, based on the application form where one exists or in a format decided by the organisation, will need to be signed by the accountable manager or the head of the design organisation of the applicant organisation and submitted to the appropriate competent authority for review and consideration.

The application for a derogation should contain preliminary information used for a pre-assessment by the competent authority, including:

— Company information and contact information;

— Affected approval(s);

— Detailed justification for the exclusion of the provisions;

— Overview of services that the organisation provides and receives;

— Architecture overview of information systems used for business operation;

— Summary of the initial information security risk assessment aligned with the above architecture;

— Methodology used to perform the information security risk assessment;

— List of people and roles involved in the information security risk assessment process;

— Date and signature.

EVALUATION OF THE REQUEST FOR A DEROGATION

The information security risk assessment and other supporting documentation is normally reviewed by the competent authority to assess whether:

— the documentation is sufficient for a proper analysis and assessment;

— the repository of digital systems, data flows and processes is comprehensive;

— the information security risk assessment has been conducted in accordance with the organisation's methodology and the appropriate diligence;

— the relevant stakeholders have been involved in the assessment process;

— the assessment has been performed by people with sufficient expertise in information security and aviation safety;

— the organisation has assigned and indicated a point of contact for enquiries.

EXPECTATIONS AND RECOMMENDATION AFTER DEROGATION APPROVAL

Once a derogation approval has been granted, the organisation is expected to undertake the following on a continual basis:

— Comply with all provisions of the regulation which are not exempted, in particular:

  — IS.D.OR.200(a)(13) which should not be limited to only protection of the received information. When transmitting information with confidential nature, the organisation needs to have secure means in place as well;

  — IS.D.OR.205(d) as the risk picture may vary due to changes in the safety and security environment over time;

  — IS.I.OR.240(a)(3) because at least someone in the organisation needs to have a basic understanding of the Regulation.

— Continuously monitor any changes in the organisation’s scope of work and identify those which may have a potential impact on the documented information, which supports the derogation approval. Where such changes are identified, the organisation should ensure that they are brought to the attention of the competent authority without delay and notified in accordance with the applicable implementing rule.

— Ensure that the accountable manager or the head of the design of the organisation can demonstrate an understanding of the derogation process and the terms on which the approval has been granted.

— Implement basic protection against information security risks according to industry best practices.

— Consult the respective national cybersecurity body for additional guidance.

[…]

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

Unacceptable risks identified in accordance with point IS.D.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 organisation ~~should~~ can 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~~ includes 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~~ includes a prioritisation of risks, the corresponding information on the objectives and means for risk treatment to reach an acceptable level of risk, as well as agreed timelines specifying when responsible personnel should have implemented the risk treatment measures. The timelines for the implementation of a risk treatment measure ~~should be agreed~~ are subject to agreement by the personnel responsible for the implementation and ~~should be~~ are communicated to and accepted by the accountable manager by the accountable manager or, in the case of design organisations, by the head of the design organisation, of the organisation or delegated person(s).

Any subsequent implementation delay, together with its cause, reason, rationale or necessity, ~~should be~~ is documented in the risk treatment plan, for risks that may lead to an unsafe condition. ~~The updated risk treatment should be communicated to the competent authority in case the materialisation of risk would lead to an unsafe condition.~~ This person may condition such acceptance on the implementation or availability of compensating controls or reactive measures to monitor, early detect and timely respond to the materialisation of the risk in treatment. In order to timely respond, the incident response team may be informed to trigger their preparedness.

[…]

GM1 IS.D.OR.240(g) Personnel requirements

NECESSARY COMPETENCE AND TRAINING PROGRAMME

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

In order to develop the list of competencies, an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the European e-Competence Framework (e-CF 4.0) or the NICE 2.0 (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 EU e-CF or, for ease of mapping, to the functions and categories of the NIST CSF. This mapping may be used to establish a baseline to identify the aforementioned competence gaps. However, it should be noticed that existing cybersecurity/information security competence frameworks ~~such as the NICE~~ typically focus primarily on the protection of standard information technologies; therefore, the proposed list of competencies may need to be adapted to the technologies or integrated with processes used in the organisation.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the organisation's needs considering the size, scope, required competencies, and complexity of the organisation.

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

ROLE-BASED COMPETENCE FRAMEWORK

Although under this Regulation there are no provisions for specific roles, besides the optional nomination of a CRP, for organisations characterised by a large number of staff members and hierarchical layers it may be convenient to identify some roles and the related required competences. To this end EASA, has developed an adaptation of the European Cybersecurity Skills Framework (ECSF) published by ENISA in September 2022 that can be found in the Appendix VI.

GM1 IS.D.OR.245 Record-keeping

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

The 'approval received' referred to in point (a)(1)(i) refers to any derogation that has been granted by the competent authority under IS.D.OR.200(e). ~~includes any 'certificate' received by the organisation when it is provided for by the implementing rule for its domain.~~

GM2 IS.D.OR.255 Changes to the information security management system

[…]

(c) Changes to ~~the methodology used for~~ risk management:

- The organisation changes the classification for likelihood or impact in their risk management methodology e.g. to obtain more granularity.
- The organisation implements changes to their risk treatment methodology.
- The organisation delays the implementation of risk treatment measures which may potentially lead to an unsafe condition and documents this in their risk treatment plan.
- The organisation integrates its information security risk management into existing management systems.

GM1 IS.D.OR.260 Continuous improvement

[…]

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

[…]

Appendix II — Main tasks stemming from the implementation of Part-IS~~, including mapping~~ mapped to the EU e-CF and the NIST CSF ~~1.1~~ 2.0 ~~competencies and ISO/IEC 27001 clauses and controls~~

Part-IS main task	**Activity type**	**Reference**		
	Management, Operational	**Part-IS**	**EU e-CF**	**NIST CSF 2.0**
			Competence Areas & Skills	**Functions & Categories**
Establish and operate an information security management system (ISMS)	Management	IS.D.OR.200(a)	ISM (E.08)	GV.OP – IS Governance
Establish the scope of the ISMS in accordance with ~~according to~~ Part-IS requirements	Management	IS.D.OR.205(a)	ISM (E.08)	GV.RM – Risk Management
Implement and maintain an information security policy	Management	IS.D.OR.200(a)(1)	ISM (E.08)	GV.OP – IS Governance
Identify and review information security risks	Management	IS.D.OR.200(a)(2) IS.D.OR.205	ISM (E.08), Risk Management (E.02)	ID.RA – Risk Assessment
Implement information security risk treatment measures	Management	IS.D.OR.200(a)(3) IS.D.OR.210	ISM (E.08), Risk Management (E.02)	PR.IP – Information Protection Processes
Implement measures to detect information security events and identify those related to aviation safety	Management	IS.D.OR.200(a)(5) IS.D.OR.220	Incident Management (C.04)	DE.AE – Anomalies and Events
Implement measures that have been notified by the competent authority	Operational	IS.D.OR.200(a)(6)		
Take appropriate remedial actions to address findings notified by the competent authority (non-compliances)	Both	IS.D.OR.200(a)(7) IS.D.OR.225		
Implement an external information security reporting scheme	Management	IS.D.OR.200(a)(8) IS.D.OR.230	Incident Management (C.04)	RS.CO – Communications

Part-IS main task	**Activity type**	**Reference**		
	Management, Operational	**Part-IS**	**EU e-CF**	**NIST CSF 2.0**
			Competence Areas & Skills	**Functions & Categories**
Monitor compliance with this Regulation and report findings to top management	Operational	IS.D.OR.200(a)(12)	Compliance (E.09)	GV.RM – Risk Management
Protect confidentiality of exchanged information	Operational	IS.D.OR.200(a)(13)	Information Security Management (E.08)	PR.DS – Data Security
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.D.OR.200(b) IS.D.OR.260	Information Security Management (E.08)	GV.IA – Improvement and Assessment
Document and maintain all key processes, procedures, roles and responsibilities	Management	IS.D.OR.200(c)	ISM (E.08), Compliance (E.09)	GV.IA – Improvement and Assessment
Identify all elements which could be exposed to information security risks	Management	IS.D.OR.205(a)	Risk Management (E.02)	ID.AM – Asset Management
Identify the interfaces with other organisations which could result in exposure to information security risks	Management	IS.D.OR.205(b)	Risk Management (E.02), Business Change Management (E.07)	ID.BE – Business Environment
Identify information security risks and assign a risk level	Management	IS.D.OR.205(c)	Risk Management (E.02)	ID.RA – Risk Assessment
Review and update the risk assessment based on certain criteria	Operational	IS.D.OR.205(d)	Risk Management (E.02)	GV.RM – Risk Management
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.D.OR.210(a)	Risk Management (E.02)	GV.RM – Risk Management

Part-IS main task	**Activity type**	**Reference**		
	Management, Operational	**Part-IS**	**EU e-CF**	**NIST CSF 2.0**
			Competence Areas & Skills	**Functions & Categories**
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.D.OR.210(b)	Risk Management (E.02), ISM (E.08)	RS.CO – Communications

Establish an internal information security reporting scheme to enable the collection and evaluation of information security events from personnel	Management	IS.D.OR.200(a)(4)
		IS.D.OR.215(a)
		IS.D.OR.215(e)
			Incident Management (C.04)	DE.CM – Security Continuous Monitoring

Ensure that contracted organisations report information security events	Management	IS.D.OR.215(c)	Supplier Relationship Management (E.10)	DE.CM – Security Continuous Monitoring
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Operational	IS.D.OR.215(b)(1)-(b)(3)	Incident Management (C.04)	DE.AE – Anomalies and Events
Implement measures to detect in processes and operations information security events which may have a potential impact on aviation safety	Operational	IS.D.OR.220(a)	ISM (E.08)	DE.CM – Security Continuous Monitoring
Implement measures to respond to information security events that may cause an information security incident	Operational	IS.D.OR.220(b)	Incident Management (C.04)	RS.RP – Response Planning
Cooperate on investigations with other organisations that contribute to the information security of its own activities	Management	IS.D.OR.215(d)	Incident Management (C.04), Legal Advice and Compliance (E.09)	RS.AN – Analysis
Implement measures to recover from information security incidents	Operational	IS.D.OR.220(c)	Incident Management (C.04)	RC.RP – Recovery Planning

Part-IS main task	Activity type	Reference		
			EU e-CF	NIST CSF 2.0
	Management, Operational	Part-IS	Competence Areas & Skills	Functions & Categories
Manage risks associated with contracted activities with regard to the management of information security	Management	IS.D.OR.235	Supplier Relationship Management (E.10)	GV.RM – Risk Management
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.D.OR.240(f)	Personnel Development (D.11)	GV.PO – Strategy, Policy, and Oversight
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding information security management	Management	IS.D.OR.240(g)	Personnel Development (D.11)	GV.PO – Strategy, Policy, and Oversight
Create and maintain a process to ensure that the personnel acknowledge the responsibilities associated with the assigned roles and tasks	Management	IS.D.OR.240(h)	Personnel Development (D.11)	GV.PO – Strategy, Policy, and Oversight
Verify the identity and trustworthiness of personnel who have access to information systems	Management	IS.D.OR.240(i)	ISM (E.08)	PR.AC – Identity Management and Access Control
Archive, protect and retain records and ensure they are traceable for a specified time	Operational	IS.D.OR.245	ISM (E.08), Compliance (E.09)	PR.DS – Data Security
Correct non-compliance findings upon notification by the competent authority within the period agreed with the competent authority	Operational	IS.D.OR.225		
Implement an information security reporting system in accordance with Regulation (EU) No 376/2014	Management	IS.D.OR.230(a)		

Part-IS main task	**Activity type**	**Reference**		
	Management, Operational	**Part-IS**	**EU e-CF**	**NIST CSF 2.0**
			Competence Areas & Skills	**Functions & Categories**

Report information security incidents or vulnerabilities to the competent authority and, under certain conditions, to others	Operational	IS.D.OR.230(b)
		IS.D.OR.230(c)
			Incident Management (C.04)	RS.CO – Communications

Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.D.OR.260(a)	ISM (E.08)	GV.IA – Improvement and Assessment
Take actions to improve the ISMS if required. Reassess the ISMS elements affected by the implemented measures.	Operational	IS.D.OR.260(b)	ISM (E.08)	GV.IA – Improvement and Assessment
Ensure accessibility of the competent authority to the contracted organisation	Management	IS.D.OR.235(b)	ISM (E.08)	GV.OP – IS Governance
Top management ensures that all necessary resources are available to comply with the Regulation	Management	IS.D.OR.240(a)(1)	ISM (E.08)	GV.PO – Strategy, Policy, and Oversight

Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Management	IS.D.OR.240(a)(2)
		IS.D.OR.240(a)(3)
			ISM (E.08)	GV.PO – Strategy, Policy, and Oversight

Appoint a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Management	IS.D.OR.240(b)
		IS.D.OR.240(c)
		IS.D.OR.240(d)
			ISM (E.08), Compliance (E.09)	GV.OP – IS Governance

Create and maintain an information security management manual (ISMM)	Management	IS.D.OR.250		
Develop a procedure on how to notify the competent authority upon changes to the ISMS	Management	IS.D.OR.255(a)	Compliance (E.09)	GV.OP – IS Governance

Part-IS main task	**Activity type**	**Reference**		
	Management, Operational	**Part-IS**	**EU e-CF**	**NIST CSF 2.0**
			Competence Areas & Skills	**Functions & Categories**

Manage changes to the ISMS and notify the competent authority and/or request for approval of changes	Management	IS.D.OR.255(a)
		IS.D.OR.255(b)
			ISM (E.08), Process Improvements (E.05)	RS.IM-Improvements

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.D.OR.200(a)	~~IDENTIFY~~	~~ID.RM~~	4 ~~6.1.1~~	-	
Establish the scope of the ISMS according to Part-IS requirements	Management	IS.D.OR.205(a)	~~IDENTIFY~~	~~ID.BE-2~~ ~~ID.BE-4~~ ~~ID.AM-5~~	~~4.3~~		
Implement and maintain an information security policy	Management	IS.D.OR.200(a)(1)	~~IDENTIFY~~	~~ID.GV-1~~	~~5.2~~	~~A5.1~~	~~A5.1~~
Identify and review information security risks	Management	IS.D.OR.200(a)(2) IS.D.OR.205	~~IDENTIFY~~	~~ID.GV-4~~ ~~ID.RA~~	~~6.1.2~~ ~~8.1~~ ~~8.2~~	-	
Implement information security risk treatment measures	Management	IS.D.OR.200(a)(3) IS.D.OR.210	~~PROTECT~~	~~PR.PT~~	~~6.1.3~~ ~~8.1~~ ~~8.3~~	-	
Implement measures to detect information security events and identify those related to aviation safety	Management	IS.D.OR.200(a)(5) IS.D.OR.220	~~DETECT~~	~~DE.AE-3~~ ~~DE.CM-1~~ ~~DE.CM-2~~ ~~DE.CM-3~~	-	~~A11.1.2~~ ~~A12.4.1~~ ~~A12.4.3~~ ~~A16.1.7~~	~~A7.2~~ ~~A8.15~~ ~~A5.28~~
Implement measures that have been notified by the competent authority	Operational	IS.D.OR.200(a)(6)		-	~~10.1~~	~~A6.1.3~~	~~A5.5~~
Take appropriate remedial actions to address findings notified by the competent	Both	IS.D.OR.200(a)(7) IS.D.OR.225		-	~~10.1~~	~~A6.1.3~~	~~A5.5~~

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**~~
authority (non-compliances)							
Implement an external information security reporting scheme	Management	IS.D.OR.200(a)(8) IS.D.OR.230	🟥	~~RS.CO-2~~ ~~RS.CO-3~~ ~~RS.CO-4~~ ~~RS.CO-5~~	~~7.4~~	~~A6.1.3~~ ~~A16.1.2~~ ~~A16.1.3~~	~~A5.5~~ ~~A6.8~~
Monitor compliance with this Regulation and report findings to top management	Operational	IS.OI.R.200(a)(12)	~~IDENTIFY~~	~~ID.GV-3~~	~~9.2~~	~~A18.2.1~~ ~~A18.2.2~~	~~A5.35~~ ~~A5.36~~
Protect confidentiality of exchanged information	Operational	IS.D.OR.200(a)(13)	~~PROTECT~~	~~PR.DS-1~~ ~~PR.DS-2~~	-	~~A8.2.2~~ ~~A13.2~~	~~A5.13~~ ~~A5.14~~
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.D.OR.200(b) IS.D.OR.260	~~IDENTIFY~~	~~ID.RA-6~~ ~~ID.SC-4~~	~~4.4~~ ~~9.1~~ ~~9.3~~ ~~10.1~~ ~~10.2~~	~~A5.1.2~~ ~~A16.1.7~~ ~~A17.1.3~~ ~~A18.2.1~~	~~A5.1~~ ~~A5.28~~ ~~A5.29~~ ~~A5.35~~
			~~PROTECT~~	~~PR.IP-7~~ ~~PR.IP-10~~			
			~~DETECT~~	~~DE.DP-5~~			
			🟥	~~RS.MI-3~~ ~~RS.IM-2~~			
			~~RECOVER~~	~~RC.IM-2~~			
Document and maintain all key processes, procedures, roles and responsibilities	Management	IS.D.OR.200(c)	~~IDENTIFY~~	~~ID.AM-6~~ ~~ID.GV-4~~ ~~ID.RM-1~~ ~~ID.SC-1~~ ~~ID.SC-2~~	~~4.2~~ ~~5.2~~ ~~5.3~~	~~A5.1~~ ~~A6.1.1~~	~~A5.1~~ ~~A5.2~~
			~~PROTECT~~	~~PR.AT-2~~ ~~PR.AT-4~~ ~~PR.AT-5~~ ~~PR.IP-12~~			
			~~DETECT~~	~~DE.DP-1~~			
			🟥	~~RS.CO-1~~ ~~RS.AN-5~~			
Identify all elements which could be exposed to information security risks	Management	IS.D.OR.205(a)	~~IDENTIFY~~	~~ID.AM-1~~ ~~ID.AM-2~~ ~~ID.AM-4~~ ~~ID.AM-5~~	~~4.3~~	~~A8.1.1~~	~~A5.9~~

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**~~
Identify the interfaces with other organisations which could result in exposure to information security risks	Management	IS.D.OR.205(b)	~~IDENTIFY~~	~~ID.BE-1~~ ~~ID.BE-2~~ ~~ID.BE-4~~ ~~ID.BE-5~~	~~4.3~~	~~-~~	
Identify information security risks and assign a risk level	Management	IS.D.OR.205(c)	~~IDENTIFY~~	~~ID.RA-1~~ ~~ID.RA-2~~ ~~ID.RA-3~~ ~~ID.RA-4~~ ~~ID.RA-5~~	~~6.1.2~~	~~-~~	
Review and update the risk assessment based on certain criteria	Operational	IS.D.OR.205(d)	~~IDENTIFY~~	~~ID.RM~~	~~8.2~~	~~-~~	~~A5.7~~
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.D.OR.210(a)	~~PROTECT~~	~~PR.IP~~ ~~PR.PT~~	~~6.1.3~~ ~~8.3~~	~~-~~	
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.D.OR.210(b)	~~IDENTIFY~~	~~ID.AM-3~~ ~~ID.BE-1~~ ~~ID.BE-2~~ ~~ID.BE-4~~ ~~ID.RM-3~~ ~~ID.SC-3~~	~~8.1~~	~~-~~	
			~~PROTECT~~	~~PR.IP-7~~			

Establish an internal information security reporting scheme to enable the collection and evaluation of information security events from personnel	Management	IS.D.OR.200(a)(4)
		IS.D.OR.215(a)
		IS.D.OR.215(e)
			~~IDENTIFY~~	~~ID.AM-3~~	~~7.4~~	~~A16.1.1~~
						~~A16.1.2~~
							~~A5.28~~
							~~A6.8~~

Ensure that contracted organisations report information security events	Management	IS.D.OR.215(c)	~~RESPOND~~	~~RS.CO-2~~ ~~RS.CO-4~~	~~7.4~~	~~A15.1.1~~ ~~A16.1.2~~	~~A5.19~~ ~~A6.8~~
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Operational	IS.D.OR.215(b)(1)-(b)(3)	~~IDENTIFY~~	~~ID.RA-1~~	~~-~~	~~A12.6.1~~ ~~A16.1.1~~ ~~A16.1.4~~	~~A8.8~~ ~~A5.24~~ ~~A5.25~~

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~~**
			~~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.D.OR.220(a)	~~DETECT~~	~~DE.AE~~ ~~DE.CM~~ ~~DE.DP~~	-	~~A11.1.2~~ ~~A12.4.1~~ ~~A12.6.1~~ ~~A16.1.1~~ ~~A16.1.2~~ ~~A16.1.3~~ ~~A16.1.4~~ ~~A16.1.5~~	~~A7.2~~ ~~A8.8~~ ~~A8.15~~ ~~A8.16~~ ~~A5.24~~ ~~A5.25~~ ~~A5.26~~ ~~A6.8~~
			~~PROTECT~~	~~PR.PT-1~~			
Implement measures to respond to information security events that may cause an information security incident	Operational	IS.D.OR.220(b)	~~RESPOND~~	~~RS.RP~~ ~~RS.AN~~ ~~RS.MI~~	-	~~A16.1.5~~	~~A5.26~~
Cooperate on investigations with other organisations that contribute to the information security of its own activities	Management	IS.D.OR.215(d)	~~RESPOND~~	~~RS.AN-3~~ ~~RS.AN-5~~	-	~~A15.1.2~~ ~~A15.1.3~~ ~~A16.1.7~~	~~A5.20~~ ~~A5.21~~ ~~A5.28~~
Implement measures to recover from information security incidents	Operational	IS.D.OR.220(c)	~~RECOVER~~	~~RC.RP-1~~ ~~RC.IM-1~~	-	~~A16.1.5~~ ~~A16.1.6~~	~~A5.26~~ ~~A5.27~~
Manage risks associated with contracted activities with regard to the management of information security	Management	IS.D.OR.235	~~IDENTIFY~~	~~ID.SC-1~~ ~~ID.SC-2~~	-	~~A15.1~~ ~~A15.2~~	~~A5.19~~ ~~A5.20~~ ~~A5.21~~ ~~A5.22~~
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.D.OR.240(f)	~~IDENTIFY~~	~~ID.AM-5~~ ~~ID.AM-6~~ ~~ID.GV-2~~	~~7.1~~	~~A6.1.1~~	~~A5.2~~
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding	Management	IS.D.OR.240(g)	~~IDENTIFY~~	~~ID.AM-5~~ ~~ID.AM-6~~	~~7.2~~	~~A7.2.2~~	~~A6.3~~
			~~PROTECT~~	~~PR.AT-1~~			

