Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of the Environment,
Transport, Energy and Communications DETEC

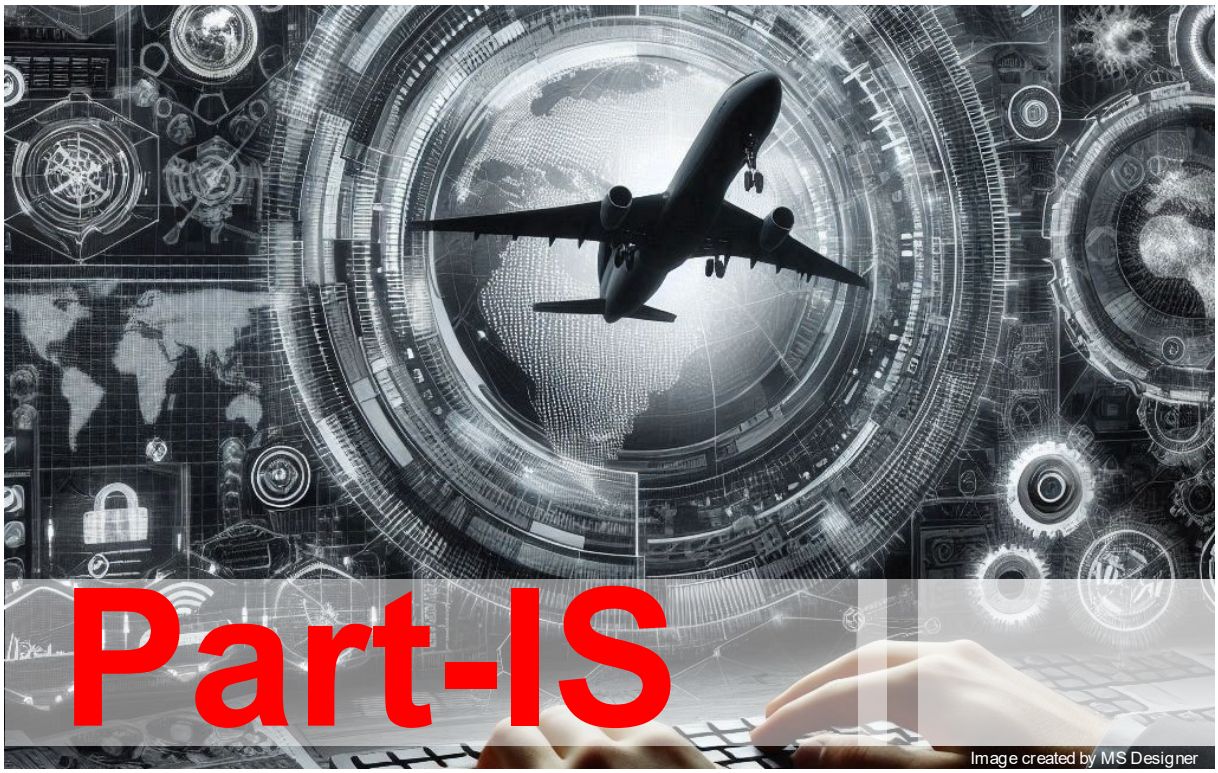
Federal Office of Civil Aviation FOCA
Safety Divisions

FOCA GM/INFO

Guidance Material / Information

Information Security

The purpose of this GM/INFO is to provide guidance for organisations to implement an information security management system.



Scope	Guidance to implement an ISMS
Applies to[1]	AOC-Holders, ATOs, AeMCs, CAMOs, NCC-, FSTD- and SPO-Operator[2], organisations holding a Part-145 maintenance or Part-21 production approval, EASA certified airports, ATM/ANS providers and USSP, Apron management service providers and Ground handling organisations
Valid from	10.07.2026
Version	ISS 01 / REV 02

Business object	308.1-1/1
Document Owner	SISE/Fachstelle Informationssicherheit
Distribution	Internal / External

[1] For exceptions, refer to chapter 0.5
[2] commercial & non-commercial with complex motor-powered aircraft

Log of Revision (LoR)

Date	Issue	Revision	Highlight of Revision	Prepared by	Released by
01.04.2025	1	0	First Issue	SBFF,STOZ, SISE	AFS/Policy (25.03.2025)
30.07.2025	1	1	External reporting and Part-IS derogation specified in more detail among smaller changes and improvements	SBFF,STOZ, SISE	Members of the project decision body Juni-Juli 2025
10.07.2026	1	2	Chapters added for declared organisation and personnel competences. Improved description on derogation, ISMM approval and reporting. Chapter 5.5 removed. Hyperlinks corrected, legal references updated and editorial changes	SBFF,STOZ, SISE	Members of the project decision body July 2026

List of Effective Chapters

LoA	ISS 1 / REV 2 / 10.07.2026	Ch. 11	ISS 1 / REV 1 / 30.06.2025
ToC	ISS 1 / REV 2 / 10.07.2026	Ch. 11.1	ISS 1 / REV 2 / 10.07.2026
Ch. 0	ISS 1 / REV 0 / 01.04.2025	Ch. 11.2	ISS 1 / REV 2 / 10.07.2026
Ch. 0.1	ISS 1 / REV 2 / 10.07.2026		
Ch. 0.2	ISS 1 / REV 2 / 10.07.2026		
Ch. 0.3	ISS 1 / REV 2 / 10.07.2026		
Ch. 0.4	ISS 1 / REV 0 / 01.04.2025		
Ch. 0.5	ISS 1 / REV 0 / 01.04.2025		
Ch. 0.6	ISS 1 / REV 1 / 30.06.2025		
Ch. 0.7	ISS 1 / REV 2 / 10.07.2026		
Ch. 1	ISS 1 / REV 0 / 01.04.2025		
Ch. 2	ISS 1 / REV 1 / 30.06.2025		
Ch. 2.1	ISS 1 / REV 2 / 10.07.2026		
Ch. 2.2	ISS 1 / REV 2 / 10.07.2026		
Ch. 2.3	ISS 1 / REV 2 / 10.07.2026		
Ch. 3	ISS 1 / REV 2 / 10.07.2026		
Ch. 4	ISS 1 / REV 2 / 10.07.2026		
Ch. 4.1	ISS 1 / REV 0 / 01.04.2025		
Ch. 4.2	ISS 1 / REV 1 / 30.06.2025		
Ch. 4.3	ISS 1 / REV 1 / 30.06.2025		
Ch. 4.4	ISS 1 / REV 2 / 10.07.2026		
Ch. 4.5	ISS 1 / REV 2 / 10.07.2026		
Ch. 4.6	ISS 1 / REV 2 / 10.07.2026		
Ch. 5	ISS 1 / REV 2 / 10.07.2026		
Ch. 5.1	ISS 1 / REV 2 / 10.07.2026		
Ch. 5.2	ISS 1 / REV 2 / 10.07.2026		
Ch. 5.3	ISS 1 / REV 2 / 10.07.2026		
Ch. 5.4	ISS 1 / REV 2 / 10.07.2026		
Ch. 6	ISS 1 / REV 2 / 10.07.2026		
Ch. 7	ISS 1 / REV 2 / 10.07.2026		
Ch. 7.1	ISS 1 / REV 2 / 10.07.2026		
Ch. 7.2	ISS 1 / REV 2 / 10.07.2026		
Ch. 7.3	ISS 1 / REV 2 / 10.07.2026		
Ch. 8	ISS 1 / REV 0 / 01.04.2025		
Ch. 9	ISS 1 / REV 2 / 10.07.2026		
Ch. 10	ISS 1 / REV 2 / 10.07.2026		

