EASA
European Union Aviation Safety Agency

Deep Dive in EASA Part-IS AMC and GM

Gian Andrea Bandieri, *Section Manager*
Cybersecurity in Aviation and Emerging Risks

Dublin, 14 September 2023

Aviation ISAC Summit

Making EU aviation cyber resilient

Products (Aircrafts, Engines, …)

- Transition from case by case approach to mandatory on all products now done.
- Positive change of mind set in industry: From defiance to full engagement.

Organisations (People, Processes)

- **Part-IS** Regulations published in October 2022 and February 2023
- AMC/GM published on 12 July 2023

Information Sharing

- Create a community to
  - Share knowledge
  - Perform Analysis
  - Collaborate
  - Reinforce the system

Capacity building & Research

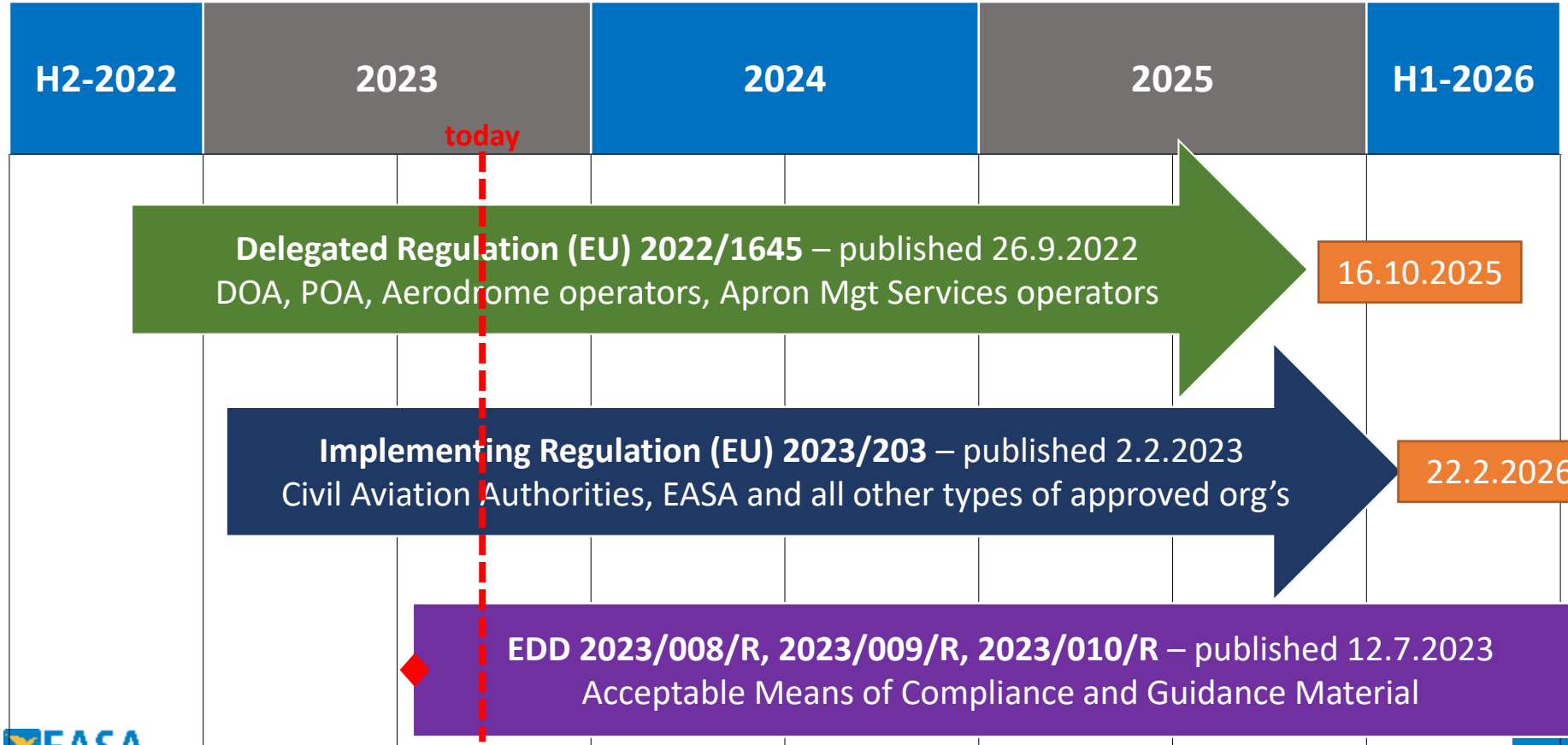
- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