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~~**
information security management							
Create and maintain a process to ensure that the personnel acknowledge the responsibilities associated with the assigned roles and tasks	Management	IS.D.OR.240(h)	~~IDENTIFY~~	~~ID.GV-2~~ ~~ID.GV-3~~	~~7.3~~ ~~7.4~~	~~A7.1.2~~	~~A6.2~~
Verify the identity and trustworthiness of personnel who have access to information systems	Management	IS.D.OR.240(i)	~~PROTECT~~	~~PR.AC-6~~ ~~PR.IP-11~~	~~7.1~~	~~A7.1.1~~	~~A6.1~~
Archive, protect and retain records and ensure they are traceable for a specified time	Operational	IS.D.OR.245	~~IDENTIFY~~	~~ID.RA-4~~	~~7.5~~	~~A8.2.2~~ ~~A8.2.3~~ ~~A11.1.3~~ ~~A11.1.4~~ ~~A12.1.3~~ ~~A12.3.1~~ ~~A12.4.1~~ ~~A12.4.2~~ ~~A12.4.3~~	~~A5.10~~ ~~A5.13~~ ~~A7.3~~ ~~A7.5~~ ~~A8.6~~ ~~A8.10~~ ~~A8.13~~ ~~A8.15~~
			~~PROTECT~~	~~PR.AC-2~~ ~~PR.AC-3~~ ~~PR.AC-4~~ ~~PR.DS-1~~ ~~PR.DS-4~~ ~~PR.DS-5~~ ~~PR.DS-6~~ ~~PR.IP-4~~ ~~PR.IP-6~~ ~~PR.PT-1~~			
Correct non-compliance findings upon notification by the competent authority within the period agreed with the competent authority	Operational	IS.D.OR.225		-	~~10.1~~	~~A18.1.1~~ ~~A18.2~~	~~A5.31~~ ~~A5.35~~ ~~A5.36~~
Implement an information security reporting system in accordance with Regulation (EU) No 376/2014	Management	IS.D.OR.230(a)		-	-	-	

Report information security incidents or vulnerabilities to the competent authority and,	Operational	IS.D.OR.230(b)
		IS.D.OR.230(c)
			~~DETECT~~	~~DE.DP-3~~	~~7.4~~	~~A16.1.1~~
						~~A16.1.2~~
						~~A16.1.3~~
							~~A5.24~~
							~~A6.8~~

				~~RS.CO-2~~ ~~RS.CO-3~~ ~~RS.CO-4~~ ~~RS.CO-5~~			

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~~
under certain conditions, to others			~~RECOVER~~	~~RC.CO-3~~			
Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.D.OR.260(a)		-	~~9~~	~~A5.1.2~~ ~~A12.7.1~~ ~~A16.1.6~~	~~A5.1~~ ~~A5.27~~ ~~A8.34~~
Take actions to improve the ISMS if required. Reassess the ISMS elements affected by the implemented measures.	Operational	IS.D.OR.260(b)		-	~~10~~	~~A5.1.2~~	~~A5.1~~
Ensure accessibility of the competent authority to the contracted organisation	Management	IS.D.OR.235(b)		-	~~9.3~~	~~A6.1.3~~ ~~A15.1~~ ~~A15.2~~	~~A5.5~~ ~~A5.20~~ ~~A5.22~~
Top management ensures that all necessary resources are available to comply with the Regulation	Management	IS.D.OR.240(a)(1)	~~IDENTIFY~~	~~ID.AM-5~~ ~~ID.AM-6~~	~~7.1~~	~~A6.1.1~~	~~A5.2~~
Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Management	IS.D.OR.240(a)(2)&(a)(3)	~~IDENTIFY~~ ~~PROTECT~~	~~ID.GV-1~~ ~~PR.AT-1~~ ~~PR.AT-4~~	~~5.1~~ ~~5.2~~ ~~7.4~~	~~A5.1.1~~ ~~A7.2.1~~ ~~A7.2.2~~	~~A5.1~~ ~~A5.4~~ ~~A6.3~~

Appoint a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Management	IS.D.OR.240(b)
		IS.D.OR.240(c)
		IS.D.OR.240(d)
			~~IDENTIFY~~
			~~PROTECT~~
				~~ID.AM-6~~
				~~ID.GV-2~~
				~~PR.AT-1~~
				~~PR.AT-4~~
					~~7.1~~
					~~7.2~~
						~~A6.1.1~~
						~~A7.2.1~~
						~~A7.2.2~~
							~~A5.2~~
							~~A5.4~~
							~~A6.3~~

Create and maintain an information security management manual (ISMM)	Management	IS.D.OR.250		-	~~7.5.1~~	~~A6.1.3~~ ~~A12.1.1~~	~~A5.5~~ ~~A5.37~~
Develop a procedure on how to notify the competent authority upon changes to the ISMS	Management	IS.D.OR.255(a)	~~IDENTIFY~~	~~ID.AM-3~~	~~7.4~~ ~~7.5.1~~	~~A6.1.3~~ ~~A13.2.1~~ ~~A13.2.2~~	~~A5.5~~ ~~A5.14~~

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~~

Manage changes to the ISMS and notify the competent authority and/or request for approval of changes	Management	IS.D.OR.255(a)
		IS.D.OR.255(b)
			~~IDENTIFY~~	~~ID.AM-3~~	~~7.4~~	~~A6.1.3~~
						~~A13.2.1~~
						~~A13.2.2~~
							~~A5.5~~
							~~A5.14~~

Appendix III — Examples of aviation services and interfaces

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 service providers

— aeronautical digital mapping services

— aeronautical information management (AIM) – external, national, regional

— airports

— air traffic control (ATC) – external, superior

— air traffic management (ATM)

— approach (APP) & area control (ACC) Services – ER ACC, APP ACC

— civil & state airspace user (AU) operations centres

— communication infrastructure

— flight information & traffic information services (FIS/TIS) data integrators

— navigation infrastructure – ground-based, satellite-based

— Non-ATM meteorological (MET) service providers

— non-aviation users (external)

— regional & sub-regional airspace management (ASM) and air traffic flow & capacity management (ATFCM)

— static aeronautical data services

— sub-regional demand & capacity balancing (DCB) common service providers

— surveillance infrastructure – airport, en-route, terminal manoeuvring area (TMA)

— time reference services (external)

— tower (TWR) services

- ~~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)~~

INTERFACES

Below are some examples of interfaces between organisations interacting in different functional chains, which can be used as a basis for identifying the scope of the risk assessment for the organisation. Note that these examples are a graphical representation of the 'Examples of ecosystem data exchange' provided in EUROCAE ED-201A, Appendix B - Tables B-14, which can be consulted for further information.

Note: Although it is not an organisation, an aircraft has been included in all these examples for the sake of completeness of the description of the data exchange. The aircraft should be considered as an element within the scope of the ISMS of the organisation to which it belongs (typically the airline).

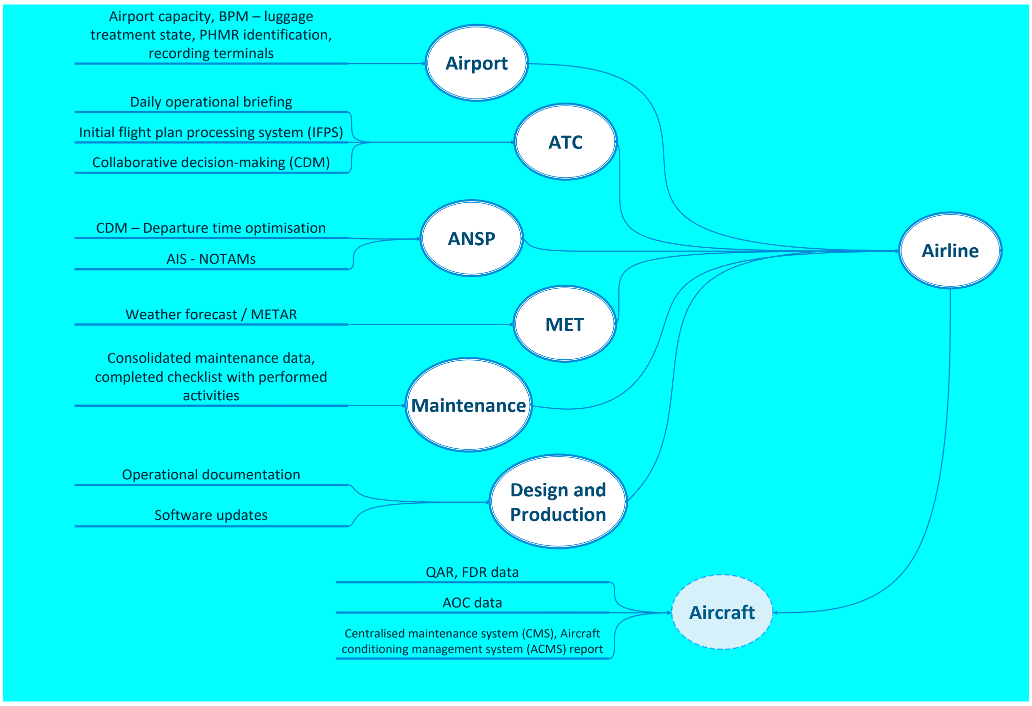

Airport capacity, BPM – luggage treatment state, PHMR identification, recording terminals
Airport
Daily operational briefing
Initial flight plan processing system (IFPS)
Collaborative decision-making (CDM)
ATC
CDM – Departure time optimisation
AIS - NOTAMs
ANSP
Airline
Weather forecast / METAR
MET
Consolidated maintenance data, completed checklist with performed activities
Maintenance
Operational documentation
Software updates
Design and Production
QAR, FDR data
AOC data
Centralised maintenance system (CMS), Aircraft conditioning management system (ACMS) report
Aircraft

Figure 1: Interfaces of other organisations with an airline operator

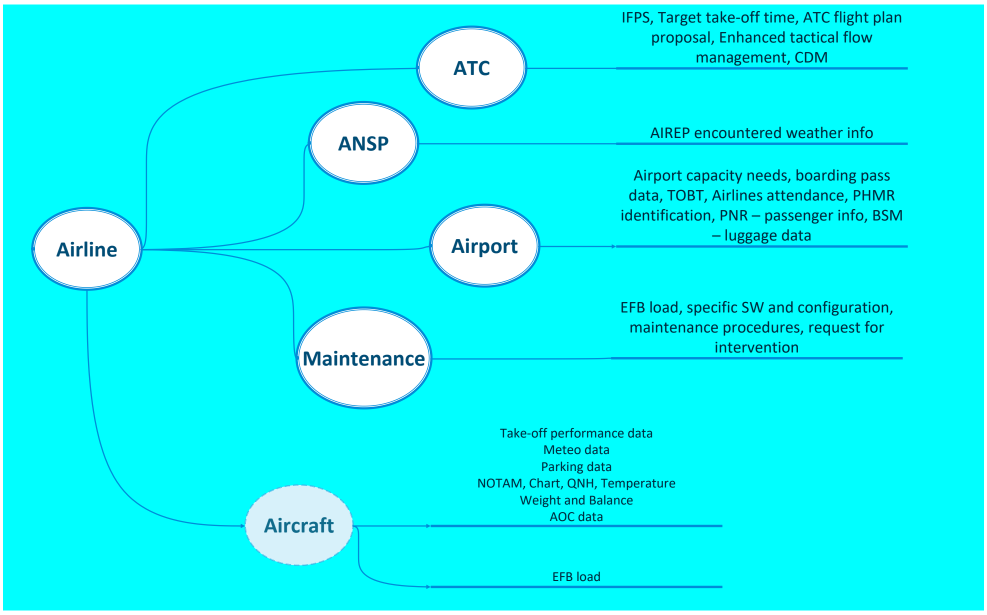

ATC
IFPS, Target take-off time, ATC flight plan proposal, Enhanced tactical flow management, CDM
ANSP
AIREP encountered weather info
Airline
Airport
Airport capacity needs, boarding pass data, TOBT, Airlines attendance, PHMR identification, PNR – passenger info, BSM – luggage data
Maintenance
EFB load, specific SW and configuration, maintenance procedures, request for intervention
Take-off performance data
Meteo data
Parking data
NOTAM, Chart, QNH, Temperature
Weight and Balance
AOC data
Aircraft
EFB load

Figure 2: Interfaces of an airline operator with other organisations

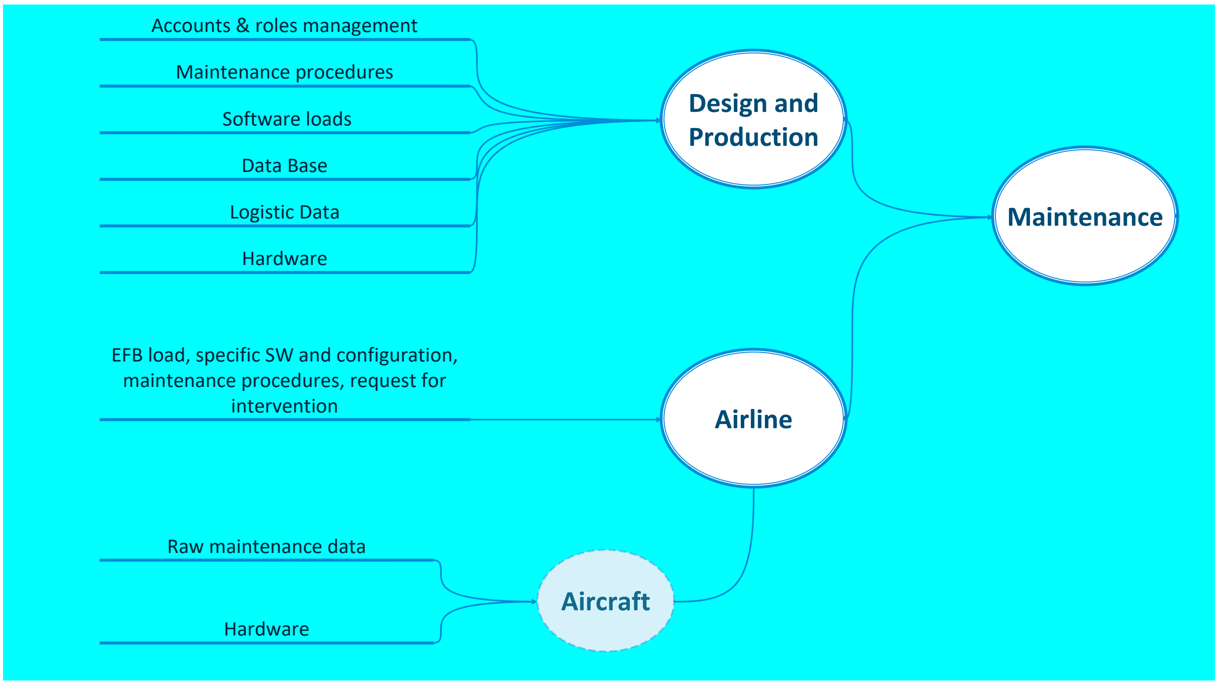


Figure 3: Interfaces of other organisations with a maintenance service provider

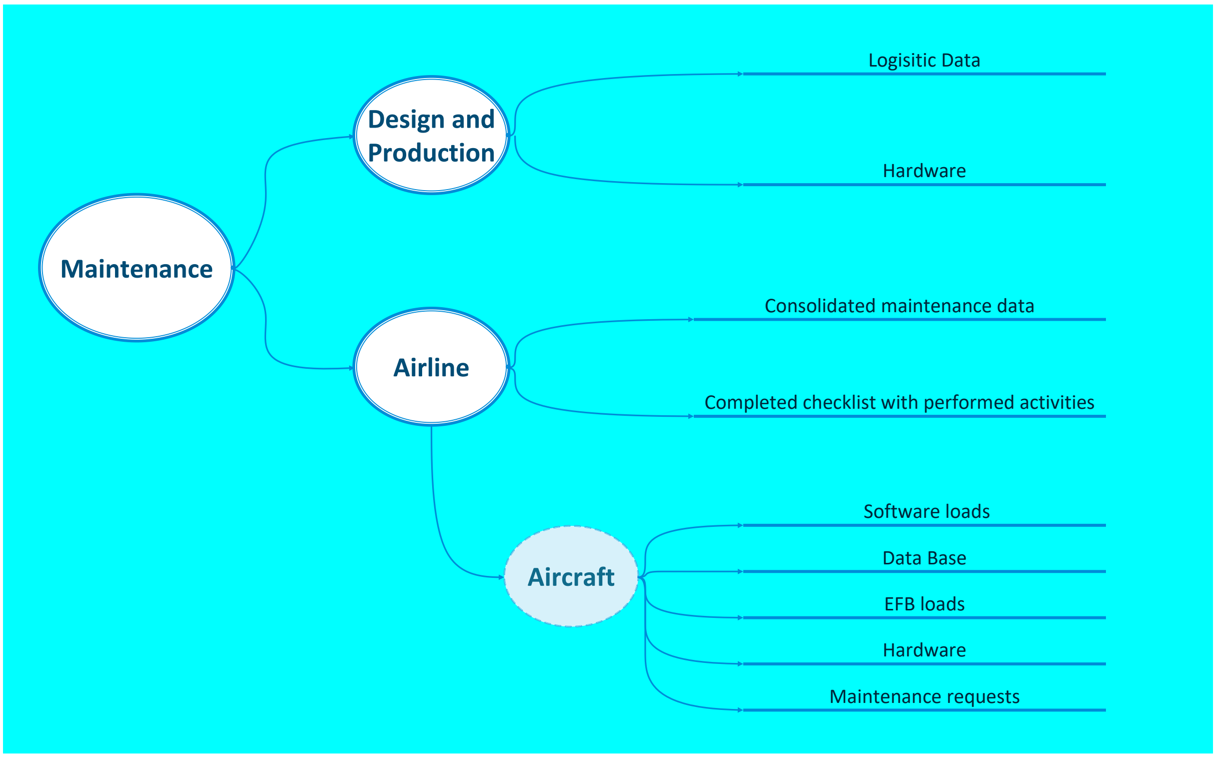


Figure 4: Interfaces of a maintenance service provider with other organisations

Appendix IV — Part-IS requirements mapping to ISO/IEC 27001 clauses and controls, and considerations on differences

The following provides guidance on how organisations that have already implemented an information security management system (ISMS) compliant with ISO/IEC 27001:2022 can integrate Part-IS requirements into their existing ISMS.

Note for the reviewer: the references to Part-IS provisions are in the format IS.OR.NNN to indicate that they are valid for the provisions in both the Delegated Regulation and the Implementing Regulation.

Part-IS requirement	ISO/IEC 27001 mapping and specific guidance
IS.OR.200(a)	**Related ISO/IEC 27001 clauses and controls**
	4. Context of the organisation 6.1.1 Actions to address risks and opportunities - General
	Part-IS particularity
	An information security management system designed in the context of an ISO/IEC 27001 ISMS, which is currently not connected to the management systems required by the delegated and implementing acts of Regulation (EU) 2018/1139, including Part-IS, may differ if these different systems do not address the same goals. Part-IS focuses on information security requirements meeting the applicable aviation safety objectives, which have an influence on elements of the information security management system. Also, the 'interested parties' and the 'internal and external issues' as laid down in Chapter 4 of ISO/IEC 27001 may be adapted to address the requirements of Part-IS for the organisation.
	Guidance on Part-IS implementation
	Please note that the IS.OR.200 requirement points to many other Part-IS requirements that the ISMS has to comply with, namely 205, 210, 215, 220, 225, 230, 235, 240,245, 255, and 260. Further details are provided in the specific chapters on the particular requirement. Regarding the other remaining requirements, not pointing out to other Part-IS requirements, and comparing them with ISO/IEC 27001, **there are four requirements left, namely IS.OR.200(a)(1), IS.OR.200(a)(6), IS.OR.200(a)(12), and IS.OR.200(a)(13).**

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200(a)(1)	**Related ISO/IEC 27001 clauses and controls**
	5.2 Policy A.5.1 Policies for information securities
	Part-IS particularity
	An information security management system designed in the context of an ISO/IEC 27001 ISMS, which is currently not connected to the management systems required by the delegated and implementing acts of Regulation (EU) 2018/1139, may differ as these different systems do often not address the same goals. Part-IS focuses on information security requirements influencing the applicable aviation safety objectives, which in their turn have an influence on the elements of the information security management system. In addition, all domain-specific delegated and implementing acts of Regulation (EU) 2018/1139, namely points ORO.GEN.200(a)(2), ORA.GEN.200(a)(2), CAMO.A.200(a)(2), 145.A.200(a)(2), 21.A.139(c)(1), 21.A.239(c)(1), ATM/ANS.OR.B.005(a)(2), ATCO.OC.C.001(b), ADR.OR.D.005(b)(2), require a 'safety policy', where information security may be integrated.
	Guidance on Part-IS implementation
	The policy on information security established in an ISO/IEC 27001 context **shall be updated with regard to the potential impact of the risks on aviation safety**. At least the elements of **AMC1 IS.OR.200(a)(1)** shall be mentioned in the policy. Therefore, the following elements may need to be added to an existing ISMS policy. The elements in **bold** and *italics* are additional guidance that might also be considered. (a) committing to comply with applicable legislation, consider relevant standards and best practices, ***including safety- and cybersecurity-related standards and guidance published or prescribed by ICAO, EASA, or the relevant civil aviation authority***; (b) setting objectives and performance measures for managing information security, ***updated to ensure meeting*** the applicable aviation safety objectives; (c) defining general principles, activities, processes for the organisation to appropriately secure information and communication technology systems and data, ***in relation to the information security / safety risk assessment required by point IS.OR.205***; (d) committing to apply ISMS requirements into the processes of the organisation; (e) committing to continually improve **towards higher levels of information security process maturity** as per IS.OR.260; (f) committing to satisfy applicable requirements regarding information security ***(including requirements stemming from civil aviation authorities)*** and its

Part-IS requirement	ISO/IEC 27001 mapping
	proactive and systematic management and to the provision of appropriate resources for its implementation and operation; (g) assigning information security as one of the essential responsibilities **for all managers**; (h) committing to promote the information security policy through training or awareness sessions within the organisation to all personnel on a regular basis or upon modifications; (i) **encouraging the implementation of a 'just-culture'** and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents; (j) committing to communicate the information security policy to all relevant parties, as appropriate.