List of Abbreviations

LoA ISS 1 / REV 2 / 10.07.2026

The following abbreviations are within this GM/INFO:

Abbreviation	Definition
AeMC	Aero Medical Centres
ACM	Accountable Manager
ANS	Air Navigation Services
AOC	Air Operator Certificate
ATO	Approved Training Organisation
ATM	Air Traffic Management
BITD	Basic Instrument Training Device
CAMO	Continuing Airworthiness Management Organisation
CAME	Continuing Airworthiness Management Exposition
CAP	Corrective Action Plan
CL	Certification Leaflet
CMPA	Complex Motor Powered Aircraft
CSH	Cyber Security Hub
CVSS	Common Vulnerability Scoring System
EASA	European Union Aviation Safety Agency
ED	Executive Director
ELA 2	European Light Aircraft
EU	European Union
FOCA	Federal Office of Civil Aviation
FNPT	Flight Navigation Procedures Trainer
FSTD	Flight Simulation Training Device
GM/INFO	Guidance Material / Information
IAM	Identity and Access Management
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technology
IJ	Implementing Journal
ISMM	Information Security Management Manual
ISMS	Information Security Management System
MOA	Maintenance Organisation Approval
MOE	Maintenance Organisation Exposition
MOPSC	Maximum Operational Passenger Seating Configuration
NASP	National Aviation Security Program
NCC	Non-Commercial air operations with Complex motor-powered aircraft
OMM	Organisation’s Management Manual
OT	Operating Technology
PAM	Privileged Access Management
POA	production organisation approval
POE	Production Organisation Exposition
SMS	Safety Management System
SOC	Security Operating Center
SPO	Specialised Operations
USSP	U-Space Service Providers

Table of Contents (ToC)

ToC ISS 1 / REV 2 / 10.07.2026

0 Introduction ... 1

0.1 Terms and Conditions ... 1

0.2 Legal References ... 1

0.3 Purpose of this GM/INFO ... 2

0.4 Scope of document ... 2

0.5 Exceptions for the applicability of Part-IS ... 2

0.6 Organisation / Operator Responsibilities ... 3

0.7 Entities in scope of the National Aviation Security Program (NASP) ... 3

1 Background Information ... 3

2 Management system integration ... 5

2.1 Key Requirements ... 6

2.2 ISMM Approval ... 9

2.3 Submission of application documents ... 10

3 Declared Organisations ... 10

4 Derogation ... 11

4.1 Air Operations, Aircrew and Aero medical Centres ... 13

4.2 Products, parts and appliances ... 14

4.3 Aerodromes ... 15

4.4 Air Traffic Management ... 15

4.5 Application procedure ... 15

4.6 Obligations after an approved derogation ... 16

5 Reporting of information Security Incidents and Vulnerabilities ... 16

5.1 Internal Reporting ... 17

5.2 External Reporting ... 17

5.3 Reporting of vulnerabilities ... 18

5.4 Reporting process ... 19

6 Proportional Implementation of Part-IS ... 20

7 Qualification of personnel ... 21

7.1 Simple organisation ... 21

7.2 Complex organisation ... 21

7.3 Competence Level by role ... 24

8 ISO/IEC 27001 Certification ... 24

9 Part-IS Development Phase 2026-2027 ... 25

10 Online Resources and References 25

11 Annex 26

11.1 Part-IS Compliance Matrix 26

11.2 ICT-Asset Inventory and Risk Assessment for Derogation 27

0 Introduction

Ch. 0 ISS 1 / REV 0 / 01.04.2025

All Guidance Material/Information (GM/INFO) are intended to assist the organisation/operator in administrative matters. The administrative requirements and processes will facilitate liaising with the Federal Office of Civil Aviation (FOCA). It is to be considered a tool for the organisation/operator to ease processes of obtaining required and defined approvals and authorisations issued by the FOCA. Using the GM/INFO will be conducive to establishing compliance with FOCA requirements and will lead through the respective certification or variation process regarding administrative tasks.

0.1 Terms and Conditions

Ch. 0.1 ISS 1 / REV 2 / 10.07.2026

The use of the male **gender** should be understood to include male and female persons.

The most frequent **abbreviations** used by the **EASA** are listed here: easa.europa.eu/abbreviations.

When used throughout the GM/INFO the following terms shall have the meaning as defined below:

Term	Meaning	Reference
shall, must, will	These terms express an obligation, a positive command.	EC English Style Guide
may	This term expresses a positive permission.	
shall not, will not	These terms express an obligation, a negative command.	
may not, must not	These terms express a prohibition.	
need not	This term expresses a negative permission.	
could	This term expresses a possibility.	
should	This term expresses an obligation when an acceptable means of compliance should be applied.	EASA Acceptable Means of Compliance publications FOCA policies and requirements
ideally	This term expresses a best possible means of compliance and/or best experienced industry practice.	FOCA recommendation

For reasons of clarity, references to Part-IS are designated as “IS.OR.xxx” (e.g. IS.OR.255) rather than distinguishing between the implementing regulation (e.g. IS.I.OR.255) and the delegated regulation (e.g. IS.D.OR.255).

0.2 Legal References

Ch. 0.2 ISS 1 / REV 2 / 10.07.2026

Basic Regulation (EU) 2018/1139

Commission Implementing Regulation (EU) 2023/203

Commission Implementing Regulation (EU) 2025/2293

Commission Delegated Regulation (EU) 2022/1645

Commission Implementing Regulation (EU) 2025/22

Commission Regulation (EU) 965/2012

Commission Regulation (EU) 1178/2011

Commission Regulation (EU) 1321/2014

Commission Regulation (EU) 748/2012

Commission Regulation (EU) 139/2014

Commission Regulation (EU) 2015/340

Commission Regulation (EU) 376/2014

Commission Implementing Regulation (EU) 2015/1018

Commission Implementing Regulation (EU) 2017/373

Commission Implementing Regulation (EU) 2021/664

Commission Delegated Regulation (EU) 2025/20

ED Decision 2023/008/R

ED Decision 2023/009/R

Bundesgesetz über die Informationssicherheit beim Bund, Informationssicherheitsgesetz, ISG

0.3 Purpose of this GM/INFO

Ch. 0.3 ISS 1 / REV 2 / 10.07.2026

This document is intended to assist the organisation/operator in implementing an ISMS in accordance with the above stated legal references. It explains the FOCA's approach and reading of various requirements and provides easy to digest information in addition to the EASA's Part-IS GM described in the Easy Access Rules for Information Security and other guidance material. It provides guidance on the process to implement the Part-IS requirements into the organisation. It is important to know that EASA Part-IS itself is not subject to a standalone certification, and FOCA will audit organisations subject to the regulation mainly as part of their regular oversight activities.

In addition, this document should serve to identify and evaluate a possible derogation within the organisation and addresses the mandatory reporting requirements for information security incidents and vulnerabilities.

0.4 Scope of document

Ch. 0.4 ISS 1 / REV 0 / 01.04.2025

The scope of the document encompasses selected topics within the regulation, of which FOCA identifies they are most relevant and crucial for all applicable organisations. The level of detail might differ and is generally held on a high level. Therefore, this document does not claim to be complete, and its application cannot be considered as fully compliant to all the regulatory requirements of Part-IS. It is meant to be used aside with the corresponding official regulatory material.