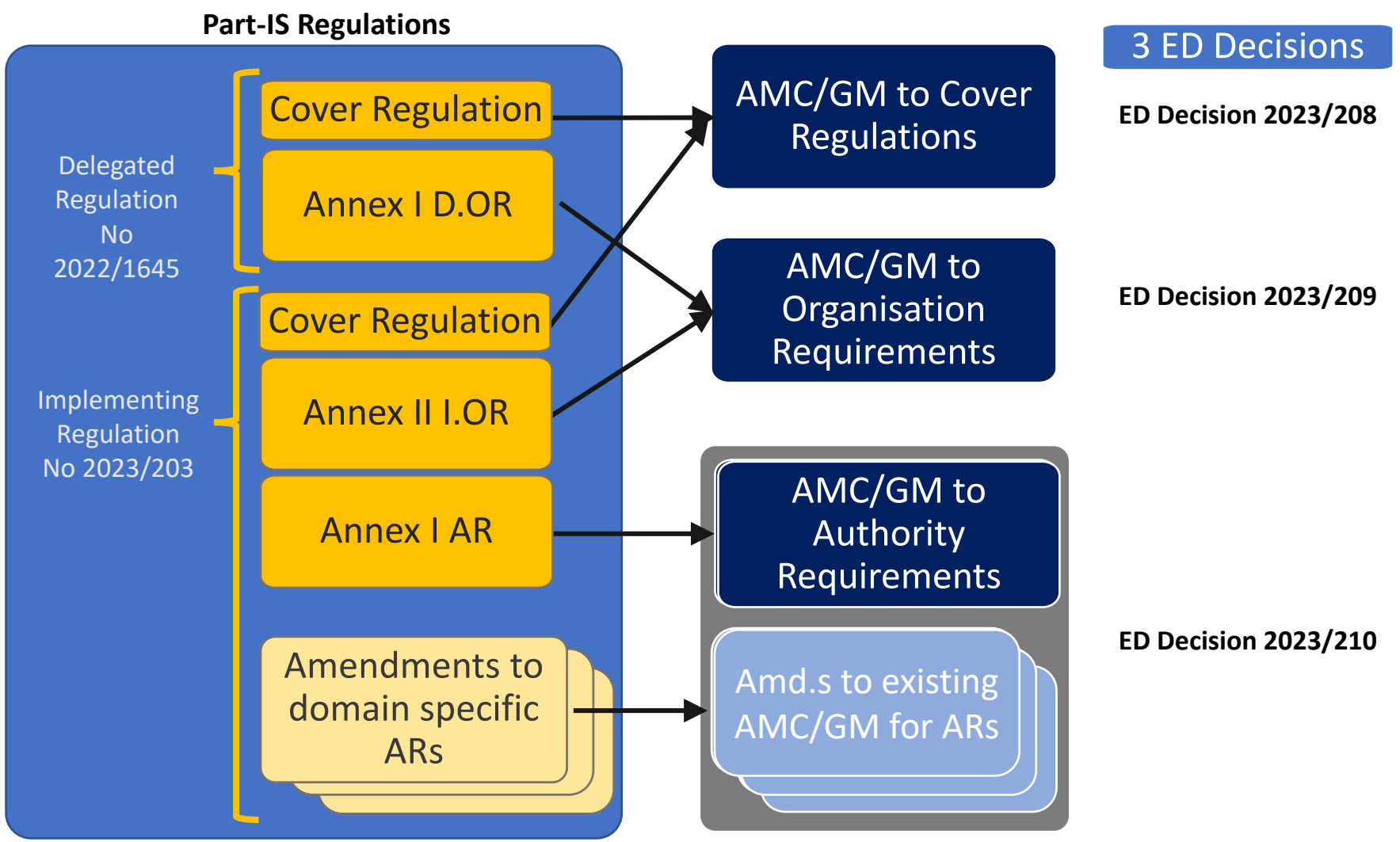
What we want to achieve with Part-IS

Objective	Protect the aviation system from information security risks **with potential impact on aviation safety**
Scope	Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes
Activity	- **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety

Part-IS implementation journey




Part-IS Regulations
Delegated Regulation No 2022/1645
Cover Regulation
Annex I D.OR
Implementing Regulation No 2023/203
Cover Regulation
Annex II I.OR
Annex I AR
Amendments to domain specific ARs
AMC/GM to Cover Regulations
AMC/GM to Organisation Requirements
AMC/GM to Authority Requirements
Amd.s to existing AMC/GM for ARs
3 ED Decisions
ED Decision 2023/208
ED Decision 2023/209
ED Decision 2023/210

AMC & GM what's in it

- → Non-binding by definition
- → To facilitate timely and harmonised application of Part-IS
- → No additional requirements. Everything is in the Regulations

Acceptable Means of Compliance	Guidance Material
• To address identified rule's objectives and processes • Possible ways to comply with the requirements	• To address elements in the rule that would require explanation • To integrate means of compliance by providing guidance on practical or operational aspects • Background information helping to understand the requirements

Ready for the deep dive?

Example 1: OR.200 (a) (b) (c) (d) - ISMS

Rule	- Implement an ISMS with certain characteristics - Do so by taking into account proportionality aspects, documenting core elements and continuously improving it

AMC	- Define Scope[→ 205 (c)] and Establish Information Security Policy
	  - Management commitment
	  - Key processes
	- Compliance monitoring

GM	- Overview of ISMS for safety aspects in aviation - Proportionality and integration with other management systems - Scope definition and its relation to AR/OR.205

Rule

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

(a) In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

(1) establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.I.OR.205;

(3) defines and implements information security risk treatment measures in accordance with point IS.I.OR.210;

(4) implements an information security internal reporting scheme in accordance with point IS.I.OR.215;