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200(a)(6)	**Related ISO/IEC 27001 clauses and controls**
	10.1 Corrective actions A5.5 Contact with authorities A5.26 Response to information security incidents A8.8 Management of technical vulnerabilities
	Part-IS particularity
	This requirement has no specific counterpart in ISO/IEC 27001.
	Guidance on Part-IS implementation
	The policies and procedures, defined as means of compliance with the requirements listed above should be extended to information security measures mandated by the competent authority.
IS.OR.200(a)(12)	**Related ISO/IEC 27001 clauses and controls**
	9.2. Internal audit 9.3 Management review 10.2 Non-conformity and corrective action A5.36 Compliance with policies, rules and standards for information security
	Part-IS particularity

Part-IS requirement	**ISO/IEC 27001 mapping**
	This requirement is strongly related to the internal audit system and the independent checking function of ISO/IEC 27001. The required feedback system to the accountable manager or the head of the design organisation fits into the requirement of 9.3. In addition, all delegated and implementing acts for the specific domains require a similar 'compliance monitoring function', where information security should be integrated as described in **AMC1 IS.OR.200(a)(12)**.
	Guidance on Part-IS implementation
	The requirements of ISO/IEC 27001 and the delegated and implementing acts of Regulation (EU) 2018/1139 are compatible. Therefore, it will be easy to add Part-IS into the audit scope of the ISO/IEC 27001 internal audit system. The role of the accountable manager or the head of the design organisation as defined under IS.OR.240(a) shall be addressed accordingly in the feedback loop if the role is not already addressed in the management review process. The accountable manager or the head of the design organisation is required to be personally briefed on the key findings so that appropriate decisions can be made. Refer also to GM1 IS.OR.200(a)(12). Note: *ISO19011:2018 provides guidance on the establishment of an internal audit system. Specifically, Chapter A.7 'Auditing compliance within a management system' provides useful guidance on how to integrate a compliance monitoring function into an internal audit system.*
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.200 (a)(13)	**Related ISO/IEC 27001 clauses and controls**
	7.5.3. Control of documented information (Note) A5.12 Classification of information A5.34 Privacy and protection of personal identifiable information (PII) A8.12 Data leakage prevention
	Part-IS particularity
	This requirement is limited to 'information from other organisations' and to confidentiality. ISO/IEC 27001 does not differentiate between 'internal' or 'external' information (as laid down e.g. in ISO 9001:2015 Chapter 8.5.3). The only reference is made in the note in Chapter 7.5.3. Part-IS stresses protection of external information received due to the sensitivity it may have regarding incidents and vulnerabilities disclosure. Insufficient confidentiality protection may result in exploitation of vulnerabilities affecting safety that the original provider of information may not have perceived.

Part-IS requirement	ISO/IEC 27001 mapping
	Guidance on Part-IS implementation
	The protection of information, specifically regarding confidentiality (as in ISO/IEC 27002:2022), is related to a set of controls that can be found in Table A.1 (Matrix of controls and attribute values) of ISO/IEC 27002:2022. See also the definition in ISO 27002:2022: *3.1.7 confidential information* *information that is not intended to be made available or disclosed to unauthorized individuals, entities or processes.* The organisation having implemented these controls should take special care that they apply to information received from external information that may result in information security threats if known by unauthorised actors. When this kind of information is further shared with other organisations or authorities, appropriate confidentiality procedures must be put in place and followed (TLP marking for instance).

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200(b)	**Related ISO/IEC 27001 clauses and controls**
	10.1 Continual improvement
	Part-IS particularity
	Part-IS and ISO/IEC 27001 are very similar regarding this requirement. See IS.OR.260 (a) and (b) for subtle differences.
	Guidance on Part-IS implementation
	The guidance is provided under IS.OR.260.

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200(c)	**Related ISO/IEC 27001 clauses and controls**
	6.3 Planning of changes 7.5.3 Control of documented information
	Part-IS particularity
	Control of documented information is one of the key processes in each ISO management system standard, following the ISO ‘high level structure’ (ISO/IEC Directives part 1 Annex SL), such as ISO/IEC 27001 :2022. For changes, see IS.OR.255. In addition, most of the delegated and implementing acts for the specific domains require a similar need to document, where information security should be integrated.
	Guidance on Part-IS implementation

Part-IS requirement	ISO/IEC 27001 mapping
	Additional guidance is provided under IS.OR.250 and IS.OR.255.

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200 (d)	**Related ISO/IEC 27001 clauses and controls**
	4.3 Determining the scope of the information security management system.
	Part-IS particularity
	The scope statement and the 'statement of applicability' (SOA) are the best references to apply the 'nature and complexity'. In addition, most of the delegated and implementing acts for the specific domains require a similar need to document where information security should be integrated.
	Guidance on Part-IS implementation
	When determining the scope, it should be noted that Part-IS is delimited to the subject matter as defined in Article 1 of the Regulation(s), which refers to *identification and management of information security risks **with potential impact on aviation safety.*** Considering this, an ISMS under ISO/IEC 27001 may have a wider scope than that required by Part-IS. It could be the case that some organisational unit, processes or locations of an organisation might be covered by the ISMS under ISO/IEC 27001, but might not applicable to Part-IS. To reduce complexity, it is advised to voluntarily implement Part-IS also for those processes. The opposite may happen too: the scope under ISO/IEC 27001 may be narrower than the one Part-IS would require (e. g. the ISO/IEC 27001 scope covers only the IT department). In both situations, scope definitions must be compared and adjusted when necessary. *Note: See also guidance on IS.OR.205(a).* The scope statement in the ISO/IEC 27001 context is the right place where this clarification is made.

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.200(e)	**Related ISO/IEC 27001 clauses and controls**
	4.1 Understanding the organisation and its context.
	Part-IS particularity
	This is a 'derogation' for organisations falling under the applicability of Article 2 of the |Regulation. This process is independent from an ISO/IEC 27001 certification process.

Part-IS requirement	ISO/IEC 27001 mapping
	Guidance on Part-IS implementation
	If an organisation which already has an established ISMS according to ISO/IEC 27001 decides to embark on this process, the full implementation of Part-IS into the ISMS may be put on hold until the decision of the competent authority is made. To demonstrate that an organisation's activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations, the existing risk assessment methodology according to ISO/IEC 27001 Chapter 6.1.2 may be used if the methodology is enhanced with a focus on the impact on safety. On the other hand, an existing risk assessment methodology used by the existing safety management system (SMS) could be enhanced by addressing potential information security risks. In any case, the competent authority responsible for the organisation will determine which process and methodology shall be used. This demonstration shall be at least verified and reassessed at regular intervals and as a mandatory part of the organisation's change process. In case of any doubt about the conclusion, the appropriate civil aviation authority must be contacted.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.205(a)	**Related ISO/IEC 27001 clauses and controls**
	4.3 Determining the scope of the information security management system 6.1.2 Information security risk assessment
	Part-IS particularity
	This requirement of Part-IS is in line with ISO/IEC 27001, however ISO/IEC 27001 allows a wider focus, whereas Part-IS puts the focus on safety already from the element's identification stage. In addition, all of the delegated and implementing acts for the specific domains require a risk assessment process, where information security can be integrated.
	Guidance on Part-IS implementation
	AMC1 IS.OR.205(a) explains that when conducting an information security risk assessment, the organisation should ensure that each relevant aviation safety impact is identified and included in the ISMS scope, which might not be the case when using ISO/IEC 27001. On the other hand, an ISO/IEC 27001 ISMS focuses its security risk assessment mainly on the business impact of infringement on Confidentiality, Integrity and

Part-IS requirement	ISO/IEC 27001 mapping
	Availability, their risks and the impact on assets (e. g. loss of IT infrastructure, breach of data). This means that, starting from an ISMS based on ISO/IEC 27001, a complementary analysis has to be made to **take into account all the elements related to aviation safety**. To bridge the two approaches of safety management systems (SMS) and ISMS, an identified information security risk may be entered as a 'cause' or 'contributing event' in the aviation-safety-focused risk assessment required by the domain-specific implementing or delegated act. The figure in GM1.IS.OR.205(c) provides a good indication of how this bridge could be built.
IS.OR.205(b)	**Related ISO/IEC 27001 clauses and controls**
	4.1 Understanding the organisation and its context 4.3 Determining the scope of the information security management system A5.19 Information security in supplier relationships A5.21 Managing information security in the information and communication technology (ICT) supply chain
	Part-IS particularity
	IS.OR.205(b) focuses on the identification of interfaces with the other organisations. ISO/IEC 27001 4.3 requires considering in point c) the interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations. So, there is more in Part-IS than that required by ISO/IEC 27001, provided that the scope considered includes safety, as required by IS.OR.205(a). The Controls A5.19 and A5.21 are a profound foundation for the requirements of IS.OR.205(b).
	Guidance on Part-IS implementation
	ISO/IEC 27001 A5.19 requires the identification of risks associated with the use of suppliers' products or services. ISO 27002 A5.19 contains additional guidance in points f) to j) on how to manage the risk exposure. ISO/IEC 27001 A5.21 requires the management of information security risks associated with the ICT products and services supply chain. ISO 27002 A5.21 contains additional guidance in points f), k), l) and m) on how to manage risks through the supply chain. The Part-IS notion about interfaces and supply chain goes beyond the respective ISO/IEC 27001 notion. GM1 IS.OR.205(b) requests interfacing organisations to share information about mutual risk exposure (including all data flows) and urges organisations to use ED-201A for that. IS.OR.205(c) also requires accounting for information acquired by interfacing organisations, which underlines the two-way nature of the considerations. Particular attention

Part-IS requirement	ISO/IEC 27001 mapping
	should be paid to the Part-IS intent to protect the so-called functional chains. The notion is that while organisations may protect themselves well enough, interfaces between organisations may pose risks to each chain when not accounted for.
IS.OR.205(c)	**Related ISO/IEC 27001 clauses and controls**
	6.1.2 Information security risk assessment
	Part-IS particularity
	IS.OR.205(c) is the 'heart' of Part-IS. ISO/IEC 27001 6.1.2 opens a 'framework' where the requirements of IS.OR.205 may fit in. It has to be assured that the risk management systems of the ISMS and those required by the SMS-regulations (see IS.OR.205(a)) do NOT operate independently, as there might be difficulties in connecting the two systems.
	Guidance on Part-IS implementation
	Further to this provision, a proper risk assessment shall be made, taking into account the scope and interfaces described in IS.OR.205(a) and IS.OR.205(b). It has to be noted (see also GM1 IS.OR.205(c)) that IS.OR.205 does not require the use of any specific information security risk assessment framework, such as ISO31000, NIST or others to develop the risk assessment. ISO/IEC 27001 tends to lean towards using ISO 27005 as a risk assessment standard, however, it does not make it mandatory. The key point is that the risk assessment carried out in the application of ISO/IEC 27001 6.1.2 does not necessarily consider safety risks, and may focus on different types of risks. With respect to safety, conditions that may lead to safety consequences are identified as ***hazards***. Their materialisation may be either directly triggered or caused by information security threats which have not been successfully prevented. Information security can thus cause or contribute to a safety consequence in four different ways: (1) it can act as a safety threat; (2) it can have a negative effect on a safety barrier, rendering it less effective than before; (3) it can directly trigger the materialisation of an already identified hazard; or (4) it can constitute a new, not yet identified, hazard, that can obviously also materialise. By using e.g. the 'bowtie-method' regarding information security, a 'hazard' would be replaced by a 'vulnerability', which can be exploited resulting in information security consequences (e.g. lack or reduction of confidentiality, integrity, availability, authenticity properties). Hence, from a methodology perspective, both considerations are very similar and can be designed to interact (e. g. consequences of the information security bow tie may connect as causes of the 'safety bow-tie').

Part-IS requirement	ISO/IEC 27001 mapping
	Guidance on organisations that are NOT required to operate an SMS, including safety risk management Any ISO/IEC 27001 risk assessment shall be reviewed and revised by introducing safety impact (consequence) considerations. Any risk matrix stemming from an ISO/IEC 27001 6.1.2 risk assessment is acceptable, provided it includes safety impacts (consequences), and the results remain within the limitations of ICAO Annex 19. If two different risk assessment schemes are used, they need to be linked accordingly. **Guidance on organisations that are required to operate an SMS, including safety risk management** In most of the cases, where an organisation is subject to the domain-specific implementing or delegated acts for SMS and operates an ISMS under voluntary compliance with ISO/IEC 27001, it may operate two risk management systems, one for safety under the oversight of a competent authority, and one for information security. The latter may ultimately be certified by an ISO/IEC 27001 accredited body. Each potential risk identified by the ISMS risk management shall be systematically assessed for its potential impact on safety. To establish the connection between the systems, the following approach should be used: 1. If a safety risk assessment is available, it should be able to provide its context and determined target likelihoods for acceptable information security risks to the information security risk assessment process. The context consists of the system architecture, including its preventative and mitigative barriers, the hazards assessed, and the safety risks identified. Based upon the information provided, the information security risk assessment can be conducted. Modifications to the system architecture, or any modifications of properties of the preventative or mitigative barriers, as well as the achieved risk properties need to be communicated back to the safety risk assessment process. Based upon this communication, the safety risk assessment shall be updated. In other words: mitigation measures put in place as a result of the information security risk assessment should also be considered as they may not only mitigate, but possibly also create a negative safety impact. 2. If a safety risk assessment is available, but the information security assessment process identifies a new hazard that was previously unknown to the safety risk assessment, a full hazard assessment of all safety aspects shall be conducted to ensure that the safety risk assessment contains the 'full picture' of the newly addressed hazard. 3. The safety risk and the information security risk assessments need to be repeated as described above until all acceptability requirements for all aspects are met.
IS.OR.205(d)	**Related ISO/IEC 27001 clauses and controls**

Part-IS requirement	**ISO/IEC 27001 mapping**
	6.3 Planning of changes 8.2 Information security risk assessment
	Part-IS particularity
	IS.OR.205(d) is about the subsequent changes to the original risk assessment, due to a change of context or interfaces or knowledge about the risks or lessons learnt. This is equivalent to ISO/IEC 27001 8.2. In both frameworks the reviews are planned and documented.
	Guidance on Part-IS implementation
	The same process as that already in place in an ISO/IEC 27001 context can be used to implement IS.OR.205(d), provided that this process has been updated to include safety criteria evaluation of changes that trigger an unplanned update of the risk assessment. Those organisations that have most experienced risk assessment updates at planned intervals will need to be proactive to trigger such updates more often in the situations listed in IS.OR.205(d) (1), (2), (3), and (4) that could affect safety. The triggering criteria and the process should be documented and tested before implementation, for example through table-top exercises. The change management process is key to keep a management system in a solid and stable condition. Considering an established ISMS according to ISO/IEC 27001, the regular updates of the risk assessment based on changes and lessons learned should be effective. The essential focus, introduced by Part-IS, is the 'impact on safety', which drives the update assessment. Change management processes focusing on changes that may have impact on safety are also set out in all domain-specific implementing and delegated acts. Without the 'bridge' of Part-IS, both systems (ISMS and SMS) are implemented independently, often without considering interdependencies. Part-IS implies the need (and provides the opportunity) to interlink the systems to provide a common risk picture for the organisation, with a focus on safety, but also opening the horizon to information security.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.205(e)	**Related ISO/IEC 27001 clauses and controls**
	6.1.2 Information security risk assessment
	Part-IS particularity
	This Part-IS requirement is specific to organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373.
	Guidance on Part-IS implementation
	Those organisations falling under Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373, which operate an ISO/IEC 27001:2022-conformed

Part-IS requirement	ISO/IEC 27001 mapping
	management system, use safety support assessment instead of the information security risk assessment required in IS.OR.205(c).
IS.OR.210(a)	**Related ISO/IEC 27001 clauses and controls**
	6.1.3 Information security risk treatment 8.3 Information security risk treatment
	Part-IS particularity
	IS.OR.210(a) is about Information security risk treatment, which is widely covered by ISO/IEC 27001, its Appendix A, and ISO/IEC 27002. IS.OR.210(a) provides however some additional inputs related to the risks that may have a safety impact.
	Guidance on Part-IS implementation
	ISO/IEC 27001 6.1.3 is about the definition of the risk treatment plan, while ISO/IEC 27001 8.3 deals with the implementation of the plan, and both are relevant. ISO/IEC 27001 Annex A contains a list of possible information security controls, and therefore should also be used in addition to the already existing controls, to mitigate information security risks having an impact of safety. All the controls of Annex A are detailed in ISO/IEC 27002. IS.OR.210(a) specifies that the measures selected in the plan shall reduce the consequences on aviation safety associated with the materialisation of the threat scenario. This is in line with IS.OR.205 since the risk treatment phase is a consequence of the risk assessment phase and shall address all the risks that have been evaluated. IS.OR.210(a) also stipulates that those (protection) measures shall not introduce any new potential unacceptable risks to aviation safety. This is an area that is not directly covered by neither ISO/IEC 27001 nor ISO/IEC 27002. The requirement addresses the so-called 'side effects' when introducing measures into a system (a well-known issue in software development which is also very relevant for information security measures). Preventive or mitigative measures specifically (e.g. physical security, access control) could lead to unintended side effects. Also, the risk treatment of the identified risks should focus on addressing safety via the same linkage/integration of ISMS and safety management.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.210(b)	**Related ISO/IEC 27001 clauses and controls**
	6.1.3.f Information security risk treatment 7.3 Awareness

Part-IS requirement	**ISO/IEC 27001 mapping**
	9.3 Management review A5.19 Information security in supplier relationships A5.21 Managing information security in the ICT supply chain
	Part-IS particularity
	IS.OR.210(b) is about the information of key personnel in the organisation, about the risks, the corresponding threat scenarios and the security risk treatment measures, which result in specific controls covered by Annex A to ISO/IEC 27001 and ISO/IEC 27002. It partially covers IS.OR.210(b) by the following requirement: obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. IS.OR.210(b) has two specific requirements which that also have equivalent requirements in ISO/IEC 27001 and ISO/IEC 27002: — Inform the accountable manager or the head of the design organisation of the risk treatment plan — which is a mandatory input to the management review. — Inform the interfacing entities (the same as in IS.OR.205(b)) of all risks shared with them — which is stated in A5.19 Guidance point l).
	Guidance on Part-IS implementation
	In addition to the risk owner's approval requested by ISO/IEC 27001 6.1.3.f, the organisation will need to inform: — the accountable manager or the head of the design organisation of the risk treatment plan. ISO/IEC 27001 9.3. f) defines 'results of risk assessment and status of risk treatment plan' as mandatory input for the management review which is the vehicle to inform the accountable managers/heads of the design organisation; — the interfacing entities (the same as in IS.OR.205(b)) of all risks shared with them. ISO/IEC 27002 A5.21 states in point f) 'defining rules for sharing of information and any potential issues and compromises between the organisations'. GM1 IS.OR.205(b) and ED-201A may also be used as guidance on risk sharing.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.215 (a)	**Related ISO/IEC 27001 clauses and controls**
	A5.24 Information security incident management planning and preparation A6.8 Information security event reporting
	Part-IS particularity

Part-IS requirement	**ISO/IEC 27001 mapping**
	Fully covered by the requirements of A5.24 and A6.8. However, the linkage to the external reporting scheme for the incidents with relation to safety (unsafe conditions) shall be established.
	Guidance on Part-IS implementation
	The linkage to the external reporting scheme for the incidents with relation to safety could be described under A5.5 (contact with authorities) in the ISO structure.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.215(b)	**Related ISO/IEC 27001 clauses and controls**
	A5.25 Assessment and decision on information security events A5.26 Response to information security incidents A5.27 Learning from information security incidents A5.28 Collection of evidence A8.8 Management of technical vulnerabilities
	Part-IS particularity
	Fully covered by the requirements from A5.25 to A5.28 and A8.8 with a need to focus on safety impacts.
	Guidance on Part-IS implementation
	The requirements of the controls A8.8, A5.25 to A5.28 and the guidance in ISO/IEC 27002:2022 are comprehensive to fulfil the requirements of IS.OR.215(b). In accordance with IS.OR.215(b)(1) the impact on safety always needs to be assessed specifically. AMC1 IS.OR.215(a)&(b) shall also be considered.
Part-IS requirement	**ISO/IEC 27001 mapping**
IS.OR.215(c)	A5.19 Information security in supplier relationships A5.20 Addressing information security within supplier agreements A5.21 Managing information security in the information and communication technology (ICT) supply chain
	Part-IS particularity
	To be covered under the procedures according to A5.19 and A5.21, as well as under the agreements according to A5.20.
	Guidance on Part-IS implementation

Part-IS requirement	ISO/IEC 27001 mapping
	However, this depends on whether the supplier is also subject to Part-IS or not. In the latter case, the external reporting shall be done by the contracting organisation. GM1 IS.OR.215(c) provides guidance on how to implement the relationship with contracted organisations.

Part-IS requirement	ISO/IEC 27001 mapping
IS.OR.215(d)	**Related ISO/IEC 27001 clauses and controls**
	A5.6 Contact with special interest groups A5.20 Addressing information security within supplier agreements A5.21 Managing information security in the information and communication technology (ICT) supply chain A5.28 Collection of evidence
	Part-IS particularity
	The requirements of the controls A5.20, A5.21 and A5.28 and the guidance in ISO 27002:2022 are comprehensive to fulfil the requirements of IS.OR.215(d) in terms of process, but Part-IS will require cooperation with a broader range of organisations.
	Guidance on Part-IS implementation
	As ISO/IEC 27001:2022 only focuses on the supply chain and Part-IS requires a broader focus, the process needs to be highlighted to other relevant stakeholders. This may be covered under A5.6. Nevertheless, ISO/IEC 27002 A5.19 has a clear statement under point (i) of the guidance. See also the cooperation in accordance with IS.OR.205(c).
IS.OR.215(d)	**Related ISO/IEC 27001 clauses and controls**
	A5.24 Information security incident management planning and preparation A6.8 Information security event reporting
	Part-IS particularity
	Fully covered by the requirements of A5.24 and A6.8.
	Guidance on Part-IS implementation
	However, the linkage to the external reporting scheme for the incidents with relation to safety (unsafe conditions) shall be established. This could be described under A5.5 (contact with authorities) in the ISO structure.
IS.OR.220(a)	**Related ISO/IEC 27001 clauses and controls**

	A5.24 Information security incident management planning and preparation A5.25 Assessment and decision on information security events A5.26 Response to information security incidents A5.27 Learning from information security incidents A5.28 Collection of evidence A5.29 Information security during disruption A7.5 Physical security monitoring A8.16 Monitoring activities
	Part-IS particularity
	Fully covered by the requirements of A5.24 to A5.29, and A7.5 for physical security and A8.16 for technical monitoring.
	Guidance on Part-IS implementation
	The requirements of the controls (both reactive and proactive) mentioned above and the guidance in ISO/IEC 27002:2022 are comprehensive to fulfil the requirements of IS.OR.220(a). Again, the impact on safety needs to be assessed and measures shall be taken to ensure safety. Part-IS refers to 'unsafe conditions', which shall be mitigated to an acceptable level. A re-assessment of risks that are related to incidents that have occurred or vulnerability that has been identified is mandatory in Part-IS to ensure that no risk becomes unacceptable. *Note: Due to historical reasons, information security and safety management using different wording in explaining situations which are more or less the same. The term 'incident' is used in a similar way (an event which already happened and infringes safety/security). A vulnerability in the sense of information security could be mapped to the term 'hazard' in the area of safety (a situation identified, which is possible to happen, but has not happened so far).*
IS.OR.220(b)	**Related ISO/IEC 27001 clauses and controls**
	A5.26 Response to information security incidents A5.29 Information security during disruption A7.5 Physical security monitoring A8.8 Management of technical vulnerabilities
	Part-IS particularity
	Fully covered by the requirements of A5.26 and A5.29.
	Guidance on Part-IS implementation
	The requirements of the control A5.26 and the guidance in ISO/IEC 27002:2022 are comprehensive to fulfil the requirements of IS.OR.220(b).