0.5 Exceptions for the applicability of Part-IS

Ch. 0.5 ISS 1 / REV 0 / 01.04.2025

If the scope of work of an organisation aligns with the exceptions stated in the table below, Part-IS requirements are not applicable for the organisation and no further actions need to be considered in terms of compliance. However, Part-IS requirements might become applicable, if any changes to the organisation exceeds the exception criteria below.

Domain	Exceptions
Technical organisations (Part-145)	Solely maintaining Part-ML aircraft
CAMO	Solely managing Part-ML aircraft
Air Operators	▪ Solely operating ELA 2 aircraft ▪ Single-engine propeller driven aeroplanes & MOPSC < 6 & non-CMPA & A to A VFR day ops ▪ Single-engine helicopter & MOPSC < 6 & non-CMPA & A to A VFR day ops
Approved Training Organisations	▪ Solely involved in training activities of ELA 2 aircraft ▪ Solely involved in theoretical training
FSTD Operators	▪ Solely involved in the operation of FSTDs for ELA 2 aircraft

ATM and ANS providers	▪ ANS providers holding a limited certificate in accordance with point ATM/ANS.OR.010 ▪ FIS providers declaring their activities in accordance with point ATM/ANS.OR.015
Production organisations (Part-21)	▪ Solely involved in the production of ELA 2 aircraft

For details refer to Article 2 of Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645.

0.6 Organisation / Operator Responsibilities

Ch. 0.6 ISS 1 / REV 1 / 30.06.2025

Before notifying FOCA about any changes according to IS.OR.255, it is essential for the organisation to be familiar with the regulation and to submit the complete and traceable documentation in respect to the applicable regulation of its or their approvals and according to the approved process.

The organisation must ensure that all parts of the exposition system are revised in a manner as to be compliant with the requirements related to information security.

0.7 Entities in scope of the National Aviation Security Program (NASP)

Ch. 0.7 ISS 1 / REV 2 / 10.07.2026

Organisations bound by the provisions of the Aviation Security Regulation (EU) 2019/1583 and consequently, by the National Aviation Security Program (NASP chapter 19) may regard the implementation of these requirements as equivalent to the requirements of Part-IS. In order to circumvent redundancy in oversight activities, FOCA may elect to employ the NASP as a legal foundation to supervise the implementation of Part-IS requirements in pertinent circumstance. Such combined oversight activities affect mainly airports, airlines and ATM/ANS organisations.

1 Background Information

Ch. 1 ISS 1 / REV 0 / 01.04.2025

The term "Part-IS" denotes a collection of European regulations established between 2022 and 2023 aimed at improving information security, commonly referred to as cybersecurity, within the aviation sector.

These regulations recognize that the aviation sector is highly interconnected and vulnerable to various information security threats, including cyber-attacks, human errors, and process failures. By implementing these rules, the European Union aims to standardise and enhance information security practices, thereby improving the resilience of aviation operations against malicious threats and ensuring public safety.

It is recommended for organisations to incorporate these information security requirements into their existing aviation safety management systems (SMS), ensuring a seamless and comprehensive approach to managing both safety and information security risks.

In today's dynamic digital landscape, the security of information is not just a business necessity but a cornerstone of organisational integrity. An ISMS serves as a structured framework to manage and protect sensitive and safety critical data, ensuring compliance, risk mitigation, and stakeholder trust.

An effective ISMS provides a risk-based approach to information security. By identifying, analysing, and mitigating information security risks, the organisation can reduce vulnerabilities and respond to incidents swiftly and efficiently. Implementing an ISMS promotes a culture of information security across all levels of the organisation. Training, awareness, and accountability become integral, empowering employees to recognize and respond to cyber threats effectively.

An ISMS is not a static framework but a continuous process of improvement. Through regular monitoring, audits, reviews and defined responsibilities, the system adapts to new threats, technologies, and business requirements, ensuring relevance and resilience.

Even though the applicable regulations primarily address the implications of aviation safety, it makes sense for an ISMS to incorporate the entire organisational landscape and to include other aspects such as business continuity, data privacy and aviation security related processes where applicable. This means that from a compliance perspective, only the aviation safety implications are relevant. However, it is in an organisation's best interest to consider all processes in its ISMS that pose a potential or actual information security risk.

2 Management system integration

Ch. 2 ISS 1 / REV 1 / 30.06.2025

Integrating an ISMS into an already existing management system (e.g. SMS) seems to be an efficient way and can reduce redundancies, as both systems, despite their different focuses, have several important similarities. Both systems are structured, systematic approaches to managing risks. From an organisational perspective, different types of risks interact with each other, and the implementation of certain controls may address more than one type of risks. Therefore, FOCA recommends considering such an integrative approach.

Here are some examples of commonalities in both systems.

- Management commitment
- Policy and procedures
- Risk management
- Record keeping
- Training and awareness
- Audits and reviews
- Stakeholder communication (internal and external reporting)
- Reporting and continuous improvement

Regarding the introduction of Part-IS, it is not necessary, unlike other changes from the past, to seek a separate approval. The obligation to implement Part-IS in the existing organisation arises from the requirements for the already existing approval (for example refer to 145.A.200A / CAMO.A.200A / 21.A.139A / 21.A.239A / ORx.GEN.200A / ... etc).

The individual parts of Part-IS must be implemented by certain deadlines based on the requirements of the various regulations listed above. At present, the FOCA does not intend to carry out separate audits and/or inspections (pre-audits) in advance to verify the compliance of the respective organisation regarding the full implementation of Part-IS. The responsibility for timely implementation lies with the organisation, based on the already implemented Management of Change process, which is mandatory for every organisation through the SMS.

In a next step, at the latest when the full implementation of Part-IS is mandatory under the existing approval, the FOCA will check compliance on this topic as part of its continuous, periodic surveillance. Should any deviations be identified during such surveillance activities, this will be documented as part of the recording of findings. This should enable the organisation to approach full compliance by dealing with the findings (CAP, root cause analysis, corrective action) in accordance with its established processes.

As mentioned above, the FOCA recommends an integrated approach to implementing the requirements of Part-IS. This is, of course, accompanied by the recommendation of an integrated description of the management system, including Part-IS. The existing manual structure can be supplemented with the topics of Part-IS and the corresponding gaps in the description can be filled.

Alternatively, the organisation can, of course, also create a stand-alone Information Security Manual (ISMM).

Table 2 of the EASA Guidelines Part-IS oversight approach lists some of the elements to be implemented by the organisations to be ready to operate the ISMS.

2.1 Key Requirements

Ch. 2.1 ISS 1 / REV 2 / 10.07.2026

Some of the key concepts of the ISMS prescribed by Part-IS are further explained in the following paragraphs.

Policies and procedures

Developing comprehensive information security policies, processes and procedures is a fundamental requirement under Part-IS. These policies and procedures form the backbone of your ISMS, providing a structured approach to managing and mitigating information security risks.

From a practical standpoint, your organisation should start by creating an inventory of all relevant systems followed by conducting a risk assessment to identify potential threats and vulnerabilities with a possible impact on aviation safety. Based on these findings, draft policies that clearly outline acceptable use of information systems, ensuring all employees understand what constitutes appropriate and inappropriate behavior when handling digital assets. These policies should cover various scenarios, including remote work, mobile device usage, and the handling of sensitive data, to ensure comprehensive coverage.
In addition to acceptable use policies, it is essential to develop detailed incident response plans. These plans should provide step-by-step guidance on how to detect, report, and respond to information security incidents. They should specify roles and responsibilities during an incident, including communication, investigation, resolution and who is taking decisions. The implementation of such is up to the organisation. FOCA does not mandate specific tools. If, for instance, an organisation was to decide that the above is suitable to be implemented in its existing ERP system, this would be acceptable to the authority.

