APPLICATION OF THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK TO AVIATION

Contents

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.

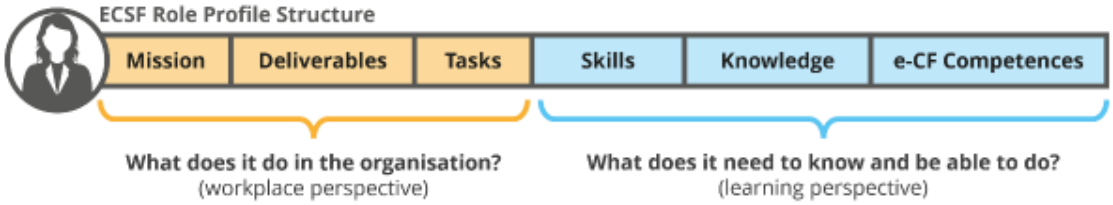
3. Identification of specific objectives to be achieved

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.



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.

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

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.

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**

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	

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.

7. Possible developments

By adopting the ECSF and developing industry-specific cybersecurity profiles, organisations can demonstrate their commitment to upholding security standards and ensuring the robustness of their security operations. In addition, adherence to recognised cybersecurity frameworks, such as the ECSF, enables job market access to professionals coming from sectors other than aviation and vice versa, may improve an organisation's reputation and fosters trust among stakeholders.

By analysing the results and insights gained from this exercise, ENISA will be able to take further steps to improve the comprehensiveness and adaptability of the framework to the evolving cybersecurity landscape and its intersection with operational and security concerns.