IS.OR.220(c)	**Related ISO/IEC 27001 clauses and controls**
	A5.26 Response to information security incidents A5.29 Information security during disruption
	Part-IS particularity
	This requirement is covered by the requirements of A5.26 and A5.29, with the difference that the recovery here is not intended to continuously ensure confidentiality, integrity, availability and integrity; instead, it is intended to maintain or return to an acceptable level of safety. In addition, some domain-specific implementing and delegated acts of Regulation (EU) 2018/1139 (e.g. ARO.GEN.200, ATM/ANS.OR.A.070, ADR.OR.B.070) require emergency response planning and/or contingency planning, where information security should be integrated.
	Guidance on Part-IS implementation
	Coupled with the requirements of controls A5.26 and A5.28 and the guidance in ISO/IEC 27002:2022, AMC1.IS.OR.220 (c) should be applied in order to revert as quickly as possible to a safe state.
IS.OR.225	**Related ISO/IEC 27001 clauses and controls**
	10.2 Non-conformity and corrective action
	Part-IS particularity
	This requirement has no specific counterpart in ISO/IEC 27001.
	Guidance on Part-IS implementation
	This issue is specifically not covered by the ISO/IEC 27001:2022 requirements.
IS.OR.230	**Related ISO/IEC 27001 clauses and controls**
	A5.5 Contact with authorities
	Part-IS particularity
	This requirement is not directly addressed in ISO/IEC 27001.
	Guidance on Part-IS implementation
	This issue is specifically not directly covered by ISO/IEC 27001 requirements. The reporting requirement should also be considered if the organisation falls under the NIS 2 Directive.
IS.OR.235(a)	**Related ISO/IEC 27001 clauses and controls**
	A5.19 Information security in supplier relationships A5.21 Managing information security in the information and communication technology (ICT) supply chain

	A5.22 Monitoring, review and change management of supplier services
	Part-IS particularity
	ISO/IEC 27001 controls A5.19, A5.21 and A5.29 may cover this requirement. The difference in the requirements of IS.OR.235 is that they are limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, etc.). In addition, all domain-specific implementing or delegated acts require procedures to deal with contracted activities in a wider scope, where information security should be integrated.
	Guidance on Part-IS implementation
	This requirement relates only to ISMS activities (e.g. internal audits, risk assessments), not to those activities not directly related to ISMS itself (e. g. hardware, software, IT and OT). The difference in the requirements of IS.OR.235 is that they are limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, etc.). The controls in ISO/IEC 27001 do not exclude those kinds of services, but sometimes they will not be in the focus of the organisation. Therefore, there is no need to establish an independent system for those contractors referred to in IS.OR.235(a). The list of suppliers should be reviewed to ensure that the suppliers providing the services mentioned in IS.OR.235 are covered.
IS.OR.235(b)	**Related ISO/IEC 27001 clauses and controls**
	A5.20 Addressing information security within supplier agreements
	Part-IS particularity
	Access provided to the authority is not covered in ISO/IEC 27001.
	Guidance on Part-IS implementation
	Organisations subject to Part-IS are required to provide access to the competent authority. If the contracted organisation is approved by an authority of another Member State, the different competent authorities will coordinate on which authority will perform oversight of the organisation according to their authority procedures (e.g. Regulation (EU) No 965/2012, ARO.GEN.300(e)). For contracted organisations not subject to Part-IS, GM1 IS.OR.235(b) provides the content to be introduced either in the 'General Terms and Conditions of Trade' of the contracting organisation, or if standard General Terms and Conditions are used (e. g. for COTS-products), the content of the GM shall be arranged on a contractual basis (e. g. through a side letter). AMC1.IS.OR.235(b) should be considered in conjunction with ISO/IEC 27001 A5.20.
IS.OR.240(a)	**Related ISO/IEC 27001 clauses and controls**

IS.OR.240(e)	5.1 Leadership and commitment 5.3 Organisational roles, responsibilities and authorities 7.1 Resources A5.2 Information security roles and responsibilities
	Part-IS particularity
	ISO/IEC 27001 does not require a specific role such as the ‘accountable manager’ or ‘head of the design organisation’.
	Guidance on Part-IS implementation
	The implementation of the requirements of IS.OR.240 (a) can be covered by the implementation of ISO/IEC 27001 requirements mentioned above, provided that the role of accountable manager/head of the design organisation is clearly defined and meets the requirements in (a). The requirement of (a)(3) shall be set in line with the roles in A5.2 (where an accountable manager or the head of the design organisation is not envisaged). However, the measures in A6.3 should be used to ensure the competency of the accountable manager or the head of the design organisation (IS.OR.240(a)(3)).

IS.OR.240(b)
IS.OR.240(c)
	Related ISO/IEC 27001 clauses and controls

	5.3 Organisational roles, responsibilities and authorities 7.1 Resources A5.2 Information security roles and responsibilities A5.3 Segregation of duties
	Part-IS particularity
	This requirement is not directly addressed in ISO/IEC 27001.
	Guidance on Part-IS implementation
	The implementation of the requirements of A5.2 and A5.3 should be used as a basis to fulfil the provisions of IS.OR.240 (b) and (c), but some adaptation may be needed. This issue is covered in A5.2, but A5.3 may also be applicable. In addition, similar requirements for the ‘safety roles’ are laid down in the domain specific ‘safety’ implementing or delegated acts of Regulation (EU) 2018/1139. AMC1 IS.OR.240(b) should be considered.
IS.OR.240(d)	**Related ISO/IEC 27001 clauses and controls**
	4.3 Determining the scope of the information security management system A5.2 Information security roles and responsibilities A5.3 Segregation of duties
	Part-IS particularity

	The implementation of the requirements of A5.2 and A5.3, as well as the guidance of ISO/IEC 27002, allow the delegation of responsibility within organisations.
	Guidance on Part-IS implementation
	This option might be useful for large organisations or groups, where the ISMS is implemented as an ‘umbrella function’ over a group of organisations, where not all of them are subject to Part-IS. The implementation of a ‘group CISO’ or an enterprise-wide ISMS could make use of this option in Part-IS. Nevertheless, the common responsible person has to fulfil the competency requirements of IS.OR.240(a)(3). This might be relevant in cases where the other activities of the organisation or group are not related to aviation.
IS.OR.240(f)	**Related ISO/IEC 27001 clauses and controls**
	7.1 Resources
	Part-IS particularity
	The requirements of 7.1 should be implemented.
	Guidance on Part-IS implementation
	A systematic capacity planning of human resources is a key element of any management system. Therefore, such a process should have been established in an ISMS. The possible additional requirement induced by Part-IS shall be assessed and the capacity planning updated accordingly. The targeted safety levels set in the safety/information security assessment should never be jeopardised by a lack of resources, even temporarily. AMC1 IS.OR.240(f) should be considered.
IS.OR.240(g)	**Related ISO/IEC 27001 clauses and controls**
	7.2 Competency A6.3 Information security awareness, education and training
	Part-IS particularity
	The implementation of the requirements of 7.2 and A6.3 is sufficient to cover the requirement.
	Guidance on Part-IS implementation
	A systematic competency management process of staff is a key element of any management system. Therefore, such a process should have been established in an ISMS. The possible additional requirement induced by Part-IS shall be assessed and the competency requirements updated accordingly. AMC1 IS.OR.240(g) should be considered.
IS.OR.240(h)	**Related ISO/IEC 27001 clauses and controls**

	A6.2 Terms and conditions of employment
	Part-IS particularity
	The implementation of the requirements of A6.2 with some adaptation would be sufficient to cover the provision of IS.OR.240(h).
	Guidance on Part-IS implementation
	IS.OR.240(h) is (at least partially) covered by ISO/IEC 27001 A.6.2 ‘The employment contractual agreements shall state the personnel’s and the organisation’s responsibilities for information security.’ and A.6.4 ‘disciplinary process’ (see ‘Just Culture’). It depends on the organisational culture and on whether job descriptions or role assignments need to be formally acknowledged. In many organisations, the assigned jobs and roles are mutually acknowledged by performing the tasks assigned.
IS.OR.240(i)	**Related ISO/IEC 27001 clauses and controls**
	A5.19 Information security in supplier relationships A6.1 Screening A7.2 Physical entry A8.3 Information access restriction A8.5 Secure authentication
	Part-IS particularity
	The implementation of the requirements of A5.19, A6.1, A7.2, A8.3 and A8.5 might be sufficient controls to cover this requirement for the personnel of the organisation, as well as for contractors and suppliers.
	Guidance on Part-IS implementation
	All the controls established in an ISO/IEC 27001-compliant ISMS are designed to ensure the confidentiality and integrity of information. The implementation of those controls will provide sufficient protection to ensure compliance with this requirement. AMC1 IS.OR.240(i) should be considered.
IS.OR.245(a)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information A5.9 Inventory of information and other associated assets A5.13 Labelling of information A8.10 Information deletion A8.13 Information backup
	Part-IS particularity

	Record-keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.9, A5.13, A8.10 and A8.13 also apply.
	Guidance on Part-IS implementation
	Chapter 7.5.1 b) states that the ISMS shall include 'documented information determined by the organisation as being necessary for the effectiveness of the information security management system.' This includes the records defined in IS.OR.245(a)(1). Chapter 7.5.3 requires, under f), also document control for retention and disposition. Part-IS requirements shall be integrated into the existing system, especially the minimum duration of record-keeping of 5 years. The minimum set of records, as defined in IS.OR.245(a)(1) should be covered in the inventory of assets. For the coverage, the content of GM1 IS.OR.245 also applies. As records are not only information assets, the requested 'record retention policy' may be integrated into a wider policy as recommended by ISO/IEC 27002:2022 above. AMC1 IS.OR.245(a)(1)(vi)&(a)(5) should be implemented.
IS.OR.245(b)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information A5.9 Inventory of information and other associated assets A5.10 Acceptable use of information and other associated assets A5.13 Labelling of information A5.34 Privacy and protection of personal identifiable information (PII) A8.10 Information deletion A8.13 Information backup
	Part-IS particularity
	Record-keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.9, A5.13, A8.10 and A8.13 will also apply and, due to GDPR issues specifically, also A5.10 and A5.34.
	Guidance on Part-IS implementation
	Chapter 7.5.1 b) states that the ISMS shall include 'documented information determined by the organisation as being necessary for the effectiveness of the information security management system.' This includes the records defined in IS.OR.245(a)(1). Chapter 7.5.3 requires, under f), also document control for retention and disposition. Part-IS requirements shall be integrated into the existing system, especially the minimum duration of record-keeping of 5 years. However, whereas there is no retention duration specified in ISO/IEC 27001, IS OR.245(a) specifies 3 years after the person has left the organisation. As these records fall under the GDPR Regulation, each organisation has to ensure that they are handled accordingly. It is recommended that the procedures are used not only for records related to ISMS, but also for the entire HR personnel files of the staff.

IS.OR.245(c)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information A5.13 Labelling of information
	Part-IS particularity
	Record-keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001 as well as the control A5.13.
	Guidance on Part-IS implementation
	Chapter 7.5.3 requires, under a), that ‘it is available and suitable for use, where and when it is needed’. Part-IS requirements shall be integrated into the existing system. ISO 27002:2022 A5.13 states ‘Procedures for information labelling should cover information and other associated assets in all formats.’; therefore, the Part-IS requirement is fulfilled with control A5.13. A series of AMC material to the implementing and delegated acts regarding safety (e.g. AMC1 ARA.GEN.220(a), AMC1 145.A.55) also covers this issue.
IS.OR.245(d)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information A5.10 Acceptable use of information and other associated assets A5.12 Classification of information A5.33 Protection of records A8.12 Data leakage prevention
	Part-IS particularity
	Record-keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.10, A5.12, A5.33 and A8.12 will also apply.
	Guidance on Part-IS implementation
	Chapter 7.5.3 requires, under d), that ‘storage and preservation, including the preservation of legibility’. Part-IS requirements shall be integrated into the existing system. The application of A5.33 and A8.12 has a strong relationship to A7.5 (Protecting against physical and environmental threats), A7.10 (Storage media), A8.3 (Information access restriction), A8.13 (Information backup), A8.14 (Redundancy of information processing facilities), A8.15 (Logging), A8.17 (Clock synchronization) and A8.24 (Use of cryptography).
IS.OR.250(a)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information A5.13 Labelling of information

	Part-IS particularity
	Document control is an inherent part of the ISMS under 7.5 of ISO/IEC 27001. The control A5.13 is also an 'anchor point' for this requirement. ISO/IEC 27001 does not specifically request a document called 'information security management manual', made available to the authority.
	Guidance on Part-IS implementation
	Chapter 7.5.1 b) states that the ISMS shall include 'documented information determined by the organisation as being necessary for the effectiveness of the information security management system' which will allow the inclusion of the ISMS manual in the documentation. Part-IS requires a specific ISMS manual, made available to the competent authority. It shall be made clear to the competent authority which set of documented information constitutes the 'approved manual'. The document 'statement of applicability' (SOA), mandatory for all ISO/IEC 27001-certified organisations may be helpful (e.g. by adding an additional column to label specific documents as part of a 'virtual' ISMS Manual). GM1 IS.OR.250(a) also provides associated guidance. It has to be ensured that all information listed in IS.OR.250(a) is covered.

IS.OR.250(b)
IS.OR.250(c)
	Related ISO/IEC 27001 clauses and controls

	7.5 Documented information A5.5 Contact with authorities
	Part-IS particularity
	Document control is an inherent part of the ISMS under 7.5 of ISO/IEC 27001.
	Guidance on Part-IS implementation
	The use of the same procedure as the one implemented for the 'safety regulations' (see above) is recommended also for the approval, update and communication processes with the competent authority. Many organisations have their documented information available via document management systems (e.g. MS SharePoint). The access of the competent authority to these systems has to be managed in accordance with the rules of any other external access in respect of A5.15, A5.18, A6.6, A7.9, A8.3, A8.7, A8.11, and A8.24.
IS.OR.250(d)	**Related ISO/IEC 27001 clauses and controls**
	7.5 Documented information
	Part-IS particularity
	This requirement (which is not mandatory) has no specific counterpart in ISO/IEC 27001. However, by following the ISO 'Annex SL' structure, ISO/IEC 27001 enables an easy integration of other management system standards.
	Guidance on Part-IS implementation

	There is a tendency in the aviation industry to integrate different management systems, depending on the structure of the organisation.
IS.OR.255(a)	**Related ISO/IEC 27001 clauses and controls**
	6.3 Planning of changes A5.5 Contact with authorities
	Part-IS particularity
	Change management is an inherent part of the ISMS under 6.3 of ISO/IEC 27001, but there is no provision for approval of a procedure by a competent authority.
	Guidance on Part-IS implementation
	The use of the same procedure as the one implemented for the 'safety regulations' (see above) is recommended also for the approval of changes not requiring prior approval by the competent authority. This procedure should be extended to Part-IS in agreement with the competent authority. *Note:* *This recommendation will only work if the competent authority is the authority as laid down in Article 6(1) of Regulation (EU) 2023/203 or Article 5(1) of Regulation (EU) 2022/1645.*
	WARNING: ***An organisation with a derogation approval in accordance with IS.OR.200(e) needs to assess for all changes (also those not requiring prior approval) whether the criteria for the approved derogation are still valid. If not, the change needs the approval of the competent authority/authorities prior to implementation of the change.***
IS.OR.255(b)	**Related ISO/IEC 27001 clauses and controls**
	6.3 Planning of changes A5.5 Contact with authorities
	Part-IS particularity
	Change management is an inherent part of the ISMS under 6.3 of ISO/IEC 27001. However, ISO/IEC 27001 does not require any kind of approval by a competent authority.
	Guidance on Part-IS implementation
	The use of the same procedure as the one implemented for the 'safety-regulations' (see above) is recommended also for the approval of changes in agreement with the competent authority. *Note:* *This recommendation will only work if the competent authority is the authority as laid down in Article 6(1) of Regulation (EU) 2023/203 or Article 5(1) of Regulation (EU) 2022/1645.*

IS.OR.260(a)	**Related ISO/IEC 27001 clauses and controls**
	9.3 Management review 10.1 Continual improvement A5.35 Independent review of information security
	Part-IS particularity
	This requirement reflects a combination of requirements 9.3 and 10.1 of ISO/IEC 27001 with references to requirements 4.4 and 5.2. While ISO/IEC 27001 focuses on ISMS suitability, adequacy and effectiveness, IS.OR.260(a) requires also a periodical maturity assessment of the ISMS be also periodically assessed.
	Guidance on Part-IS implementation
	ISO/IEC 27001, 4.4 shows a clear requirement ('shall') for ISMS maintenance and improvement. The top management has a responsibility for continuous ISMS improvement as per ISO/IEC 27001 5.2(d). The planning section also requires continuous improvement (ISO/IEC 27001 6.1.1(c)). IS.OR.260(a) requires an assessment of the effectiveness and maturity of the ISMS on a calendar basis or following an information security incident. This assessment should be performed by using indicators. ISO/IEC 27001 Chapter 9.3.1 defines a very similar approach for the management review process. Chapter 10.1 indicates a more independent process to improve the ISMS. The process in Chapter 10.1 is seen as more of a bottom-up approach, whereas that in Chapter 9.3 is intended to be top-down. The results from A5.35 should all be used as inputs for continuous improvement. IS.OR.260(a) requires also a maturity assessment of the ISMS. Each organisation should establish which maturity model will be followed and which targeted maturity level is expected to be reached and by when. For the maturity assessment, point (b) of AMC1 IS.OR.260 (a) and GM1 IS.OR.260(a) provides guidance on how to ensure compliance with IS.OR.260 (a).
IS.OR.260(b)	**Related ISO/IEC 27001 clauses and controls**
	10.2 Non-conformity and corrective action A5.7 Threat intelligence
	Part-IS particularity
	IS.OR.260(b) addresses the improvement measures, i.e. corrections and corrective actions for the deficiencies detected in IS.OR.260(a) and the continuous improvement process. This requirement reflects mainly requirement 10.2 of ISO/IEC 27001, even if the term used is 'non-conformity', while IS.OR.260(b) uses the term 'deficiencies'. Deficiency has a broader meaning than non-conformity. It encompasses the case of a targeted maturity level that would not be reached at the planned date; that would be a deficiency but not necessarily a non-conformity.

	Guidance on Part-IS implementation
	The provisions listed in ISO/IEC 27001 10.2 can be used to take corrective actions, to resolve both non-conformities and maturity level gaps.

Appendix V — Proportionality considerations related to indicators of complexity

The following is a non-exhaustive list of activities related to the implementation of the ISMS under this Regulation that may be performed in a manner proportional to each complexity indicator.

1. Organisation role in the functional chain, and number and criticality of interfacing organisations

The organisation's position in the functional chain and its overall contribution to the safety of related functional processes are key indicators of complexity. This should impact the depth of risk assessment required and the level of assurance needed to ensure the effectiveness of measures implemented to mitigate unacceptable risks.

For organisations whose position in the functional chain and their interfaces do not pose a risk of unsafe conditions, the following approach may be adopted:

Risk assessment and treatment

— **Simplified risk assessment**: A streamlined risk assessment process that prioritises risks based on their potential impact on safety is used. The assessment focuses on high-impact areas; more detailed assessments are performed only where and if necessary.

— **Risk treatment prioritisation**: A risk treatment plan that prioritises high-impact risks with cost-effective measures is adopted. In such cases, cost-effective controls that reduce risks to acceptable levels may be used. These controls can often leverage existing processes, physical controls or technology.

For organisations whose position in the functional chain and their interfaces may pose a risk of unsafe conditions, the following approach should be adopted:

Risk assessment and treatment

Detailed risk assessments: Detailed and often more frequent risk assessments are carried out.

2. Complexity of the organisational structure and hierarchies

The complexity of an organisation's structure — typically determined by the number of staff, departments and hierarchical layers — directly influences the level of internal coordination required and the extent to which information exchange needs to be formalised and proceduralised.

For organisations characterised by a combination of limited number of staff members, few hierarchical layers and departments, the following approaches may be adopted:

(a) Policy and procedure simplification

— **Streamlined documentation:** Policies and procedures can be concise, clear and easy to understand. Overly complex documents are avoided to ensure the usability by a small team. Templates and frameworks may be used in order to speed up the creation of the necessary documentation.

— **Focus on key policies:** During the development, the key policies have been prioritised in order to address the most critical aspects of information security, such as management commitment, access control and incident response.

(b) Employee training and awareness

— **Targeted training programmes**: Focused training programmes that target the specific roles and responsibilities of employees are provided. The training should be relevant to the organisation's specific risks and operational context.

— **Security culture:** A culture of security awareness is encouraged throughout the organisation. Short training sessions and awareness campaigns are conducted on a regular basis.

(c) Outsourcing and partnerships

— **Outsourcing**: For areas where the organisation lacks expertise, outsourcing to providers of managed-security services is adopted.

— **Collaboration with peers:** Information-sharing with similar organisations (e.g. through the European Centre for Cyber Security in Aviation (ECCSA)) or industry groups is carried out. Collaboration provides insights to evaluate the evolution of the security environment with limited effort.

(d) Engagement with management

Simplified management reporting: Reports to management are concise, and focused on key metrics that demonstrate the effectiveness of the ISMS. Continued support and resource allocation from top management is ensured.

(e) Compliance monitoring and continuous improvement

— **Regular but scaled audits**: Internal audits are regularly conducted, but the effort is scaled to the organisation's size and complexity. The focus should be on the most critical areas and the audit results should be provided to the accountable manager or the head of the design organisation and utilised to guide continuous improvement.

— **Agile review process**: The ISMS should be regularly reviewed and, if necessary, adapted to ensure that it remains aligned with the organisation's evolving needs and threats.

For organisations characterised by a combination of large number of staff members, hierarchical layers and departments and interfaces, the following approaches should be adopted:

(a) Robust governance structure

— **Information security governance committees**: Governance committees to oversee the ISMS should be present, to ensure alignment with the organisation's safety and security objectives. These committees should include representation from senior management, IT, legal and key business units.

— **Metrics and reporting**: Comprehensive metrics and reporting structures to track the effectiveness of the ISMS should be implemented. Report on key performance indicators

(KPIs) to senior management and the management board should be provided to ensure ongoing support and resource allocation.

(b) Extensive policy and procedure framework

- **Detailed policies and procedures**: More complex organisations need a more extensive set of policies and procedures to cover various business units, compliance requirements and operational processes. This includes specialised policies for areas like cloud security, third-party management and mobile device management.
- **Policy harmonisation**: Ensure that policies are harmonised across the organisation to avoid conflicting practices between different departments or regions. This requires a centralised governance model to oversee policy development and enforcement.

(c) Risk assessment and treatment

- **Cross-risk assessments:** Cross-risk assessments include assessing risks across various departments, geographic locations and technological platforms.
- **Risk aggregation and correlation**: With a larger volume of information, risks assessments should be aggregated and correlated to identify systemic issues and ensure that risks are managed and escalated at an organisational level, not just within individual silos.

(d) Comprehensive training and awareness programmes

- **Role-based Training**: Extensive role-based training programmes tailored to different functions within the organisation are implemented. For example, IT staff, executives and end-users all have different levels of training specific to their roles.
- **Continuous security awareness campaigns**: Security awareness campaigns using various methods (e.g. phishing simulations, workshops and e-learning modules) are continuously deployed to keep security top-of-mind for all employees across the organisation.