Access control measures are another critical component; these policies should define how access to information systems and data is granted, managed, and revoked.
Establish clear guidelines for data protection, including encryption, data retention, and secure disposal practices. To ensure the effectiveness of these policies, they must be easily accessible to all employees and regularly reviewed and updated to reflect changes in technology, regulations, and emerging threats. Regular training and awareness programs should be conducted to keep staff informed and compliant with the latest security practices.

Mapping of dependencies

Mapping dependencies within your organisation is a critical step in implementing an effective Information Security Management System (ISMS) as required by Part-IS.OR. This process involves identifying and documenting how each department relies on others and on external service providers. Understanding these interdependencies is essential for creating a comprehensive risk management strategy.

Start by engaging each department to outline their key functions and the internal and external resources they depend on to conduct their operations. This includes identifying software systems, information, data flows, and third-party services that support daily activities.

IS.OR.235 places specific emphasis on the role of external service providers, such as software vendors and outsourcing companies, in your organisation's information security framework. When mapping these dependencies, it is important to assess the security posture of these external partners, and whether they are themselves subject to the requirements of Part-IS.

Evaluate their information security policies, practices, and controls to ensure they meet your organisation's standards and regulatory requirements. According to GM1 IS.OR.205(b), the interfaces with other parties, such as service providers and supply chains, should be identified based on the exchange of data and information, as these could lead to increased information security risks due to mutual exposure.

Contracts with these providers should include clauses that mandate compliance with your security requirements and allow for audits to verify their adherence to these standards.

Risk Management

In the initial implementation phase of Part-IS, conducting thorough risk assessments is crucial for identifying information security risks that could impact aviation safety. Start by assembling a dedicated team with representatives from various departments, including IT, ground operations, flight operations, training, maintenance, charter, finance, human resources, and management.

This team should undertake a comprehensive review of all information and communication technology systems and data to identify potential vulnerabilities and threats. Document the findings in a risk register, categorising risks based on their potential impact and likelihood of occurrence. This structured approach ensures that all potential risks are identified and prioritised effectively.

Once the initial risk assessment is complete, the next step is to develop and implement risk treatment plans to mitigate the identified risks. This involves selecting appropriate controls and measures to address each risk based on its severity. For technical risks, consider implementing solutions such as firewalls, encryption, password management, and intrusion detection systems. For process-related risks, introduce improvements such as regular audits, incident response protocols, and access control measures.

Ensure that all mitigation measures are managed within the ISMS.

Regularly review and update these plans to adapt to new threats and changes in the organisational environment, maintaining a proactive approach to information security management.

Information security incident detection, response and recovery

Setting up robust mechanisms for information security incident detection, response, and recovery is critical for safeguarding your organisation's information assets. Begin by installing and configuring advanced monitoring tools that can detect potential security threats. These tools should be capable of identifying unusual patterns, such as unauthorized access attempts, malware activity, and data exfiltration.

Designate a team (internal or outsourced) responsible for continuously monitoring these alerts and ensuring swift detection of incidents. Develop a clear incident response plan that outlines the steps to be taken once a potential threat is identified, including immediate actions to contain the threat and to prevent further damage.

Equally important is establishing comprehensive procedures for responding to and recovering from information security incidents. These procedures should detail the roles and responsibilities of all relevant personnel during an incident, ensuring coordinated and efficient action.

Implement a structured process for assessing the impact of the incident, determining its scope, and identifying affected systems and data. This should be followed by containment measures to limit the spread of the threat, eradication efforts to remove malicious elements, and recovery steps to restore affected systems and data to normal operation. Ensure that all actions taken are documented for post-incident analysis and reporting.

Develop a business continuity plan that includes strategies for maintaining essential operations and flight safety during an incident, minimising disruption, and ensuring a quick return to normality. Regularly test and update these procedures through simulations and drills to ensure readiness and effectiveness in real-world scenarios.

Training and awareness

When considering information security, our thoughts typically focus on the two elements, human factors and processes.

Even though profound IT-knowledge is required in many aspects in the context of information security, it is widely recognised that one of the most vulnerable points in an organisation's security is its personnel. Human error, lack of awareness, and inadequate training can all lead to significant security

breaches. Thus, it should not come as a surprise that personnel requirements is a crucial component of the Information Security Management System (ISMS) outlined in IS.OR.240

In the initial implementation phase, it is essential to develop a comprehensive training program that covers all aspects of information security relevant to your organisation. This program should be designed to equip all employees, including those not directly involved in the implementation of Part-IS, with the necessary knowledge and skills to adhere to ISMS procedures.

Begin by conducting a training needs analysis to identify the specific knowledge gaps and training requirements for different roles within your organisation. Develop tailored training modules that address these needs, including topics such as recognising phishing attempts, proper personal data handling practices, and the importance of following security protocols.

Regular training sessions, workshops, and e-learning modules can be effective in maintaining a high level of security awareness among staff. Additionally, periodic assessments and refresher courses should be implemented to ensure that employees remain up to date with the latest security practices and threats.

Reporting and continuous improvement

Maintaining comprehensive records of information security incidents and actions taken is essential for the effectiveness of your Information Security Management System (ISMS). In the initial implementation phase, establish robust internal reporting mechanisms that ensure timely communication of incidents within the organisation. A formal liaison between information security and safety roles is essential.

This involves creating a clear and accessible reporting protocol that all employees can follow to report potential security issues. Document each incident meticulously, including the nature of the incident, the response actions taken, and the outcomes. This documentation not only helps in understanding the incident better but also provides valuable data for analysing trends and identifying recurring issues. Ensure that the incident records are securely stored and easily retrievable for future reference, compliance audits, and analytics.

In addition to internal reporting, it is imperative to report significant incidents to relevant authorities as mandated by IS.OR.230. This ensures transparency and compliance with legal requirements, helping to build trust with regulatory bodies and stakeholders. For detailed National and European legal requirements and associated reporting process see chapter “Reporting process”.

Regularly review and update your policies, procedures, and controls based on lessons learned from past incidents and evolving threats. Conduct periodic audits and assessments to evaluate the effectiveness of your security measures and identify areas for enhancement. Encourage a culture of feedback within the organisation where employees can suggest improvements and report potential vulnerabilities without fear of retribution.

2.2 ISMM Approval

Ch. 2.2 ISS 1 / REV 2 / 10.07.2026

In accordance with IS.OR.250, an organisation must draw up an Information Security Management Manual (ISMM). The initial version the ISMM must be approved by the FOCA.

However, according to IS.OR.250(d) the ISMM can also be integrated into already existing management expositions or manuals. It is up to the organisation to decide how it will reflect the Part-IS relevant processes in its documentation landscape. To date, different variants of ISMM have been observed.

Standalone ISMM

All requirements, processes, procedures are documented within a single document called ISMM.

“+” Clear single source of truth for Part-IS.

“+” Easier for auditors and authorities to review.

“+” Strong ownership by the Information Security / Part-IS function.

“-“ Risk of duplicating procedures already described in OMM, CAME, Airport Manual, MOE, POE, etc.

“-“ Higher risk of inconsistencies between manuals.

“-“ May feel detached from daily operations.