(5) defines and implements, in accordance with point IS.I.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.I.OR.205(e), and responds to, and recovers from, those information security incidents;

(6) implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;

(7) takes appropriate action, in accordance with point IS.I.OR.225, to address findings notified by the competent authority;

(8) implements an external reporting scheme in accordance with point IS.I.OR.230 in order to enable the competent authority to take appropriate actions;

(9) complies with the requirements contained in point IS.I.OR.235 when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations;

(10) complies with the personnel requirements laid down in point IS.I.OR.240;

(11) complies with the record-keeping requirements laid down in point IS.I.OR.245;

(12) monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager to ensure effective implementation of corrective actions;

(13) protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.

(b) In order to continuously meet the requirements referred to in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.I.OR.260.

(c) The organisation shall document, in accordance with point IS.I.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.I.OR.200(a), and shall establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.I.OR.255.

(d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.I.OR.200(a) shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the organisation.

GM

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 on levels of aviation safety, which are deemed acceptable. Hence, all roles, processes, or information systems, which may cause or contribute to aviation safety consequences, are within the scope of Regulation (EU) 2023/203. The ISMS provides for means to decide on needed information security controls for all architectural layers (governance, business, application, technology, data) and domains (organisational, human, physical, technical). It further allows to manage the selection, implementation, and operation of information security controls. Finally, it allows to manage the governance, risk management and compliance (GRC) within the ISMS scope.