(e) Enhanced contracted activities management

- **Supply chain risk management**: Thorough security assessments of contracted organisations and ongoing monitoring of third-party risks should be carried out. Security requirements should be integrated into contracts.
- **Third-party audits**: Regular audits of contracted organisations should be conducted in order to ensure they comply with the organisation’s security objectives.

(f) Comprehensive incident management

- **Dedicated security operations centre (SOC)**: A dedicated SOC should be established in order to monitor security events 24/7, manage incidents and coordinate response efforts across the enterprise.
- **Complex incident response plans**: Detailed incident response plans that cover a variety of scenarios, including cross-departmental coordination, communication strategies and operational continuity planning should be developed and maintained.

- **Crisis simulation exercises**: Crisis simulation exercises that involve key stakeholders across the organisation are regularly conducted to test the effectiveness of incident response and operational continuity plans.

(g) Continuous improvement and compliance monitoring programmes

- **Internal and external audits**: Comprehensive internal and external audits are regularly conducted to assess compliance with the ISMS and identify areas for improvement.
- **Continuous improvement programmes**: A continuous improvement process to update and refine the ISMS based on audit findings, incident post-mortems and changes in the threat landscape is implemented.

3. Complexity of the ICT systems and data used by the organisation

The complexity of the information and communication technology systems and data used by the organisation, and their connection to external parties directly influences the level of customisation and tailoring required for risk management and incident detection, response and recovery.

For organisations characterised by a combination of usage of a few ICT tools and utilisation of standard ICT products, the following approaches may be adopted:

(a) Use of standards and tools

- **Leverage ISO/IEC 27001 controls**: Usage of the ISO/IEC 27001 Annex A controls as a checklist to ensure that all critical areas are covered while reducing the effort of designing controls from scratch. In such cases, the Part-IS vs ISO/IEC 27001 comparison guide shall be referenced to ensure that Part-IS specificities have been correctly addressed.
- **Simplified incident management:** A basic incident management process that allows for quick identification, reporting and response to security incidents is adopted. Lessons learned from incidents should be in any case integrated into the ISMS for continuous improvement.
- **Automated tools**: Automated tools for monitoring, logging and managing security incidents are used in order to reduce manual effort while maintaining continuous compliance.

(b) Documentation and record-keeping

- **Essential records**: Only records that are essential to demonstrate compliance and the effectiveness of the ISMS are kept. Excessive documentation that does not add value or is burdensome to maintain is avoided.
- **Use of digital solutions:** Digital tools are used for document management to simplify access and version control, and to ensure the security of records.

For organisations characterised by a combination of usage of several and diverse ICT tools, amongst which bespoke ICT solutions, the following approaches should be adopted:

(a) Advanced security technologies

— **Integration of advanced security tools**: Security technologies like security information and event management (SIEM), data loss prevention (DLP), and endpoint detection and response (EDR) systems should be utilised to help manage the scale and complexity of monitoring, detecting and responding to security incidents across the organisation.

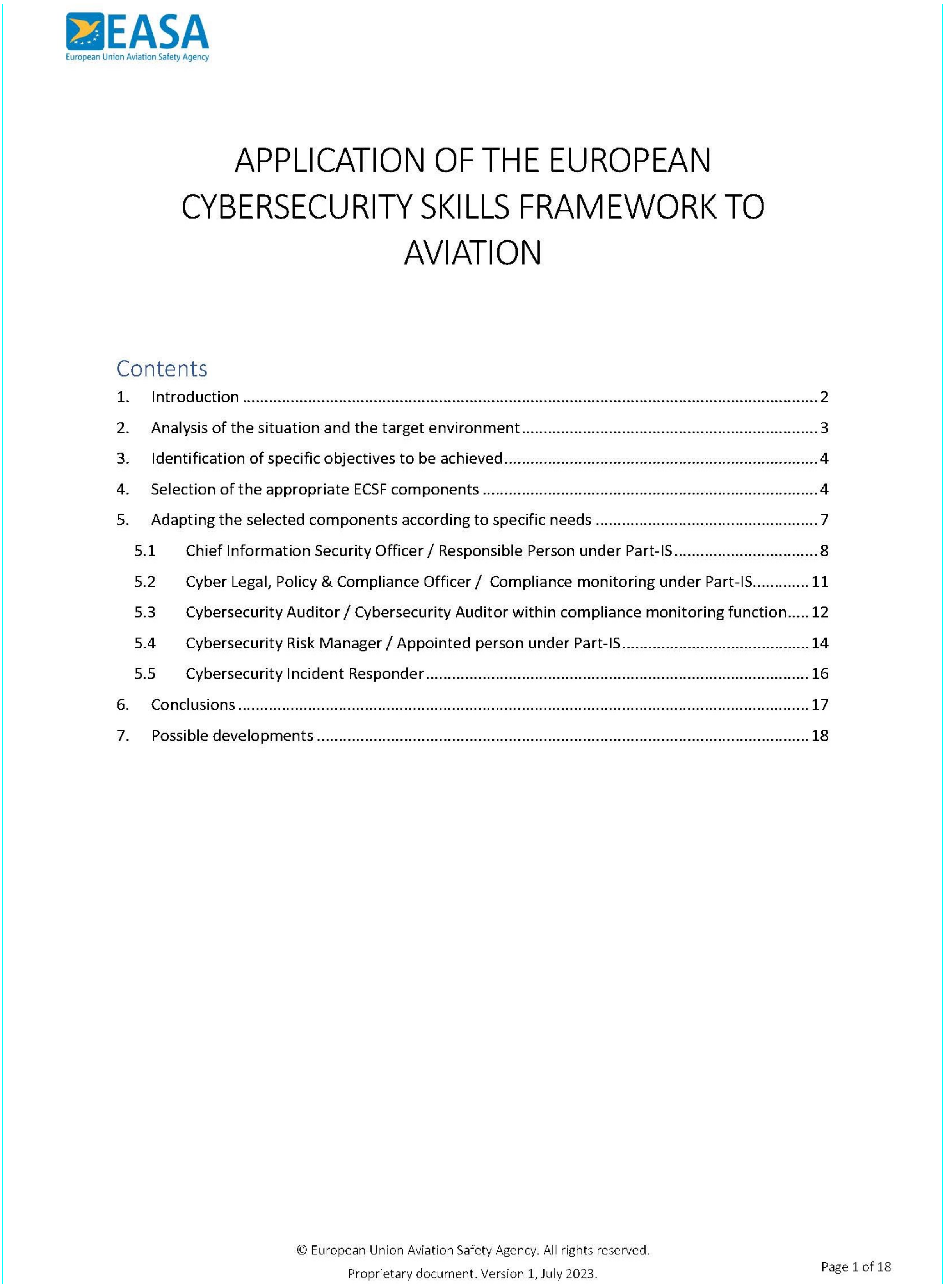
— **Automated threat intelligence**: Automated threat intelligence platforms should be used to enable real-time threat detection and response across the broad threat surface.

(b) Extensive record-keeping and documentation

— **Detailed documentation**: An extensive documentation of all ISMS processes, risk assessments, incident reports and compliance activities is carried out.

— **Record retention**: Records and data are widely collected, retained and securely stored, and are accessible over extended periods.

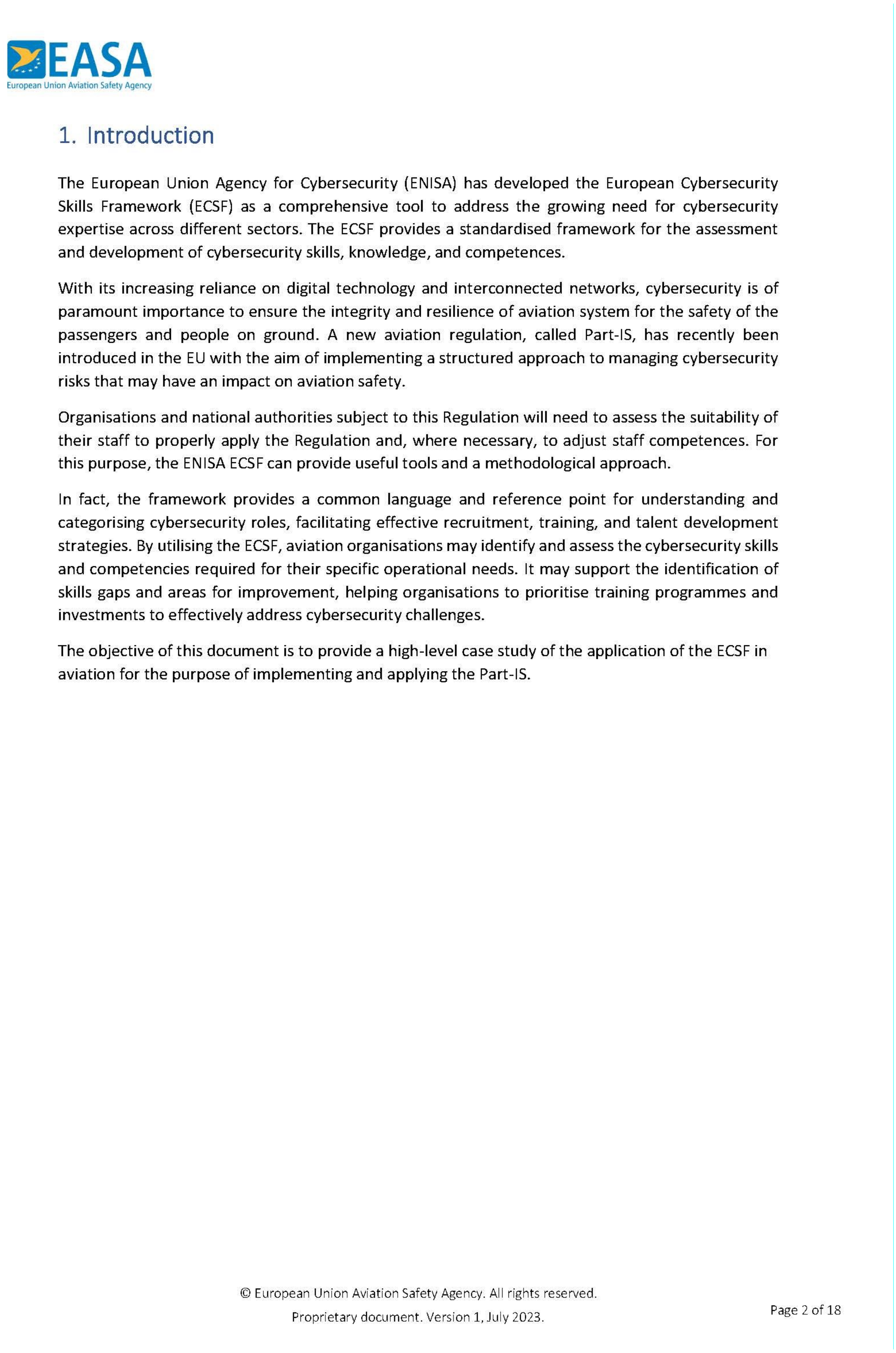
Appendix VI — Adaptation of the EU Cybersecurity Skills Framework (ECSF)



APPLICATION OF THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK TO AVIATION

Contents

1. Introduction 2
2. Analysis of the situation and the target environment 3
3. Identification of specific objectives to be achieved 4
4. Selection of the appropriate ECSF components 4
5. Adapting the selected components according to specific needs 7
   5.1 Chief Information Security Officer / Responsible Person under Part-IS 8
   5.2 Cyber Legal, Policy & Compliance Officer / Compliance monitoring under Part-IS..... 11
   5.3 Cybersecurity Auditor / Cybersecurity Auditor within compliance monitoring function..... 12
   5.4 Cybersecurity Risk Manager / Appointed person under Part-IS 14
   5.5 Cybersecurity Incident Responder 16
6. Conclusions 17
7. Possible developments 18



1. Introduction

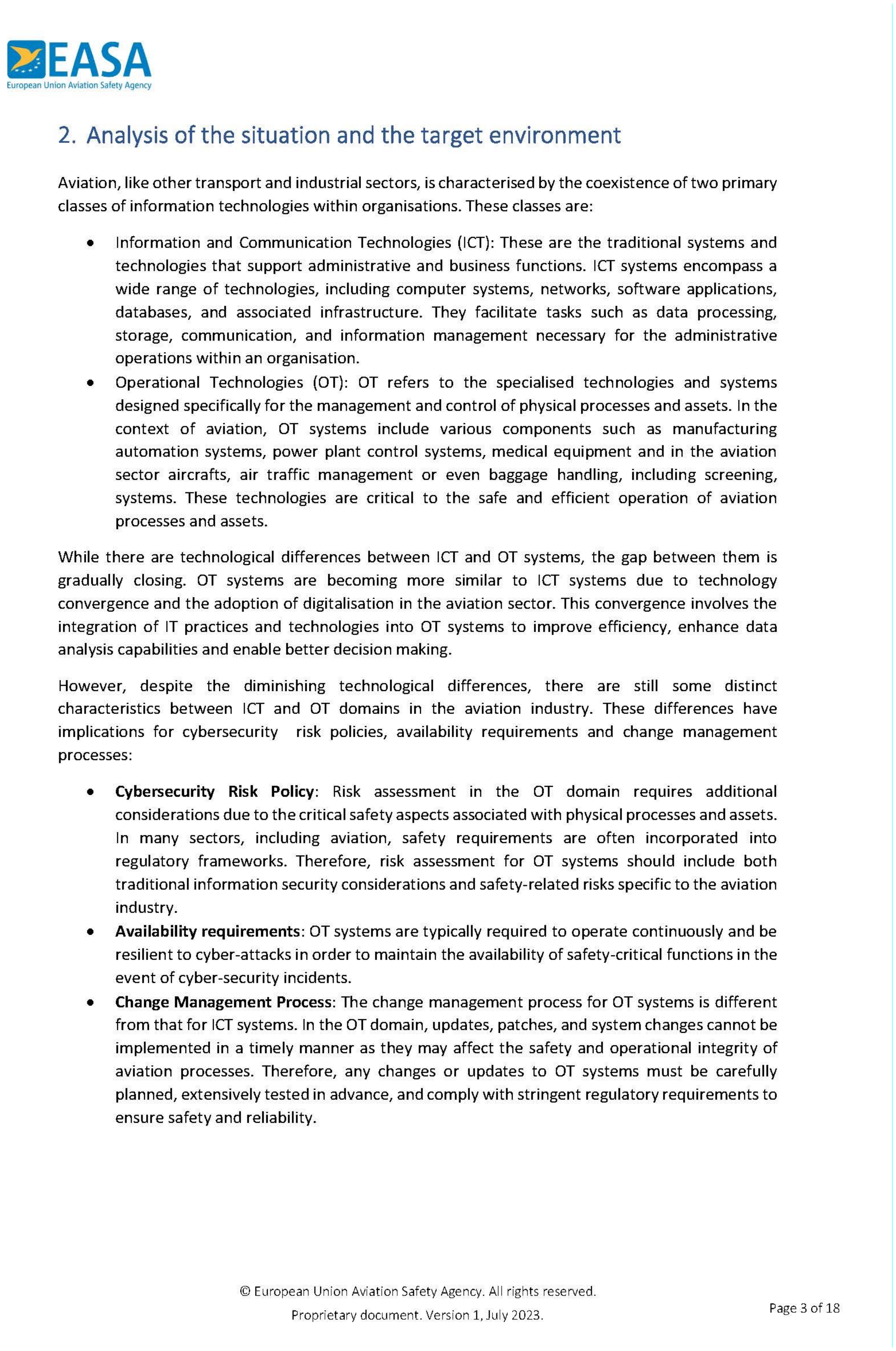
The European Union Agency for Cybersecurity (ENISA) has developed the European Cybersecurity Skills Framework (ECSF) as a comprehensive tool to address the growing need for cybersecurity expertise across different sectors. The ECSF provides a standardised framework for the assessment and development of cybersecurity skills, knowledge, and competences.

With its increasing reliance on digital technology and interconnected networks, cybersecurity is of paramount importance to ensure the integrity and resilience of aviation system for the safety of the passengers and people on ground. A new aviation regulation, called Part-IS, has recently been introduced in the EU with the aim of implementing a structured approach to managing cybersecurity risks that may have an impact on aviation safety.

Organisations and national authorities subject to this Regulation will need to assess the suitability of their staff to properly apply the Regulation and, where necessary, to adjust staff competences. For this purpose, the ENISA ECSF can provide useful tools and a methodological approach.

In fact, the framework provides a common language and reference point for understanding and categorising cybersecurity roles, facilitating effective recruitment, training, and talent development strategies. By utilising the ECSF, aviation organisations may identify and assess the cybersecurity skills and competencies required for their specific operational needs. It may support the identification of skills gaps and areas for improvement, helping organisations to prioritise training programmes and investments to effectively address cybersecurity challenges.

The objective of this document is to provide a high-level case study of the application of the ECSF in aviation for the purpose of implementing and applying the Part-IS.



2. Analysis of the situation and the target environment

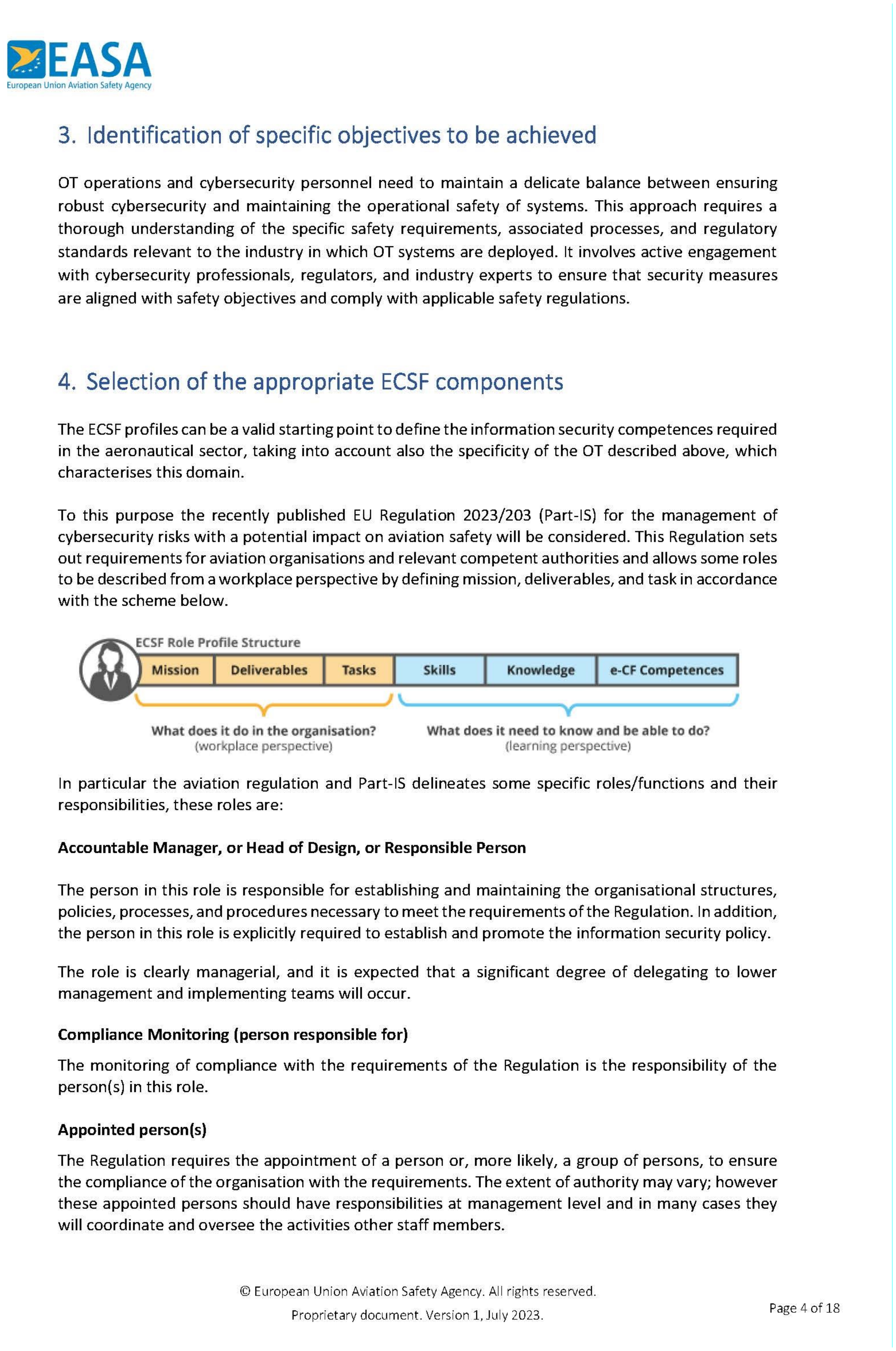
Aviation, like other transport and industrial sectors, is characterised by the coexistence of two primary classes of information technologies within organisations. These classes are:

- Information and Communication Technologies (ICT): These are the traditional systems and technologies that support administrative and business functions. ICT systems encompass a wide range of technologies, including computer systems, networks, software applications, databases, and associated infrastructure. They facilitate tasks such as data processing, storage, communication, and information management necessary for the administrative operations within an organisation.
- Operational Technologies (OT): OT refers to the specialised technologies and systems designed specifically for the management and control of physical processes and assets. In the context of aviation, OT systems include various components such as manufacturing automation systems, power plant control systems, medical equipment and in the aviation sector aircrafts, air traffic management or even baggage handling, including screening, systems. These technologies are critical to the safe and efficient operation of aviation processes and assets.

While there are technological differences between ICT and OT systems, the gap between them is gradually closing. OT systems are becoming more similar to ICT systems due to technology convergence and the adoption of digitalisation in the aviation sector. This convergence involves the integration of IT practices and technologies into OT systems to improve efficiency, enhance data analysis capabilities and enable better decision making.

However, despite the diminishing technological differences, there are still some distinct characteristics between ICT and OT domains in the aviation industry. These differences have implications for cybersecurity risk policies, availability requirements and change management processes:

- **Cybersecurity Risk Policy**: Risk assessment in the OT domain requires additional considerations due to the critical safety aspects associated with physical processes and assets. In many sectors, including aviation, safety requirements are often incorporated into regulatory frameworks. Therefore, risk assessment for OT systems should include both traditional information security considerations and safety-related risks specific to the aviation industry.
- **Availability requirements**: OT systems are typically required to operate continuously and be resilient to cyber-attacks in order to maintain the availability of safety-critical functions in the event of cyber-security incidents.
- **Change Management Process**: The change management process for OT systems is different from that for ICT systems. In the OT domain, updates, patches, and system changes cannot be implemented in a timely manner as they may affect the safety and operational integrity of aviation processes. Therefore, any changes or updates to OT systems must be carefully planned, extensively tested in advance, and comply with stringent regulatory requirements to ensure safety and reliability.



3. Identification of specific objectives to be achieved

OT operations and cybersecurity personnel need to maintain a delicate balance between ensuring robust cybersecurity and maintaining the operational safety of systems. This approach requires a thorough understanding of the specific safety requirements, associated processes, and regulatory standards relevant to the industry in which OT systems are deployed. It involves active engagement with cybersecurity professionals, regulators, and industry experts to ensure that security measures are aligned with safety objectives and comply with applicable safety regulations.