ISMM Reference Manual

A relatively short ISMM, which contains most information security only related processes but mainly serves as a reference platform to other existing expositions like OMM, CAME, Airport Manual (e.g. Policies, Asset inventory, Reporting, Safety Risk Management, Roles and Responsibilities, etc.)

“+” Lean and efficient. Avoids duplication by referencing existing approved procedures.

“+” Good for organisations with mature manuals and document control.

“+” Supports an integrated management-system approach without rewriting all manuals.

“-“ Depends heavily on precise references.

“-“ Weak if links, paragraph numbers or document ownership are unclear.

“-“ Revision is more complex because changes in referenced documents may affect Part-IS compliance.

Full Integration

All Part-IS requirements are integrated into already existing documents like an OMM, CAME or other types of expositions.

“+” Part-IS becomes part of normal business processes.

“+” Reduces the feeling of “another manual”.

“+” Staff find requirements where they already work, for example in OMM, CAME or Airport Manual procedures.

“-“ Harder to demonstrate complete Part-IS compliance at a glance.

“-“ Requirements may become scattered across many manuals.

“-“ Risk that information security governance becomes diluted inside operational procedures.

The content requirements of the ISMM is defined in IS.OR.250(a). Among those requirements the FOCA considers the following points in particular to be the most important.

- Applicable certifications.
- Management commitment to information security.
- Information security policy with a strong link to aviation safety.
- Clear defined scope of the ISMS.
- Organisational structure with clear roles, responsibilities and qualifications for IS related roles.
- Information security risk management with impact on safety.
- Coordination between information security and safety roles.
- Internal and external reporting procedures for incidents and vulnerabilities.

Regardless of the form of documentation chosen, it is important to the FOCA for the approval process that

- there are clear and unambiguous references to the relevant Part-IS requirement for each specific issue.
- there are clear and unambiguous references to the documents cited, including the version, chapter and/or page.
- a comprehensive Part-IS compliance matrix is submitted together with the ISMM and/or associated documents (for each submission).

2.3 Submission of application documents

Ch. 2.3 ISS 1 / REV 2 / 10.07.2026

FOCA expects that all concerned organisations submit the documentation at least a minimum of 8 weeks in advance of the planned certification.

Documents to be submitted

- ISMM and/or updated OMM, CAME or other exposition in case of ISMM integration into existing document landscape
- All referenced documents containing description of Part-IS implementation
- Complete Part-IS compliance matrix with clear references where to find the description in the documents (file, page, chap.).

In the case of an integrated description of the Part-IS topics, the OMM adjustment can be requested accordingly through the applicable FOCA processes.

If special Part-IS topics need to be described in other expositions (e.g. CAME, MOE, POE etc.), these changes are to be handled by means of a description in the respective exposition (→ Changes requires prior approval). To assist the organisation with the initial compliance, FOCA provides a compliance matrix, which can be found in the Annex of this document.

3 Declared Organisations

Ch. 3 ISS 1 / REV 2 / 10.07.2026

Organisation working under a declared regime (e.g. NCC, SPO, apron management- and ground handling service providers) that fall within the scope of the Part-IS regulation, must equally establish an ISMS, subject to the following exceptions.

- The ISMM does not require approval by the FOCA.[3]
- The change management procedure does not require approval by the FOCA.[4]
- Changes to the ISMS do not require approval by the FOCA.[5]

[3] IS.OR.250(b)
[4] IS.OR.255(a)
[5] IS.OR.255(b)

However, if an organisation seeks for a derogation as per IS.OR.200(e) the normal application procedure needs to be applied as described in chapter "Derogation" and a formal approval must be obtained by FOCA.

4 Derogation

Ch. 4 ISS 1 / REV 2 / 10.07.2026

The FOCA recognises the possibility of an organisation to obtain an approval not to implement the requirements of Part-IS in accordance with IS.OR.200(e) and will support an application wherever possible and appropriately.

Without prejudice to the obligation to comply with the reporting requirements laid down in Commission Regulation (EU) No 376/2014 and the requirements of point IS.OR.200(a)(13), the organisation may be granted an approval by the FOCA not to apply the requirements set out in points (a) to (d) and the related requirements set out in points IS.OR.205 to IS.OR.260 if it demonstrates to the satisfaction of the FOCA that its activities, facilities and resources, and the services it operates, provides, receives and maintains, do not pose an information security risk with a potential impact on aviation safety, either to itself or to other organisation. This is then to be considered a derogation.

In any case, the approval of the FOCA is based on a documented risk assessment of information security, which must be carried out by the organisation or a third party in accordance with point IS.OR.205 and reviewed and approved by the FOCA as appropriate. This risk assessment can be carried out and documented using the organisation's existing risk assessment procedure, or by using the templates which FOCA provides for the derogation assessment. The resulting risks, if any, should be identified and monitored in the organisation's risk register.

The continued validity of this approval of deviation will be reviewed by the FOCA following the respective surveillance audit cycle and whenever there is a change in the organisation's scope of work.

The risk assessment according to IS.OR.205 of an organisation builds the foundation of the assessment, whether FOCA denies or grants a request. In addition to the risk assessment, other considerations are also taken into account.

For example:

High level consideration describing the exposure to the aviation landscape:

- The position of the organisation within the aviation functional chain, and
- its level of contribution to safety consequences.

Detailed consideration about processed or produced safety related information:

- The services the organisation provides and receives incl. their interfaces
- The processes the organisation has established to provide and receive the services

To assist organisations in the assessment of their application, the FOCA has developed basic criteria and conditions that provide **an indication** of whether a corresponding application for derogation has **a prospect of success**. Even though basically any organisation in the scope of Part-IS can apply for a derogation, FOCA will triage applications based on those criteria and conditions stated below, before a detailed assessment.

It is important to note that the conditions and justifications noted below cannot be considered as an automatic authorisation or refusal. Each application of an organisation will be assessed individually. Furthermore, applications for partial exemption from individual articles are not possible.

Domain	Potential approval of a derogation application
Air Operators (incl. CAMO)	Yes, under certain conditions
Approved Training Organisations	Yes, under certain conditions
CAMO (without AOC)	Yes, under certain conditions
FSTD Operators	Yes, under certain conditions
Technical organisations (Part-145)	Yes, under certain conditions
Production organisations (Part-21)	Yes, under certain conditions
Airports	No
ATM and ANS providers	No
USSP	No
Aeromedical Centers AeMC	No

4.1 Air Operations, Aircrew and Aero medical Centres

Ch. 4.1 ISS 1 / REV 0 / 01.04.2025

Likelihood of approval[6]	Condition	Affected Approvals

A request on derogation is most likely denied by FOCA	• The organisation is systemically relevant at the federal level:
	  • Monopoly/systemically important (aviation policy = international accessibility), e.g. Flag Carriers
	  • The organisation operates on behalf of the Swiss Confederation (e.g. international transport of Federal Councils or SWISSINT)
		CAT / NCC / SPO

A request on derogation is likely to be approved by FOCA	• VFR operations only	
	• Operation with non-complex aircraft only	
	• Organisation operating airplane with MTOM < 5.7 t • Organisation operating helicopters with MTOM < 3.175 t	**ATO**
	• FSTD operators operating: BITD, FNPT, FTD only	**FSTD**

Likelihood of approval	Justification	Affected Approvals
A request on derogation is most likely denied by FOCA	Due to the sensitivity nature and general high volume of medical data including personal related data and medical licenses, a potential, at least indirect, safety impact seems obvious. Therefore, FOCA does not consider it appropriate or proportionate to approve an application in accordance with IS.OR.200(e).	**AeMC**

[6] For applications from organisation to which the listed conditions do not apply, no probability can be given for approval of the derogation request. However, derogations could be granted based on submitted documents and risk assessment.