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

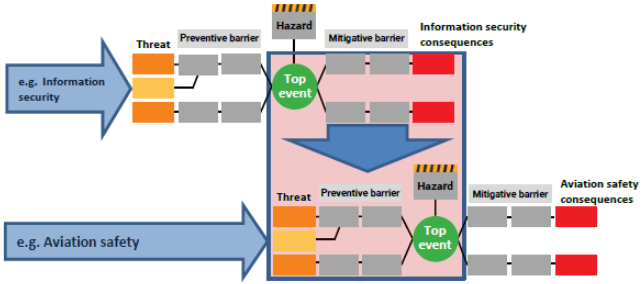


Figure 1: Bow-tie representation of management of aviation safety risks posed [illegible] security threats

8 pages

AMC

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

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

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

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

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

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

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

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

3 pages

GM and AMC

Example 2: OR.215 – Internal reporting scheme

Rule	- Collect and evaluate IS events - Identify incidents and vulnerabilities with potential safety impact, including their causes and contributing factors - Distribute information internally - Collect reports also from the supply chain
AMC	- Means to detect security incidents and vulnerabilities - Each event should be analysed - Develop vulnerability management strategy - Identify all internal stakeholders that require notification
GM	- Internal reports should be assessed in a timely manner - Use SOC or SIEM, of not feasible, establish processes - If possible introduce corrections to processes and investigate root causes - Manage shared risks, establish external agreements

Rule

IS.I.OR.215 Information security internal reporting scheme

(a) The organisation shall establish an internal reporting scheme to enable the collection and evaluation of information security events, including those to be reported pursuant to point IS.I.OR.230.

(b) That scheme and the process referred to in point IS.I.OR.220 shall enable the organisation to:

(1) identify which of the events reported pursuant to point (a) are considered information security incidents or vulnerabilities with a potential impact on aviation safety;

(2) identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified in accordance with point (1), and address them as part of the information security risk management process in accordance with points IS.I.OR.205 and IS.I.OR.220;

(3) ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified in accordance with point (1);

(4) ensure the implementation of a method to distribute internally the information as necessary.

(c) Any contracted organisation which may expose the organisation to information security risks with a potential impact on aviation safety shall be required to report information security events to the organisation. Those reports shall be submitted using the procedures established in the specific contractual arrangements and shall be evaluated in accordance with point (b).

(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.

(e) The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

GM

GM1 IS.I.OR.215(a)&(b) Information security internal reporting scheme

RELATIONSHIP BETWEEN INTERNAL AND EXTERNAL REPORTING

Organisations should collect and report internally incidents and vulnerabilities aiming at covering all items within the scope of this Regulation. Both internal and external reporting are necessary for a complete and effective reporting system. Internal reports should be assessed in a timely manner and where the potential impact on safety is an unsafe condition, organisations should initiate reporting of these internal reports according to IS.I.OR.230.

GM2 IS.I.OR.215(a)&(b) Information security internal reporting scheme

ORGANISATION OF COLLECTION AND EVALUATION OF INFORMATION SECURITY EVENTS

It is a common practice in large organisations to centralise information security operations in a security operations centre (SOC) and make use of an information security information and event management (SIEM) system. A SIEM system collects all events from sources such as log files in a common database and allows the analysts and responders in a joint SOC to review and act on these events. Organisations may choose to use a SOC for events relevant to Part-IS in isolation or in combination with events not subject to Part-IS but of interest to the organisation, such as events relating to business interests. Events can be automatically aggregated, correlated and analysed in order to detect abnormal behaviour leading to information security incidents.

Organisations that do not have a SOC capability and do not use a SIEM system need to consider how to establish processes to meet the required collection and evaluation capabilities as well as detection and response times.