4. Selection of the appropriate ECSF components

The ECSF profiles can be a valid starting point to define the information security competences required in the aeronautical sector, taking into account also the specificity of the OT described above, which characterises this domain.

To this purpose the recently published EU Regulation 2023/203 (Part-IS) for the management of cybersecurity risks with a potential impact on aviation safety will be considered. This Regulation sets out requirements for aviation organisations and relevant competent authorities and allows some roles to be described from a workplace perspective by defining mission, deliverables, and task in accordance with the scheme below.

ECSF Role Profile Structure
Mission
Deliverables
Tasks
Skills
Knowledge
e-CF Competences
What does it do in the organisation?
(workplace perspective)
What does it need to know and be able to do?
(learning perspective)

In particular the aviation regulation and Part-IS delineates some specific roles/functions and their responsibilities, these roles are:

Accountable Manager, or Head of Design, or Responsible Person

The person in this role is responsible for establishing and maintaining the organisational structures, policies, processes, and procedures necessary to meet the requirements of the Regulation. In addition, the person in this role is explicitly required to establish and promote the information security policy.

The role is clearly managerial, and it is expected that a significant degree of delegating to lower management and implementing teams will occur.

Compliance Monitoring (person responsible for)

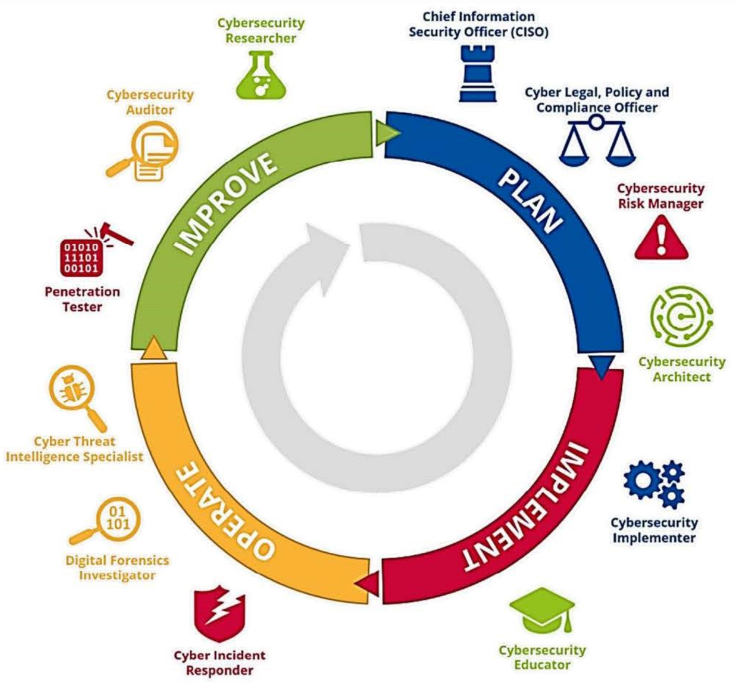
The monitoring of compliance with the requirements of the Regulation is the responsibility of the person(s) in this role.

Appointed person(s)

The Regulation requires the appointment of a person or, more likely, a group of persons, to ensure the compliance of the organisation with the requirements. The extent of authority may vary; however these appointed persons should have responsibilities at management level and in many cases they will coordinate and oversee the activities other staff members.

EASA
European Union Aviation Safety Agency

The ECSF instead proposes 12 standard roles involved in different phases of the management cycle, as illustrated below.


Cybersecurity Researcher
Chief Information Security Officer (CISO)
Cyber Legal, Policy and Compliance Officer
Cybersecurity Auditor
IMPROVE
PLAN
Cybersecurity Risk Manager
Penetration Tester
01010
11101
00101
Cybersecurity Architect
Cyber Threat Intelligence Specialist
OPERATE
IMPLEMENT
Cybersecurity Implementer
01
101
Digital Forensics Investigator
Cyber Incident Responder
Cybersecurity Educator

An initial mapping between the ECSF roles and the roles delineated in Part-IS can be performed by **comparing the deliverables expected from the different roles** as reported in the below Table 1. As described above, some roles are well described in Part-IS, others can be considered expected in order to comply with the requirements of the regulation (e.g. incident detection, response and recovery).

The mapping shows that there are different levels of matching between ECSF and Part-IS roles. Four levels have been used, ranging from "high level of match" to "no match". In more details the rationale for the classification of the level of matching is the following:

- **High level of match**: In the Part-IS regulation, both a role and a deliverable can be found that is very close to the one described in the framework.
- **Not Specified, but expected**: In order to comply with the provisions of Part IS, an organisation is expected to produce the deliverable under the ECSF profile, but the Regulation does not mention a specific role associated with this deliverable.
- **Not Specified, may be useful in complex setting:** Same as the previous level of matching, with the addition that this role may only be justified in complex organisations.
- **Not foreseen:** In the Part-IS regulation, both a matching role and a deliverable cannot be found.

According to the level of match between the roles the following colour background has been used in the table rows:

High level of match	Medium level of match	Low level of match	No match

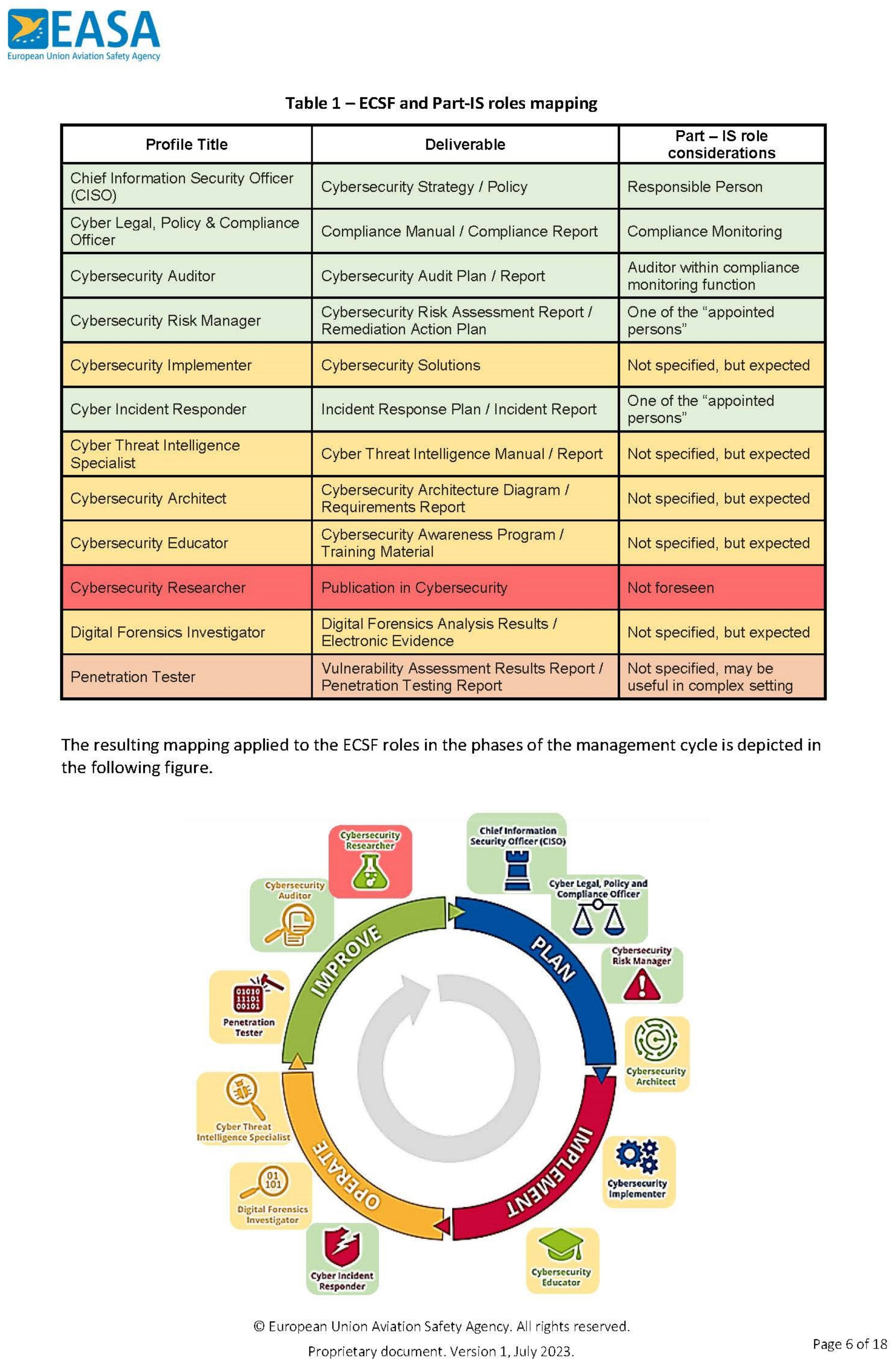


Table 1 – ECSF and Part-IS roles mapping

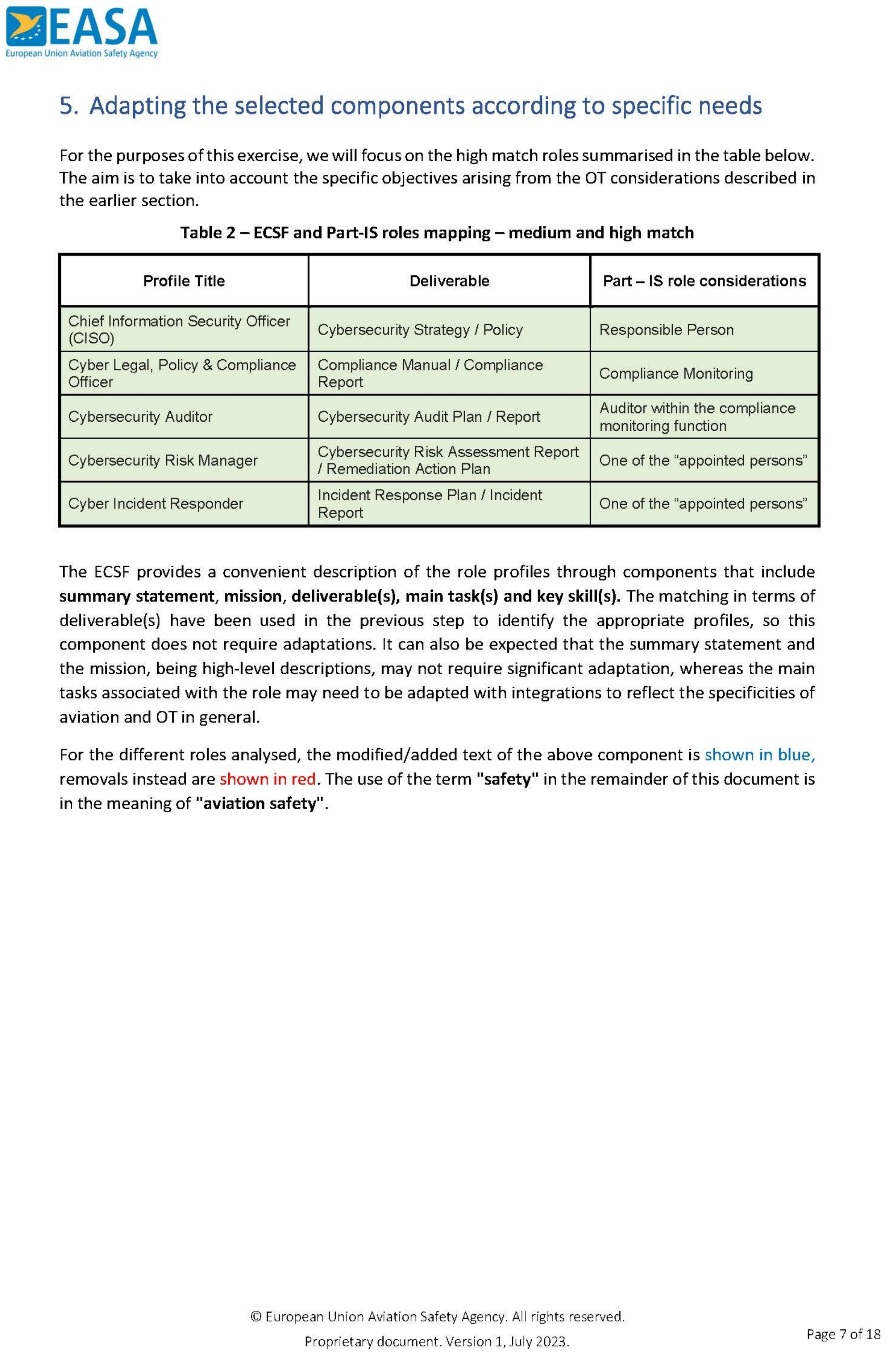
Profile Title	Deliverable	Part – IS role considerations
Chief Information Security Officer (CISO)	Cybersecurity Strategy / Policy	Responsible Person
Cyber Legal, Policy & Compliance Officer	Compliance Manual / Compliance Report	Compliance Monitoring
Cybersecurity Auditor	Cybersecurity Audit Plan / Report	Auditor within compliance monitoring function
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report / Remediation Action Plan	One of the “appointed persons”
Cybersecurity Implementer	Cybersecurity Solutions	Not specified, but expected
Cyber Incident Responder	Incident Response Plan / Incident Report	One of the “appointed persons”
Cyber Threat Intelligence Specialist	Cyber Threat Intelligence Manual / Report	Not specified, but expected
Cybersecurity Architect	Cybersecurity Architecture Diagram / Requirements Report	Not specified, but expected
Cybersecurity Educator	Cybersecurity Awareness Program / Training Material	Not specified, but expected
Cybersecurity Researcher	Publication in Cybersecurity	Not foreseen
Digital Forensics Investigator	Digital Forensics Analysis Results / Electronic Evidence	Not specified, but expected
Penetration Tester	Vulnerability Assessment Results Report / Penetration Testing Report	Not specified, may be useful in complex setting

The resulting mapping applied to the ECSF roles in the phases of the management cycle is depicted in the following figure.

Cybersecurity Researcher
Chief Information Security Officer (CISO)
Cyber Legal, Policy and Compliance Officer
Cybersecurity Risk Manager
Cybersecurity Architect
Cybersecurity Implementer
Cybersecurity Educator
Cyber Incident Responder
Digital Forensics Investigator
01 101
Cyber Threat Intelligence Specialist
Penetration Tester
01010 11101 00101
Cybersecurity Auditor
PLAN
IMPLEMENT
OPERATE
IMPROVE

© European Union Aviation Safety Agency. All rights reserved.
Proprietary document. Version 1, July 2023.

Page 6 of 18



5. Adapting the selected components according to specific needs

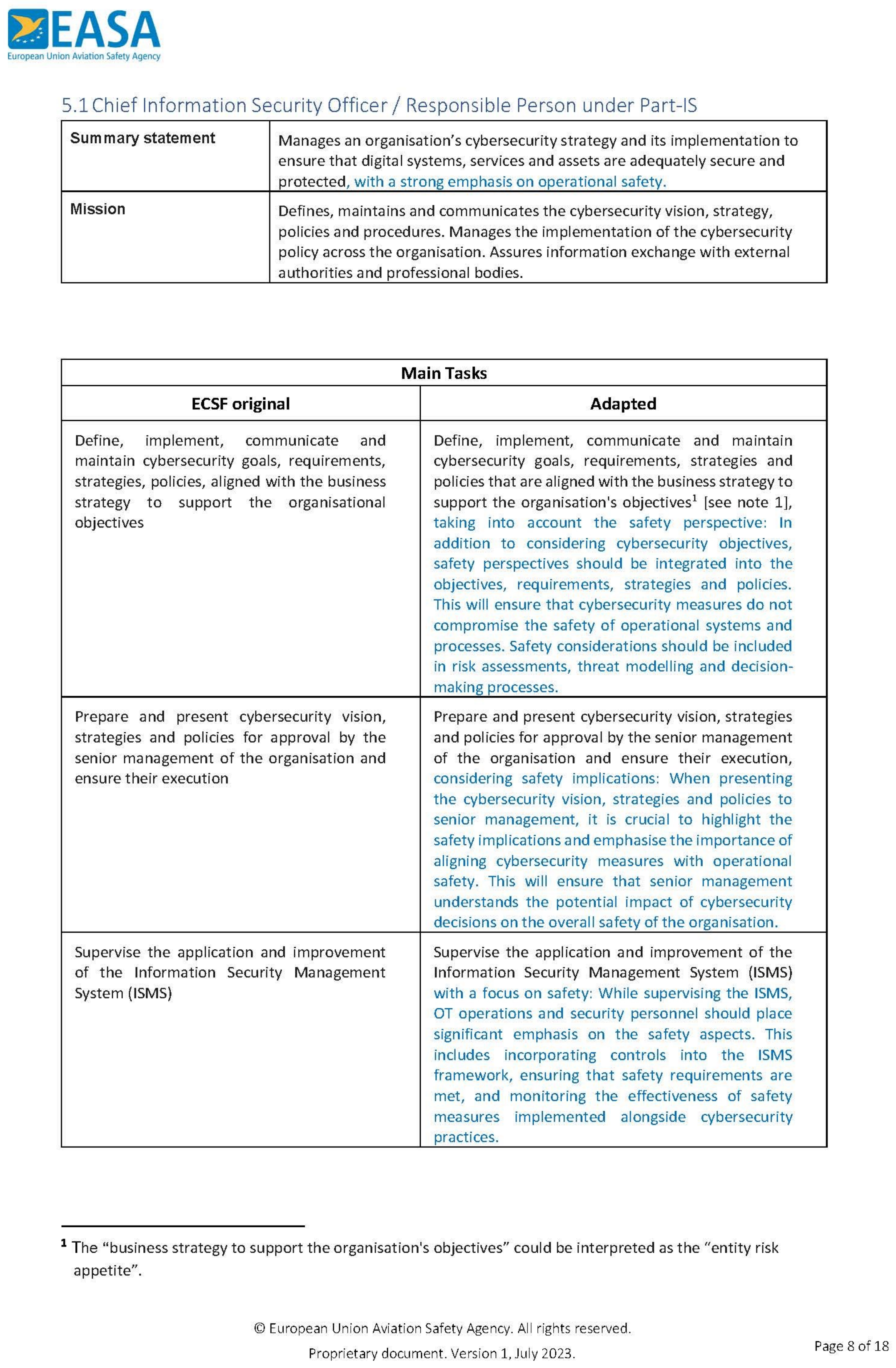
For the purposes of this exercise, we will focus on the high match roles summarised in the table below. The aim is to take into account the specific objectives arising from the OT considerations described in the earlier section.

Table 2 – ECSF and Part-IS roles mapping – medium and high match

Profile Title	Deliverable	Part – IS role considerations
Chief Information Security Officer (CISO)	Cybersecurity Strategy / Policy	Responsible Person
Cyber Legal, Policy & Compliance Officer	Compliance Manual / Compliance Report	Compliance Monitoring
Cybersecurity Auditor	Cybersecurity Audit Plan / Report	Auditor within the compliance monitoring function
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report / Remediation Action Plan	One of the "appointed persons"
Cyber Incident Responder	Incident Response Plan / Incident Report	One of the "appointed persons"

The ECSF provides a convenient description of the role profiles through components that include **summary statement**, **mission**, **deliverable(s), main task(s) and key skill(s).** The matching in terms of deliverable(s) have been used in the previous step to identify the appropriate profiles, so this component does not require adaptations. It can also be expected that the summary statement and the mission, being high-level descriptions, may not require significant adaptation, whereas the main tasks associated with the role may need to be adapted with integrations to reflect the specificities of aviation and OT in general.

For the different roles analysed, the modified/added text of the above component is shown in blue, removals instead are shown in red. The use of the term **"safety"** in the remainder of this document is in the meaning of **"aviation safety"**.