4.2 Products, parts and appliances

Ch. 4.2 ISS 1 / REV 1 / 30.06.2025

Likelihood of approval	Condition	Affected Approvals
A request for an exemption is generally accepted and can be approved by FOCA under certain conditions (case-by-case[7] assessment).	**1. Safety-related or critical services and products of the organisations are not provided by digital processes and informations**	
	1.A The shelf life or usage times of materials, components, and/or maintenance intervals are not fully monitored digitally using an externally hosted system.	**POA / MOA**
	2. Reliance on third parties ISMS	
	2.A. No digital maintenance records or organisation which rely on third-party software or platforms (e.g. AMOS, CAMP, Blue Eye) which are already certified or managed with ISMS compliant processes.	**MOA, CAMO[8]**
	3. Reduced attack surface[9]	
	3. A. A large portion of maintenance, CAMO and production systems are offline and have little to no exposure to the public network.	**POA / MOA / CAMO[8]**
	3 B. OT systems are not or only minimally interconnected with IT systems and are not connected to the public network	**POA / MOA**
	3 C. No interconnected calibration tools and test stands	**MOA / POA**
	3 D.CNC production systems for critical and structural A/C parts are not connected to the internet	**POA / partly MOA (if applicable)**
	3.E The organisation does not operate any web applications that have a direct or indirect influence on its productive systems	**POA, MOA, CAMO[8]**
A request on derogation is most likely denied by FOCA	**If a CAMO is incorporated into an AOC[10] (for exceptions, refer to 3.1).**	**CAMO**

[7] Case-by-case: It generally depends on the respective requirement. The case-by-case basis for an application always refers to the actual activities of the organization or organizational unit. Therefore, a detailed internal analysis (risk analysis) should be provided with the application.

[8] CAMO: In this context, this refers to a so-called “stand-alone” CAMO or other CAMO (e.g. within Part-SPO or Part-NCC) that is not integrated into an AOC (in accordance with Part-CAT).

[9] Reduced attack surface: A reduced attack surface refers to minimizing the number of potential entry points or vulnerabilities that attackers can exploit in a system.

[10] CAMO incorporated into an AOC: There is no existing AOC without a CAMO. For this reason, a CAMO within a comprehensive management system (including ISMS) cannot derogate individually from the requirements of Part-IS, even if the above criteria apply to the CAMO. The risk to information security therefore does not arise from the activities of the CAMO alone, but from the perspective of the AOC. A derogation would only be possible if the AOC had obtained approval for the derogation from the FOCA in accordance with the criteria listed in 3.1 of Part-IS (i.e., VFR operations only / operation with non-complex aircraft only).

4.3 Aerodromes

Ch. 4.3 ISS 1 / REV 1 / 30.06.2025

Likelihood of approval	Condition	Affected Approvals
A request on derogation is most likely denied by FOCA	1. The airport operator is under the applicability of the National Aviation Security Program, NASP chap. 19.	**EASA certified airports**
	2. The airport is considered a critical infrastructure in terms of national security.	
A request on derogation is likely to be approved by FOCA	3. None of the above conditions apply.	
No request required	4. Non EASA certified airports (e.g. LSZG, LSGC) are not in scope of Part-IS. Therefore is no need to issue a derogation request.	**ICAO airports**

4.4 Air Traffic Management

Ch. 4.4 ISS 1 / REV 2 / 10.07.2026

Likelihood of approval	Justification	Affected Approvals
A request on derogation is most likely denied by FOCA	Due to the general complexity of ICT systems, the potential safety implications and the applicability of the National Aviation Security Program, NASP chap. 19, FOCA does not consider it appropriate or proportionate to approve an application in accordance with IS.OR.200(e).	**ATM/ANS**
No request required	AFIS providers (e.g. Airport LSZS) are not in scope of Part-IS. Therefore is no need to issue a derogation request.	

Likelihood of approval	Justification	Affected Approvals
A request on derogation is most likely denied by FOCA	Due to the high degree of digitalization and automation of ICT systems, the potential safety implications and the information security requirements in regulation (EU)2021/664, FOCA does not consider it appropriate or proportionate to approve an application in accordance with IS.OR.200(e). In addition, considering the novelty of U-space services and the absence of a sufficiently established operational track record for USSPs, FOCA considers derogations to be unjustified at this stage.	**USSP**

4.5 Application procedure

Ch. 4.5 ISS 1 / REV 2 / 10.07.2026

An application for derogation must be filed according to the approved change processes of the corresponding approvals. It is highly recommended for organisation holds multiple approvals to get in touch with all relevant FOCA sections prior to submit the application.

1. Submit a change request in accordance with the standardised procedure. The relevant FOCA form might already offer a section on derogation with specific questions. If this is not the case, the organisation shall provide information to the items below.
    - Affected approval(s) for which a derogation will be applied for.
    - Justification for the exclusion of the provisions. The justification is a written statement signed by the ACM to explain in detail why the organisation does not have any information security risks which can lead to a safety impact.

- Overview of services the organisation provides and receives, including the interfaces to other organisations.
- Overview of the architecture of information systems used for business operation. Ideally this is a visual representation of a logical network diagram.
- Information on how the initial information security risk assessment aligned with the above architecture is intended to be carried out.
- Information on the methodology to be used in performing the information security risk assessment.
- List of persons and roles intended to be involved in the information security risk assessment process.
- Identification of any third parties to be involved in the information security risk assessment.

2. In addition, the organisation needs to submit more detailed information, such as an ICT Asset inventory and a risk assessment. To speed up the process, FOCA recommends using their dedicated templates.

3. Receive FOCA's decision through your assigned inspector upon finalization of the change process.

4.6 Obligations after an approved derogation

Ch. 4.6 ISS 1 / REV 2 / 10.07.2026

A granted derogation from Part-IS is not an indefinite permission. Its ongoing validity is assessed during regular oversight activities and upon changes to the organisation. Therefore, it is important to maintain the regulation in scope of the compliance monitoring system and to adhere to the provisions still applicable regardless of an active derogation status. In particular

- IS.OR.200(a)(13) is still applicable
- Compliance to (EU)376/2014 needs to be assured
- Monitor the risk picture for any variation due to changes in the safety and security environment over time. To this end, point IS.OR.205(d) should be considered.
- Implement basic protection against information security risks according to industry best practices.
- For every change, regardless of whether it requires prior approval, the organisation must verify whether the Part-IS derogation remains in effect. This verification and the basis for the respective decision must be recorded in the documented MoC. If necessary, an additional risk analysis may be required.

5 Reporting of information Security Incidents and Vulnerabilities

Ch. 5 ISS 1 / REV 2 / 10.07.2026

As mentioned in the key requirements in chapter 2.1, maintaining comprehensive records of information security incidents and actions taken is essential for the effectiveness of your Information Security Management System. It is essential that detected anomalies, suspected or confirmed security events are reported to a designated and responsible person within the organsation who then initiates the necessary actions.
Typically basic first steps involved:

1. Acknowledge and record the internal report
   Capture who reported it, when, affected system, what was observed, screenshots/logs, and whether data, accounts, customers, or operations may be affected.
2. Classify: incident, vulnerability, or false alarm
   An information security event or incident indicates that something may already be occurring, such as malware infection, unauthorized access, data leakage, or system disruption. In contrast, a vulnerability is a weakness that could potentially be exploited but has not necessarily been exploited yet.
3. Escalate to the relevant internal roles
   Notify the incident-response lead, safety manager, compliance manager, and management according to the organisation's incident response plan.
4. Assess scope, severity and safety impact
   Determine the safety relevance of the affected systems, users, data, third parties, and business processes.