GM3 IS.I.OR.215(a)&(b) Information security internal reporting scheme

RELEVANT INFORMATION FOR INCIDENTS AND VULNERABILITIES

Understanding the causes of, and contributing factors to, information security incidents and vulnerabilities relevant to Part-IS allows lessons learned to be gained and to introduce corrections to processes and asset design. However, understanding causes and contributing factors may not always be possible or may not aid in continuous improvement of aviation safety. Where vulnerabilities arise from assets developed solely or primarily for aviation, it is expected to be possible to perform the necessary investigation on the root causes. These root causes will inform the affected organisation(s) to improve processes and asset design to remediate vulnerability and to ensure that such vulnerabilities are not introduced in other assets. Understanding the root causes of vulnerabilities also allows the aviation community to learn and thus avoid similar vulnerabilities in the future.

GM1 IS.I.OR.215(c) Information security internal reporting scheme

If contracted organisations are also subject to this Regulation, the exchange of information and reporting should be covered under the management of shared risks and through the establishment of an external agreement between the organisations. Guidance regarding the development of external agreements can be found in EUROCAE ED-201A, Chapter 4.4 External agreements.

More in general, and in all other cases, any service contract should include standard clauses concerning obligations for the contracted organisation to:

report within an agreed time information security incidents that may have an impact on the contracting organisation. Incidents and vulnerabilities which could lead to unsafe conditions should be reported as soon as possible and in such a manner that the external reporting obligation under IS.I.OR.230 can be ensured;

designate a point of contact for the incident management and possible crisis management.

In some cases contracted organisations, such as service providers with distributed resources, may not be able to offer any ad hoc reporting. In these cases the internal reporting requirement may be fulfilled through other means that satisfy the objective of this provision. For instance, the contracted organisations may provide an up-to-date list of vulnerabilities affecting the systems within the scope of the contracted services. This list should be monitored by the contracting organisation as part of the internal reporting of information security events.

GM1 IS.I.OR.215(d) Information security internal reporting scheme

The cooperation under point IS.I.OR.215(d) can be substantiated by sharing elements from incident records that can support other organisations' information security activities. In case the organisations are bound by contractual obligations, this contract may also include commitment to cooperate. Organisations may consider developing formal agreements (e.g. a memorandum of understanding) outlining roles and responsibilities for information security collaboration such as governance meetings, joint development activities, and real-time indicators of compromise (IoC) sharing.

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

GM and AMC

AMC

AMC1 IS.I.OR.215(a)&(b) Information security internal reporting scheme

Organisations should use as a source the incidents detected during activities performed to show compliance with IS.I.OR.220(a). Organisations should have a mechanism to collect notifications of events by personnel and by sources outside the company including suppliers, partners, customers, open-source software, and information security researchers. The mechanism for collecting information by personnel and external sources should be easily accessible and communicated.

The organisation should collect all events gathered through the detection means for internal analysis. Each event should be analysed to identify whether it is reportable and if so, what potential or actual impact on aviation safety has occurred. Information security events should be considered in combination with other events to provide correlation to identify incidents or vulnerabilities with a potential impact on aviation safety.

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

The organisation should identify all internal stakeholders that require notification of a specific incident or vulnerability and ensure that these stakeholders receive all necessary information on the incident or vulnerability in order to act effectively and in a timely manner to support the required detection and response periods.

EASA
European Union Aviation Safety Agency

Thank you for your attention !