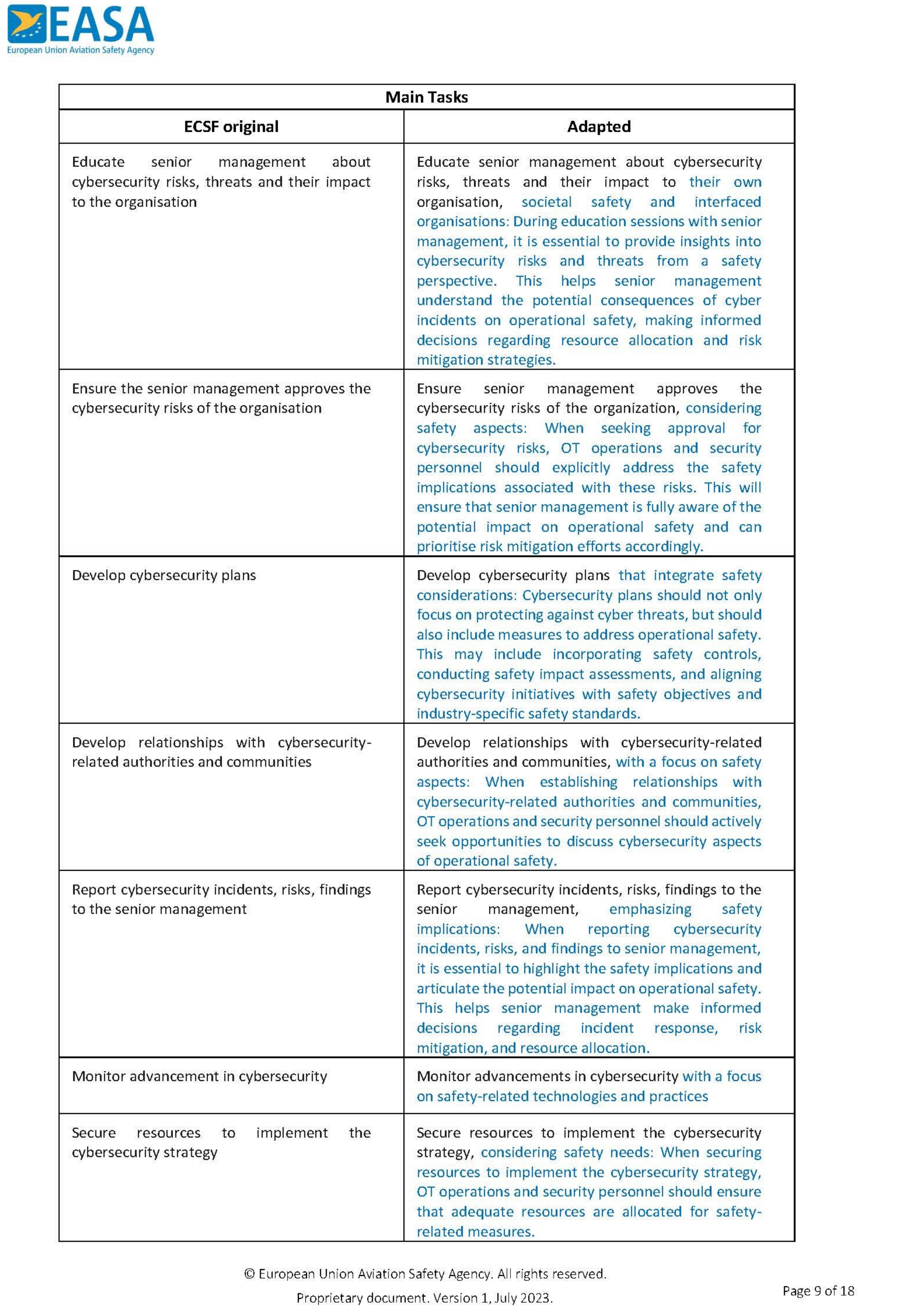


5.1 Chief Information Security Officer / Responsible Person under Part-IS

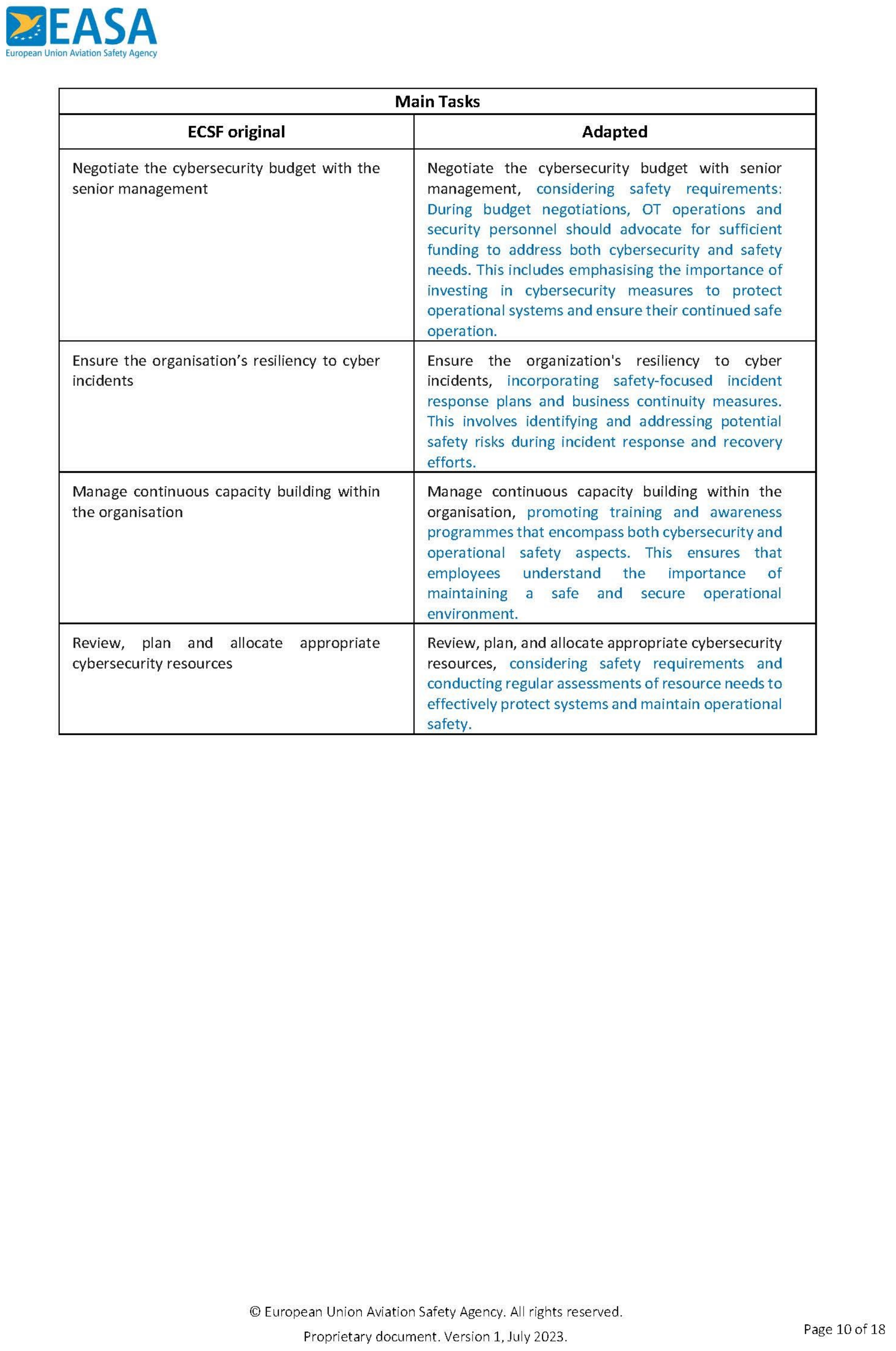
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected, with a strong emphasis on operational safety.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.

Main Tasks	
ECSF original	**Adapted**
Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives	Define, implement, communicate and maintain cybersecurity goals, requirements, strategies and policies that are aligned with the business strategy to support the organisation's objectives[1] [see note 1], taking into account the safety perspective: In addition to considering cybersecurity objectives, safety perspectives should be integrated into the objectives, requirements, strategies and policies. This will ensure that cybersecurity measures do not compromise the safety of operational systems and processes. Safety considerations should be included in risk assessments, threat modelling and decision-making processes.
Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution	Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution, considering safety implications: When presenting the cybersecurity vision, strategies and policies to senior management, it is crucial to highlight the safety implications and emphasise the importance of aligning cybersecurity measures with operational safety. This will ensure that senior management understands the potential impact of cybersecurity decisions on the overall safety of the organisation.
Supervise the application and improvement of the Information Security Management System (ISMS)	Supervise the application and improvement of the Information Security Management System (ISMS) with a focus on safety: While supervising the ISMS, OT operations and security personnel should place significant emphasis on the safety aspects. This includes incorporating controls into the ISMS framework, ensuring that safety requirements are met, and monitoring the effectiveness of safety measures implemented alongside cybersecurity practices.

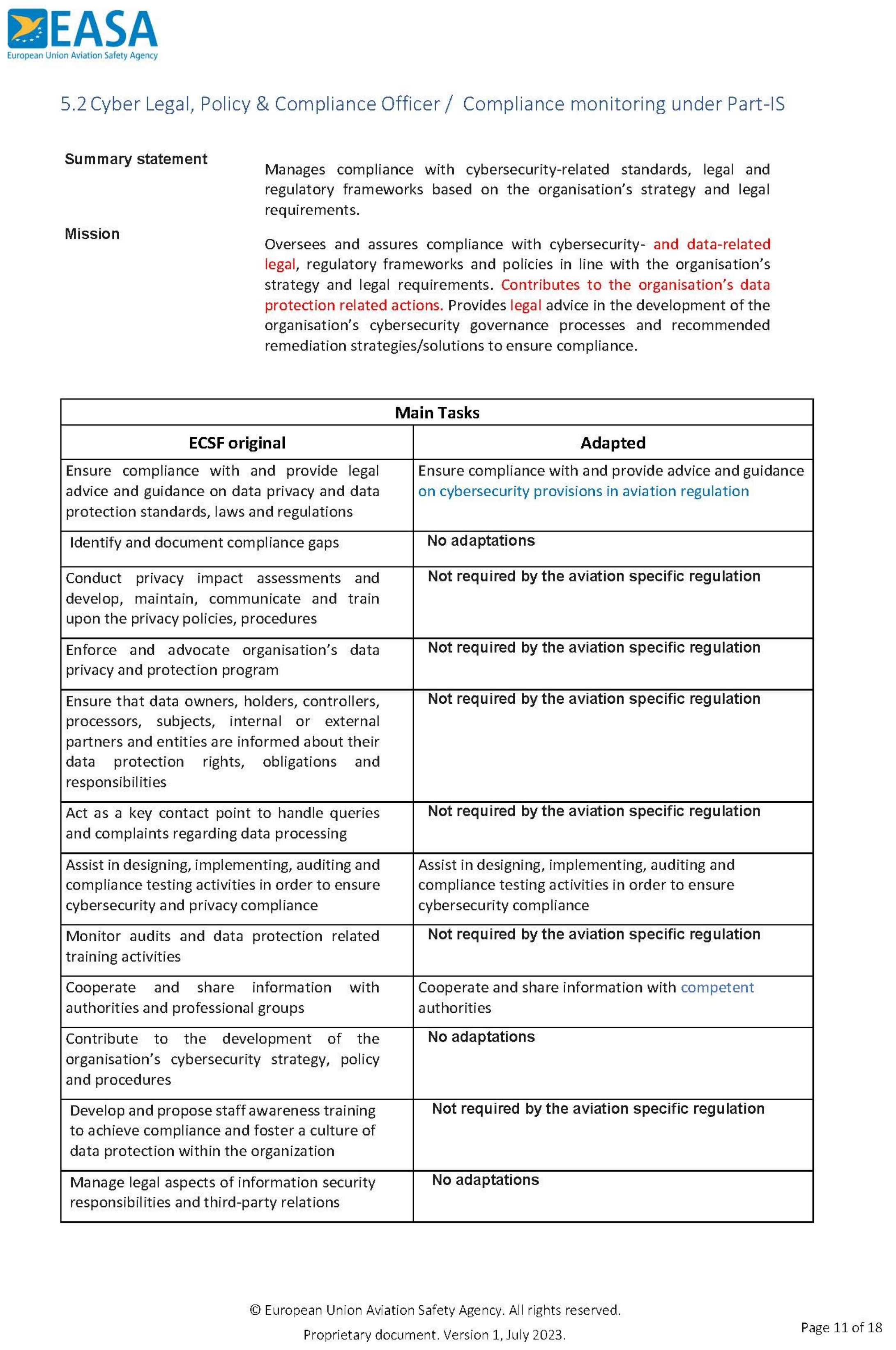
[1] The "business strategy to support the organisation's objectives" could be interpreted as the "entity risk appetite".



Main Tasks	
ECSF original	**Adapted**
Educate senior management about cybersecurity risks, threats and their impact to the organisation	Educate senior management about cybersecurity risks, threats and their impact to their own organisation, societal safety and interfaced organisations: During education sessions with senior management, it is essential to provide insights into cybersecurity risks and threats from a safety perspective. This helps senior management understand the potential consequences of cyber incidents on operational safety, making informed decisions regarding resource allocation and risk mitigation strategies.
Ensure the senior management approves the cybersecurity risks of the organisation	Ensure senior management approves the cybersecurity risks of the organization, considering safety aspects: When seeking approval for cybersecurity risks, OT operations and security personnel should explicitly address the safety implications associated with these risks. This will ensure that senior management is fully aware of the potential impact on operational safety and can prioritise risk mitigation efforts accordingly.
Develop cybersecurity plans	Develop cybersecurity plans that integrate safety considerations: Cybersecurity plans should not only focus on protecting against cyber threats, but should also include measures to address operational safety. This may include incorporating safety controls, conducting safety impact assessments, and aligning cybersecurity initiatives with safety objectives and industry-specific safety standards.
Develop relationships with cybersecurity-related authorities and communities	Develop relationships with cybersecurity-related authorities and communities, with a focus on safety aspects: When establishing relationships with cybersecurity-related authorities and communities, OT operations and security personnel should actively seek opportunities to discuss cybersecurity aspects of operational safety.
Report cybersecurity incidents, risks, findings to the senior management	Report cybersecurity incidents, risks, findings to the senior management, emphasizing safety implications: When reporting cybersecurity incidents, risks, and findings to senior management, it is essential to highlight the safety implications and articulate the potential impact on operational safety. This helps senior management make informed decisions regarding incident response, risk mitigation, and resource allocation.
Monitor advancement in cybersecurity	Monitor advancements in cybersecurity with a focus on safety-related technologies and practices
Secure resources to implement the cybersecurity strategy	Secure resources to implement the cybersecurity strategy, considering safety needs: When securing resources to implement the cybersecurity strategy, OT operations and security personnel should ensure that adequate resources are allocated for safety-related measures.



Main Tasks	
ECSF original	**Adapted**
Negotiate the cybersecurity budget with the senior management	Negotiate the cybersecurity budget with senior management, considering safety requirements: During budget negotiations, OT operations and security personnel should advocate for sufficient funding to address both cybersecurity and safety needs. This includes emphasising the importance of investing in cybersecurity measures to protect operational systems and ensure their continued safe operation.
Ensure the organisation’s resiliency to cyber incidents	Ensure the organization's resiliency to cyber incidents, incorporating safety-focused incident response plans and business continuity measures. This involves identifying and addressing potential safety risks during incident response and recovery efforts.
Manage continuous capacity building within the organisation	Manage continuous capacity building within the organisation, promoting training and awareness programmes that encompass both cybersecurity and operational safety aspects. This ensures that employees understand the importance of maintaining a safe and secure operational environment.
Review, plan and allocate appropriate cybersecurity resources	Review, plan, and allocate appropriate cybersecurity resources, considering safety requirements and conducting regular assessments of resource needs to effectively protect systems and maintain operational safety.



5.2 Cyber Legal, Policy & Compliance Officer / Compliance monitoring under Part-IS

Summary statement

Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements.

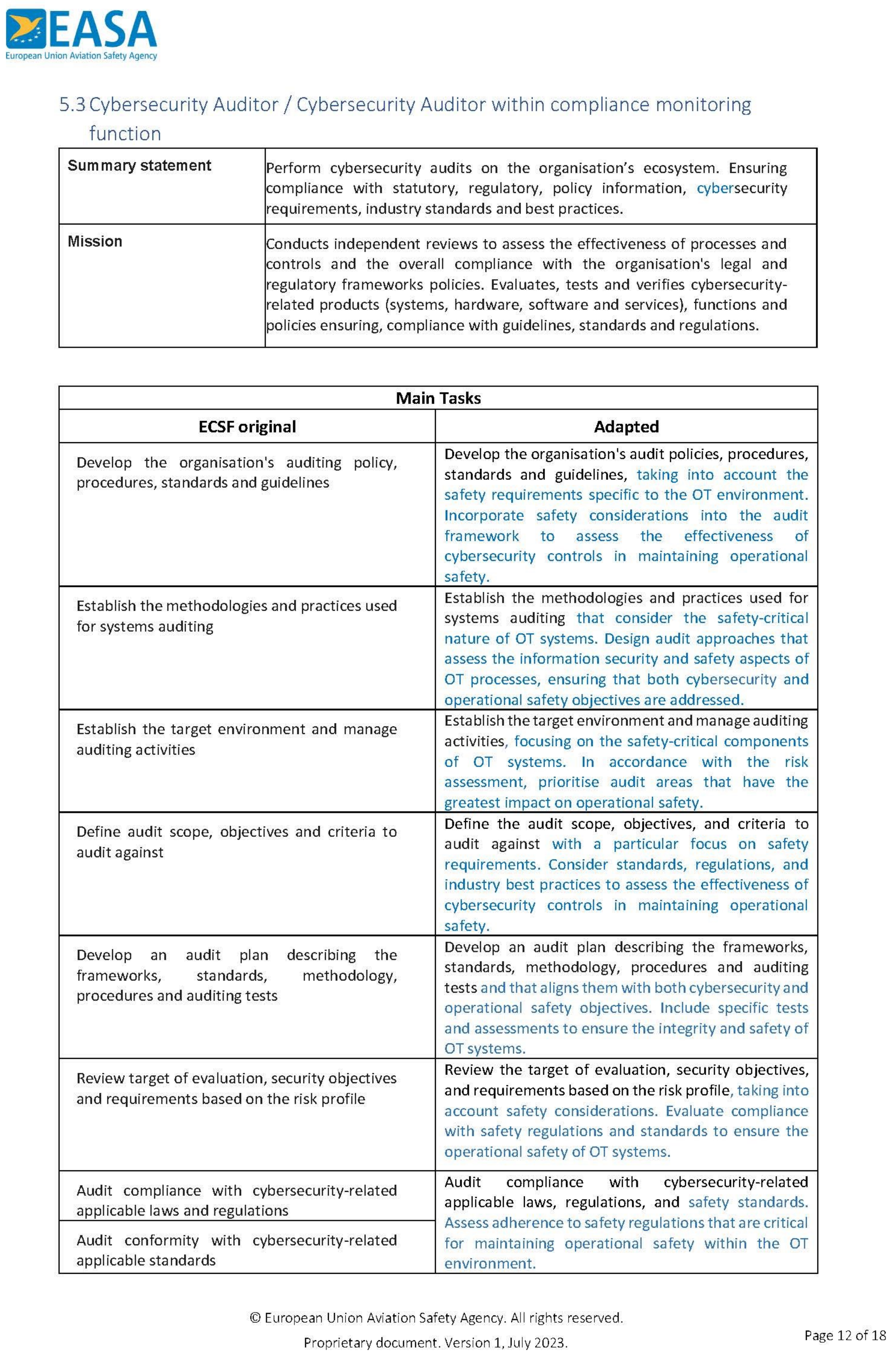
Mission

Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes and recommended remediation strategies/solutions to ensure compliance.

Main Tasks	
ECSF original	**Adapted**
Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations	Ensure compliance with and provide advice and guidance on cybersecurity provisions in aviation regulation
Identify and document compliance gaps	**No adaptations**
Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	**Not required by the aviation specific regulation**
Enforce and advocate organisation's data privacy and protection program	**Not required by the aviation specific regulation**
Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities	**Not required by the aviation specific regulation**
Act as a key contact point to handle queries and complaints regarding data processing	**Not required by the aviation specific regulation**
Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity compliance
Monitor audits and data protection related training activities	**Not required by the aviation specific regulation**
Cooperate and share information with authorities and professional groups	Cooperate and share information with competent authorities
Contribute to the development of the organisation's cybersecurity strategy, policy and procedures	**No adaptations**
Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	**Not required by the aviation specific regulation**
Manage legal aspects of information security responsibilities and third-party relations	**No adaptations**

© European Union Aviation Safety Agency. All rights reserved.
Proprietary document. Version 1, July 2023.

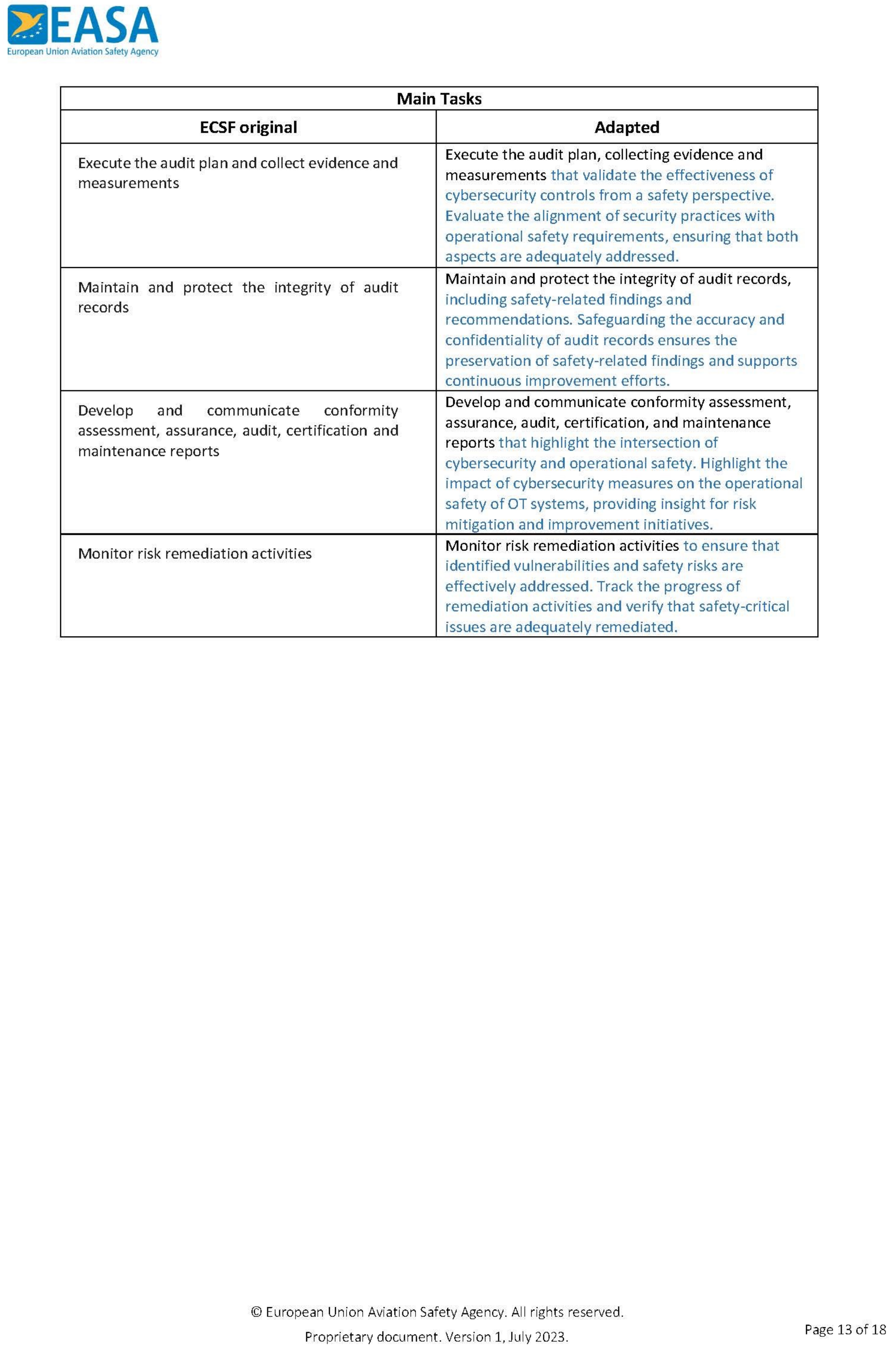
Page 11 of 18



5.3 Cybersecurity Auditor / Cybersecurity Auditor within compliance monitoring function

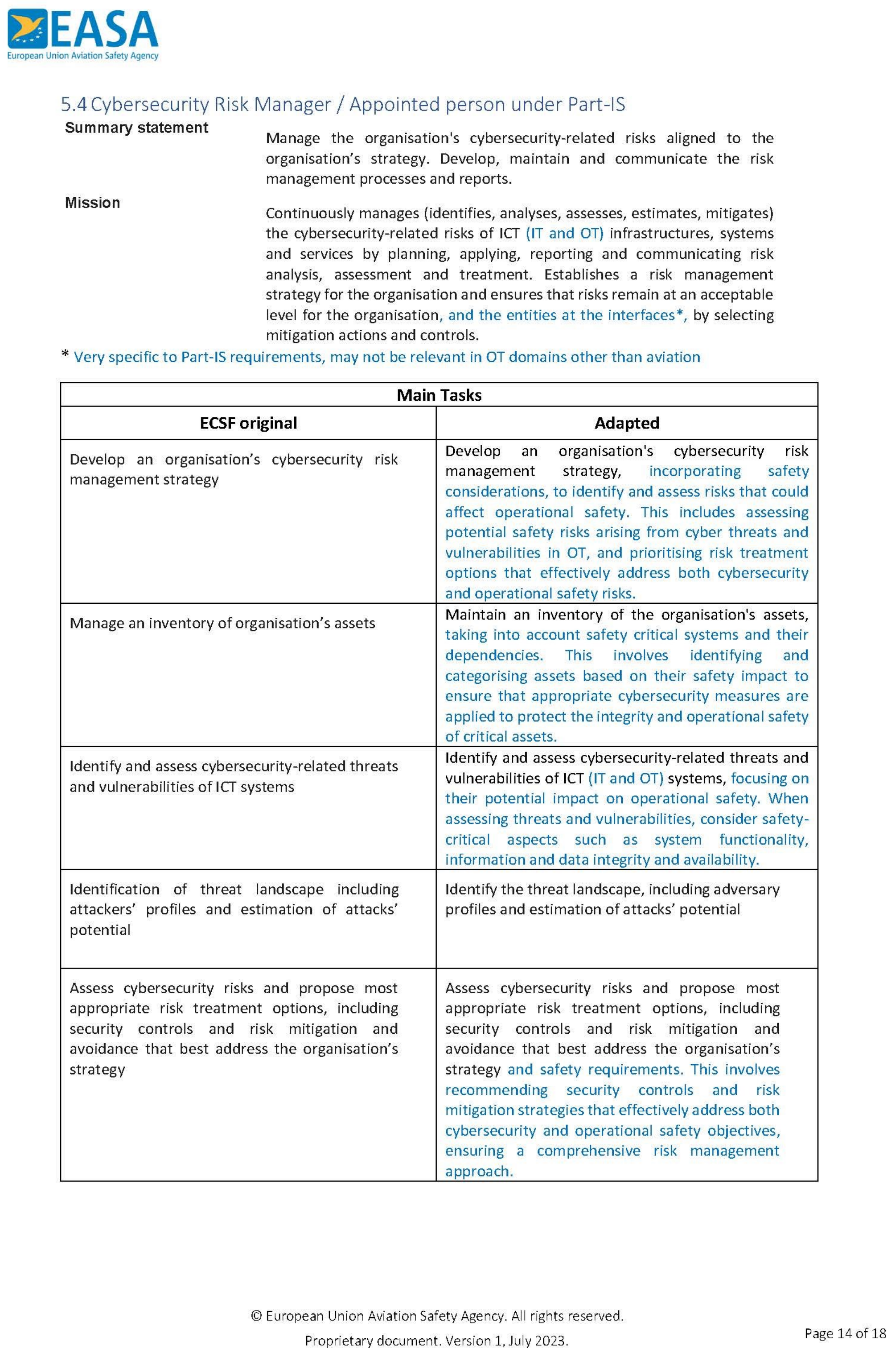
Summary statement	Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, cybersecurity requirements, industry standards and best practices.
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.