5.1 Internal Reporting

Ch. 5.1 ISS 1 / REV 2 / 10.07.2026

Establish clear internal processes and procedures for staff to report observed or suspected information security events. Procedures and responsibilities need to be defined for the evaluation of events and for deciding which ones have to be considered incidents or vulnerabilities. This encourages a proactive security culture within the organisation.

The following non-exhaustive examples describe some information security incidents that may be considered a reason to report them **internally**.

- Unauthorised access: Any instance where an unauthorised individual or system gains access to data or other systems.
- Data breach: The exposure of confidential information to unauthorized parties, either accidentally or through malicious actions.
- Malware infection: Detection of viruses, worms, ransomware, or other malicious software on the organisation's network or devices.
- Phishing attack: Attempts to deceive employees into providing sensitive information through fraudulent emails or websites.
- Loss or theft of devices: Incidents involving the loss or theft of laptops, smartphones, or other devices containing sensitive information.
- Unlawful modifications: Unauthorized changes to software, data, or network configurations.
- Compromised user accounts: Detection of user accounts that have been accessed or used without authorization.
- Suspicious network activity: Unusual patterns of network traffic that may indicate a potential security threat.
- Social engineering: Attempts to manipulate employees into divulging confidential information or performing actions that compromise security.
- Policy violations: Instances where employees or contractors violate the organisation's security policies or procedures.
- Information security vulnerabilities: Identification of weaknesses in software, hardware, or network configurations that could be exploited by attackers.
- Insider Threat: Malicious or negligent actions by employees or contractors that compromise the organisation's information security.
- Failed security controls: Detection of security controls that have failed to operate as intended, potentially exposing the organisation to risk.

5.2 External Reporting

Ch. 5.2 ISS 1 / REV 2 / 10.07.2026

Notify FOCA about significant incidents, especially those with potential safety impacts, within specified timeframes. Procedures to identify which incidents and vulnerabilities are to be externally reported need to be developed.

The following non-exhaustive examples describe some information security incidents that may be considered a reason to report them internally (IS.OR.215) and externally to FOCA and if applicable to the design approval holder (IS.OR.230).

- All of the above examples, which are considered to have a potential impact on aviation safety.
- Remote Hijacking: Gaining access and control of aviation’s critical system which leads to compromised information.
- Supply Chain Attacks: Compromising the supply chain for aircraft parts can result in the introduction of faulty or malicious components, impacting aircraft safety.
- Maintenance System Compromise: Unauthorized access to aircraft maintenance records can result in incorrect or falsified maintenance data, leading to potential mechanical failures.
- In-Flight Entertainment System (IFE) Breach: While primarily for passenger use, a breach in the IFE system can provide a pathway to more critical aircraft systems, posing a security risk.

- Aircraft Communication Addressing and Reporting System (ACARS) Hacking: Unauthorized access to ACARS can lead to the manipulation of flight plans and communication between aircraft and ground stations, potentially causing navigation errors and safety risks.
- Flight Management System (FMS) Tampering: Cyberattacks targeting the FMS can alter flight paths, fuel calculations, and other critical flight parameters, endangering the aircraft's safe operation.

5.3 Reporting of vulnerabilities

Ch. 5.3 ISS 1 / REV 2 / 10.07.2026

FOCA does not expect or recommend reporting any commonly known vulnerabilities within the vast landscape of software components, such as operating systems and applications. However, if an organisation detects any vulnerabilities with a potential impact on safety and/or with a flavor of novelty, reports as per IS.OR.230 are expected.

The following non-exhaustive examples describe some vulnerabilities that may be considered a reason to report them internally (IS.OR.215) and externally to FOCA and if applicable to the design approval holder. (IS.OR.230).

- Commonly known vulnerabilities within a critical information system (operating system, application) which renders a CVSS Score of 8.7[11] or higher affecting integrity and/or availability and which is exposed and which cannot be mitigated.
- Weak access controls: Inadequate access controls can allow unauthorized individuals to gain access to critical systems and data.
- Potential wireless communication exploits: Vulnerabilities in wireless communication systems used for aircraft operations can be exploited to disrupt or manipulate data transmissions.
- Legacy, outdated and unsupported systems exposed to the public network may lack the necessary modern security features, making them more susceptible to cyberattacks.
- Detection of compromised components or software from suppliers, which introduce vulnerabilities into aviation systems.

[11] NIST CVSS Calculator V4.0

5.4 Reporting process

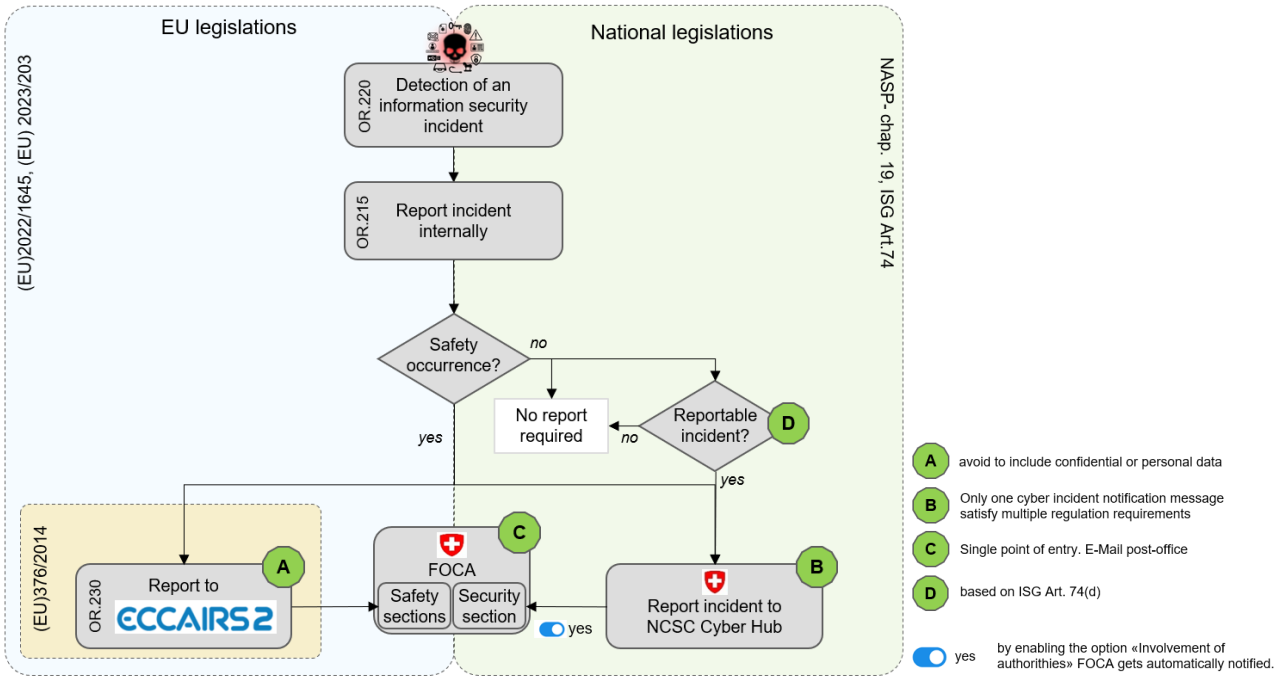
Ch. 5.4 ISS 1 / REV 2 / 10.07.2026

Overview of applicable reporting obligations for aviation stakeholders.