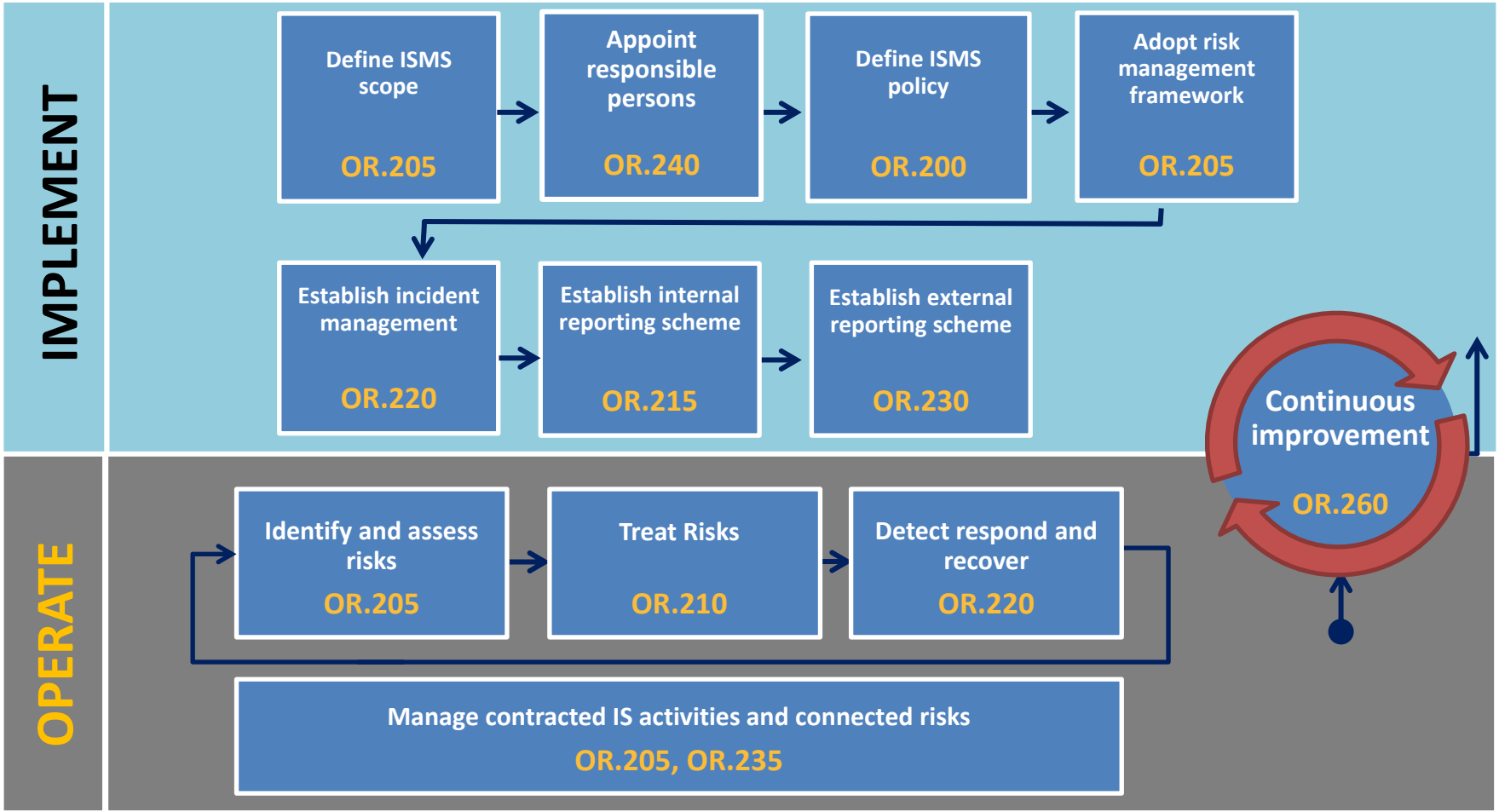
Join our Community:

easa.europa.eu/connect

Contact us at:
cybersec@easa.europa.eu

Your safety is our mission.

An Agency of the European Union


IMPLEMENT
Define ISMS scope
OR.205
Appoint responsible persons
OR.240
Define ISMS policy
OR.200
Adopt risk management framework
OR.205
Establish incident management
OR.220
Establish internal reporting scheme
OR.215
Establish external reporting scheme
OR.230
Continuous improvement
OR.260
OPERATE
Identify and assess risks
OR.205
Treat Risks
OR.210
Detect respond and recover
OR.220
Manage contracted IS activities and connected risks
OR.205, OR.235