Main Tasks	
ECSF original	**Adapted**
Develop the organisation's auditing policy, procedures, standards and guidelines	Develop the organisation's audit policies, procedures, standards and guidelines, taking into account the safety requirements specific to the OT environment. Incorporate safety considerations into the audit framework to assess the effectiveness of cybersecurity controls in maintaining operational safety.
Establish the methodologies and practices used for systems auditing	Establish the methodologies and practices used for systems auditing that consider the safety-critical nature of OT systems. Design audit approaches that assess the information security and safety aspects of OT processes, ensuring that both cybersecurity and operational safety objectives are addressed.
Establish the target environment and manage auditing activities	Establish the target environment and manage auditing activities, focusing on the safety-critical components of OT systems. In accordance with the risk assessment, prioritise audit areas that have the greatest impact on operational safety.
Define audit scope, objectives and criteria to audit against	Define the audit scope, objectives, and criteria to audit against with a particular focus on safety requirements. Consider standards, regulations, and industry best practices to assess the effectiveness of cybersecurity controls in maintaining operational safety.
Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests	Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests and that aligns them with both cybersecurity and operational safety objectives. Include specific tests and assessments to ensure the integrity and safety of OT systems.
Review target of evaluation, security objectives and requirements based on the risk profile	Review the target of evaluation, security objectives, and requirements based on the risk profile, taking into account safety considerations. Evaluate compliance with safety regulations and standards to ensure the operational safety of OT systems.
Audit compliance with cybersecurity-related applicable laws and regulations	Audit compliance with cybersecurity-related applicable laws, regulations, and safety standards. Assess adherence to safety regulations that are critical for maintaining operational safety within the OT environment.
Audit conformity with cybersecurity-related applicable standards	



EASA
European Union Aviation Safety Agency

Main Tasks	
ECSF original	**Adapted**
Execute the audit plan and collect evidence and measurements	Execute the audit plan, collecting evidence and measurements that validate the effectiveness of cybersecurity controls from a safety perspective. Evaluate the alignment of security practices with operational safety requirements, ensuring that both aspects are adequately addressed.
Maintain and protect the integrity of audit records	Maintain and protect the integrity of audit records, including safety-related findings and recommendations. Safeguarding the accuracy and confidentiality of audit records ensures the preservation of safety-related findings and supports continuous improvement efforts.
Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports	Develop and communicate conformity assessment, assurance, audit, certification, and maintenance reports that highlight the intersection of cybersecurity and operational safety. Highlight the impact of cybersecurity measures on the operational safety of OT systems, providing insight for risk mitigation and improvement initiatives.
Monitor risk remediation activities	Monitor risk remediation activities to ensure that identified vulnerabilities and safety risks are effectively addressed. Track the progress of remediation activities and verify that safety-critical issues are adequately remediated.



5.4 Cybersecurity Risk Manager / Appointed person under Part-IS

Summary statement

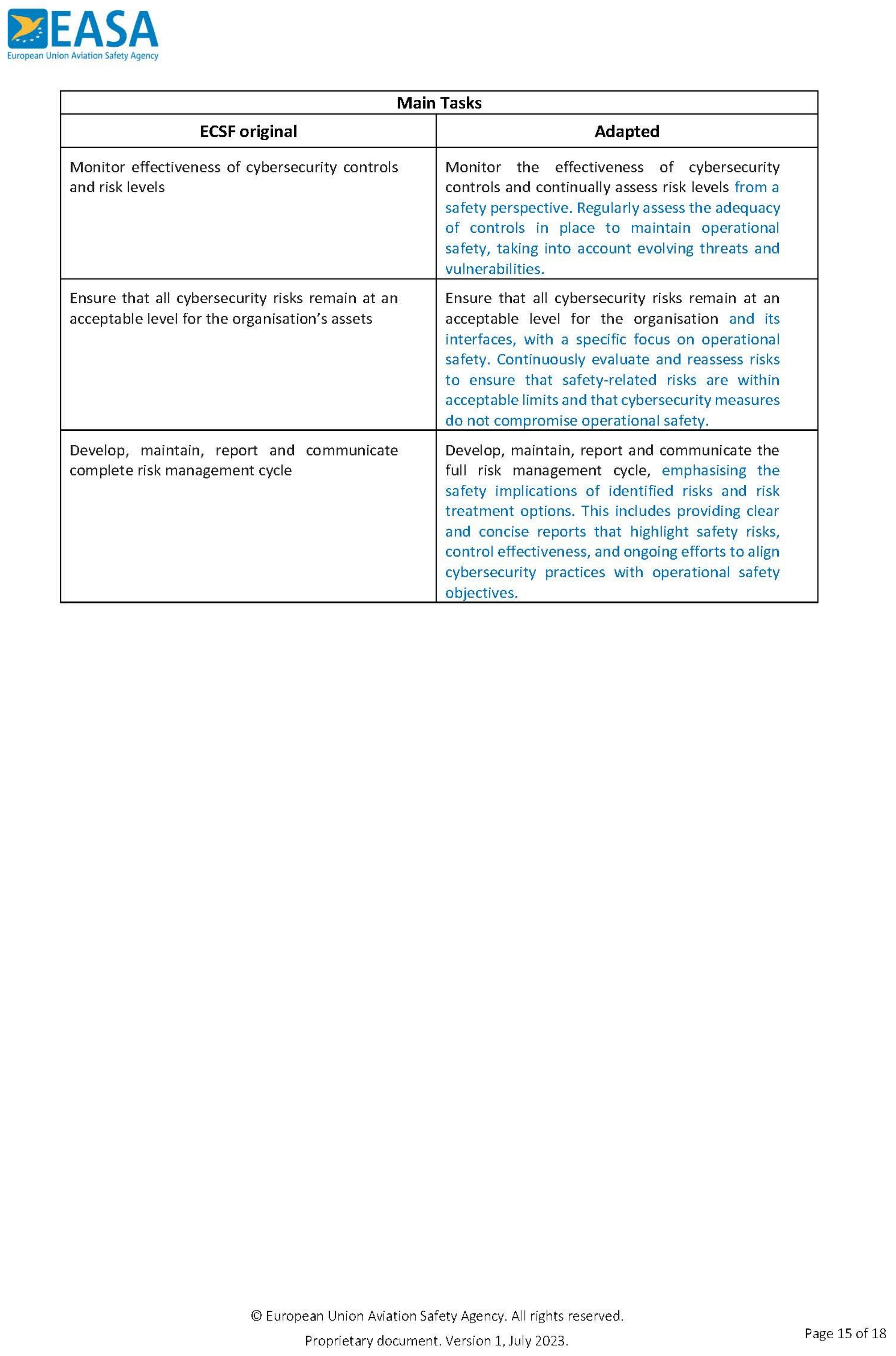
Manage the organisation's cybersecurity-related risks aligned to the organisation’s strategy. Develop, maintain and communicate the risk management processes and reports.

Mission

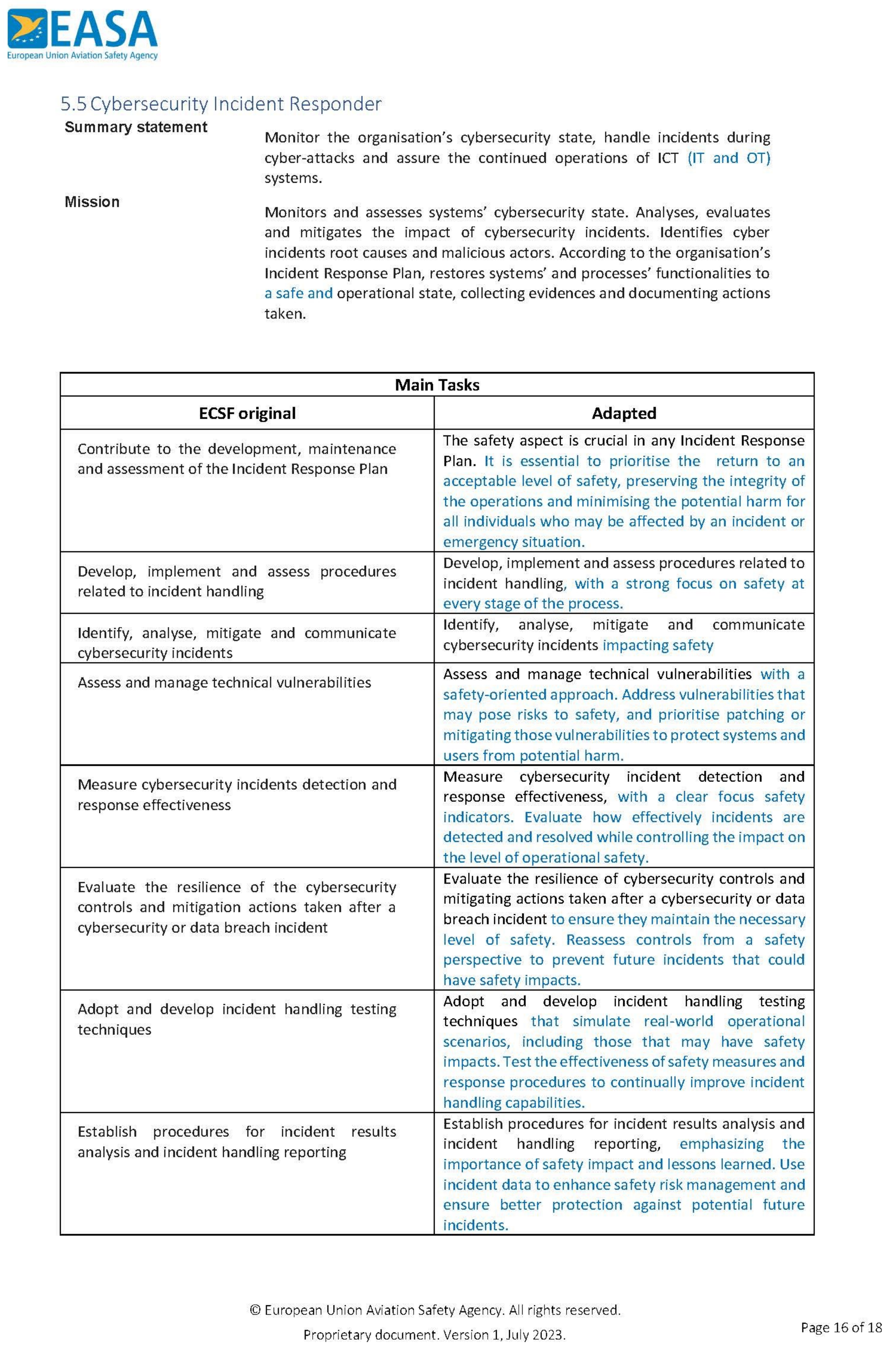
Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT (IT and OT) infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation, and the entities at the interfaces*, by selecting mitigation actions and controls.

* Very specific to Part-IS requirements, may not be relevant in OT domains other than aviation

Main Tasks	
ECSF original	**Adapted**
Develop an organisation’s cybersecurity risk management strategy	Develop an organisation's cybersecurity risk management strategy, incorporating safety considerations, to identify and assess risks that could affect operational safety. This includes assessing potential safety risks arising from cyber threats and vulnerabilities in OT, and prioritising risk treatment options that effectively address both cybersecurity and operational safety risks.
Manage an inventory of organisation’s assets	Maintain an inventory of the organisation's assets, taking into account safety critical systems and their dependencies. This involves identifying and categorising assets based on their safety impact to ensure that appropriate cybersecurity measures are applied to protect the integrity and operational safety of critical assets.
Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems	Identify and assess cybersecurity-related threats and vulnerabilities of ICT (IT and OT) systems, focusing on their potential impact on operational safety. When assessing threats and vulnerabilities, consider safety-critical aspects such as system functionality, information and data integrity and availability.
Identification of threat landscape including attackers’ profiles and estimation of attacks’ potential	Identify the threat landscape, including adversary profiles and estimation of attacks’ potential
Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation’s strategy	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation’s strategy and safety requirements. This involves recommending security controls and risk mitigation strategies that effectively address both cybersecurity and operational safety objectives, ensuring a comprehensive risk management approach.



Main Tasks	
ECSF original	**Adapted**
Monitor effectiveness of cybersecurity controls and risk levels	Monitor the effectiveness of cybersecurity controls and continually assess risk levels from a safety perspective. Regularly assess the adequacy of controls in place to maintain operational safety, taking into account evolving threats and vulnerabilities.
Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets	Ensure that all cybersecurity risks remain at an acceptable level for the organisation and its interfaces, with a specific focus on operational safety. Continuously evaluate and reassess risks to ensure that safety-related risks are within acceptable limits and that cybersecurity measures do not compromise operational safety.
Develop, maintain, report and communicate complete risk management cycle	Develop, maintain, report and communicate the full risk management cycle, emphasising the safety implications of identified risks and risk treatment options. This includes providing clear and concise reports that highlight safety risks, control effectiveness, and ongoing efforts to align cybersecurity practices with operational safety objectives.



5.5 Cybersecurity Incident Responder

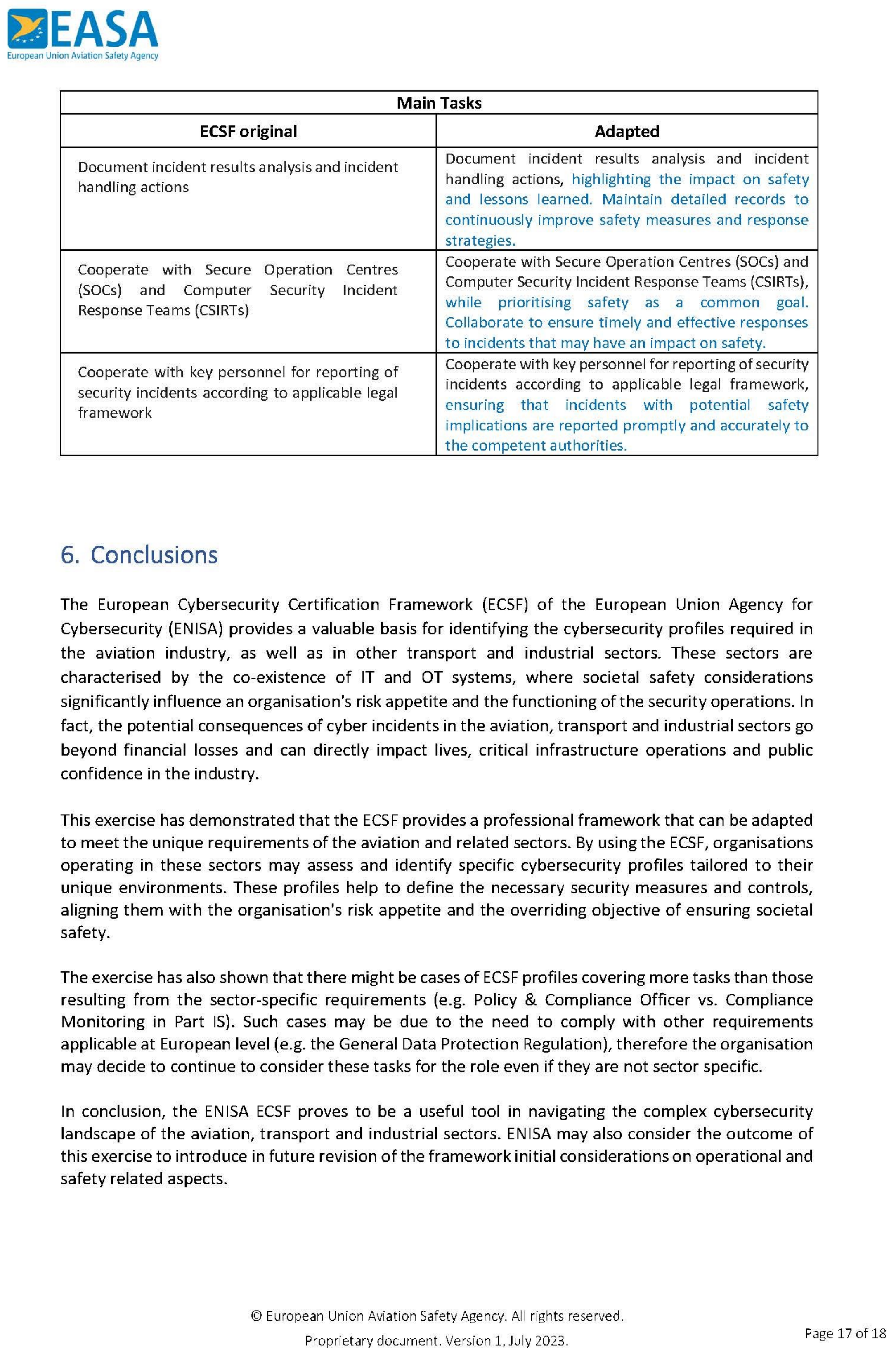
Summary statement

Monitor the organisation's cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT (IT and OT) systems.

Mission

Monitors and assesses systems' cybersecurity state. Analyses, evaluates and mitigates the impact of cybersecurity incidents. Identifies cyber incidents root causes and malicious actors. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to a safe and operational state, collecting evidences and documenting actions taken.

Main Tasks	
ECSF original	**Adapted**
Contribute to the development, maintenance and assessment of the Incident Response Plan	The safety aspect is crucial in any Incident Response Plan. It is essential to prioritise the return to an acceptable level of safety, preserving the integrity of the operations and minimising the potential harm for all individuals who may be affected by an incident or emergency situation.
Develop, implement and assess procedures related to incident handling	Develop, implement and assess procedures related to incident handling, with a strong focus on safety at every stage of the process.
Identify, analyse, mitigate and communicate cybersecurity incidents	Identify, analyse, mitigate and communicate cybersecurity incidents impacting safety
Assess and manage technical vulnerabilities	Assess and manage technical vulnerabilities with a safety-oriented approach. Address vulnerabilities that may pose risks to safety, and prioritise patching or mitigating those vulnerabilities to protect systems and users from potential harm.
Measure cybersecurity incidents detection and response effectiveness	Measure cybersecurity incident detection and response effectiveness, with a clear focus safety indicators. Evaluate how effectively incidents are detected and resolved while controlling the impact on the level of operational safety.
Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident	Evaluate the resilience of cybersecurity controls and mitigating actions taken after a cybersecurity or data breach incident to ensure they maintain the necessary level of safety. Reassess controls from a safety perspective to prevent future incidents that could have safety impacts.
Adopt and develop incident handling testing techniques	Adopt and develop incident handling testing techniques that simulate real-world operational scenarios, including those that may have safety impacts. Test the effectiveness of safety measures and response procedures to continually improve incident handling capabilities.
Establish procedures for incident results analysis and incident handling reporting	Establish procedures for incident results analysis and incident handling reporting, emphasizing the importance of safety impact and lessons learned. Use incident data to enhance safety risk management and ensure better protection against potential future incidents.



Main Tasks	
ECSF original	**Adapted**
Document incident results analysis and incident handling actions	Document incident results analysis and incident handling actions, highlighting the impact on safety and lessons learned. Maintain detailed records to continuously improve safety measures and response strategies.
Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)	Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs), while prioritising safety as a common goal. Collaborate to ensure timely and effective responses to incidents that may have an impact on safety.
Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Cooperate with key personnel for reporting of security incidents according to applicable legal framework, ensuring that incidents with potential safety implications are reported promptly and accurately to the competent authorities.

6. Conclusions

The European Cybersecurity Certification Framework (ECSF) of the European Union Agency for Cybersecurity (ENISA) provides a valuable basis for identifying the cybersecurity profiles required in the aviation industry, as well as in other transport and industrial sectors. These sectors are characterised by the co-existence of IT and OT systems, where societal safety considerations significantly influence an organisation's risk appetite and the functioning of the security operations. In fact, the potential consequences of cyber incidents in the aviation, transport and industrial sectors go beyond financial losses and can directly impact lives, critical infrastructure operations and public confidence in the industry.

This exercise has demonstrated that the ECSF provides a professional framework that can be adapted to meet the unique requirements of the aviation and related sectors. By using the ECSF, organisations operating in these sectors may assess and identify specific cybersecurity profiles tailored to their unique environments. These profiles help to define the necessary security measures and controls, aligning them with the organisation's risk appetite and the overriding objective of ensuring societal safety.

The exercise has also shown that there might be cases of ECSF profiles covering more tasks than those resulting from the sector-specific requirements (e.g. Policy & Compliance Officer vs. Compliance Monitoring in Part IS). Such cases may be due to the need to comply with other requirements applicable at European level (e.g. the General Data Protection Regulation), therefore the organisation may decide to continue to consider these tasks for the role even if they are not sector specific.

In conclusion, the ENISA ECSF proves to be a useful tool in navigating the complex cybersecurity landscape of the aviation, transport and industrial sectors. ENISA may also consider the outcome of this exercise to introduce in future revision of the framework initial considerations on operational and safety related aspects.