Context	Reporting platform	Recipients	Regulatory Framework
Incident / Vulnerability with impact on **Aviation Safety**	ECCAIRS 2.0	FOCA	(EU)2022/1645, IS.OR.230 (a)(b)[12] (EU)2023/203, IS.OR.230 (a)(b)[12]
Incidents with impact on **Aviation Safety or Security**	NCSC Cyber Security Hub	FOCA	NASP Chapter 19.2.4.6[13][14]
Incidents on **Critical Infrastructure**	NCSC Cyber Security Hub	NCSC	ISG Art.74[15]

FOCA and NCSC have developed a solution for aviation stakeholders that satisfies different regulatory reporting requirements while maintaining a single streamlined and straightforward reporting process. This process has been implemented and is available to organisations since October 2025.

The following flowchart depicts the reporting process for better clarification.



[12] The organisation shall implement an information security reporting system that complies with the requirements laid down in Regulation (EU) No 376/2014 (…). (…), the organisation shall ensure that any information security incident or vulnerability, which may represent a significant risk to aviation safety, is reported to their competent authority.

[13] Applicable for airlines, airports and ATM/ANS only

[14] Cyber attacks with a potential effect on either aviation safety or aviation security **shall** be reported to FOCA according to the existing reporting channels

[15] Applicable to all organisations which are not specifically excluded in "Verordnung über die Cybersicherheit CSV" Art. 12 d.

This reporting structure combines the currently valid requirements from various legislations, which make it easier for organisations. It is also worth noting that the organisation could request any support it may need from the NCSC directly through this notification.

The onboarding to the Cyber Security Hub of the NCSC is a simple one time process, which can be initiated here.

Reporting classified information over ECCAIRS 2.0

It is important to note that reporting vulnerabilities often involves sensitive information that needs to be kept confidential. Those responsible for reporting must ensure that no confidential information is reported unless the system protects the sensitivity of the submitted information. If a report involves sensitive information, only metadata shall be provided. FOCA may contact the organisation to provide a secure means of submitting sensitive data.

Examples of sensitive information relating to the reporting of vulnerabilities and incidents include:

- Proof-of-concept exploit code
- Severity assessment before fix
- Step-by-step reproduction instruction
- Credentials and secrets (e.g. tokens, passwords, API keys, DB connections strings)
- Personal, HR and financial data
- Backup setup
- Security controls
- Detection rules
- IoC
- Malware samples

6 Proportional Implementation of Part-IS

Ch. 6 ISS 1 / REV 2 / 10.07.2026

IS.OR.200(d) states that the processes, procedures, roles and responsibilities established by the organisation shall be proportionate to its nature and complexity. FOCA adheres to EASA's published guideline on 'Part-IS proportional implementation'. This guidance classifies the terms 'simple' and 'complex' based on three independent factors.

• Indicator of the degree of safety relevance.

• Indicator of complexity related to the organisational structure and hierarchies.

• Indicator of complexity related to the complexity of the information and communication technology (ICT) systems and data used by the organisation.

Please refer to the published EASA guideline for details.

FOCA further understands that the terms “non-complex”, “simple” and “small” are sometimes used interchangeably to refer to an organisation that has:

- fewer than 20 employees, or a similarly small active user base
- one main office or a small number of locations, with no international setup
- standard office IT only, such as laptops, email, cloud storage, standard SaaS tools and basic networking
- no custom-built business-critical systems, or only a small number of simple applications

Considering the Swiss aviation landscape, many air operators (e.g. helicopter businesses), flight schools and maintenance and CAMO service providers fit into this category.

7 Qualification of personnel

Ch. 7 ISS 1 / REV 2 / 10.07.2026

IS.OR.240(g) requires to ensure that the personnel have the necessary competence to perfom their tasks. The organisation may consult the Part-IS Easy Access Rules Appendix VI – Adaption of the EU Cybersecurity Skills Framework (ECSF), which has been tailored to aviation to learn more about required qualifications for IS related activities. This chapter and the list below shall be treated as an additional reference to understand qualification in regard to information security for different types of aviation organisations in terms of complexity and size.

The below listed competences shall be treated as guidance only and the actual competences need to be tailored to the organisations need.

7.1 Simple organisation

Ch. 7.1 ISS 1 / REV 2 / 10.07.2026

For a simple, small, organisation, it is acceptable and proportionate that one responsible person coordinates information security, provided it has enough competence to understand aviation safety relevance, manage the ISMS basics, and know when to use external expertise.

The responsible person should be able to…

- understand the requirements and objectives of the Part-IS regulation.
- explain the organisation's Part-IS scope and excluded areas.
- maintain a simple asset and supplier inventory.
- identify systems and data with possible aviation safety relevance.
- perform or coordinate basic information security risk assessments.
- define proportionate controls and track implementation.
- recognise and escalate information security incidents.
- coordinate with the safety manager and compliance monitoring function.
- maintain ISMS documentation, including policy, procedures, risk register and evidence.
- challenge the IT provider and understand whether technical controls are adequate.
- report residual risks to the accountable manager for decision.

Minimum recommended competence profile for a small organisation

Role	Minimum level
Accountable Manager	Awareness of Part-IS obligations, safety impact, resource needs and residual risk acceptance
Information Security Responsible Person	Working knowledge of ISMS, Part-IS, aviation safety interfaces, basic cyber risk management and supplier control
Safety / Compliance Manager	Working knowledge of how cyber risks can create safety or compliance consequences
External IT / Information Security Provider	Practitioner or expert competence in technical controls, logging, backups, patching, access management and incident support
All Staff	Awareness level

7.2 Complex organisation

Ch. 7.2 ISS 1 / REV 2 / 10.07.2026

For a complex organisation, the competence requirement cannot realistically be fulfilled by one person. The organisation should establish a structured role model with dedicated governance, risk, technical, monitoring, incident response, supplier and assurance functions.

The responsible function should be distributed across specialists who collectively cover:

- Regulatory compliance and authority interface.
- Aviation information security risk assessment with impact on safety.
- Enterprise security architecture.
- SOC, logging and detection engineering.
- Incident response and crisis management.
- Vulnerability and patch management.
- IAM and privileged access management.
- Supplier and subcontractor security.
- Internal audit and compliance monitoring.
- Security awareness and competence management.
- Executive reporting and continuous improvement.

Role	Competence area	Required competence
Accountable Manager, CISO, ISMS / Part-IS Manager	Part-IS governance	Establish governance, responsibilities, policy, ISMS scope, interfaces and management reporting
ISMS / Part-IS Manager, Compliance Monitoring	Regulatory interpretation	Interpret Part-IS, AMC/GM, authority expectations, applicability, declarations/approvals and evidence requirements
Safety Manager, Information Security Risk Manager	Aviation safety risk integration	Translate cyber scenarios into aviation safety consequences and align cyber risk with SMS risk processes
Information Security Risk Manager	Enterprise security risk management	Maintain risk methodology, risk register, risk acceptance, treatment plans and residual risk governance
Risk Manager, Security Architect, SOC Lead	Threat scenario analysis	Identify credible aviation-relevant cyber threat scenarios, including operational disruption, data manipulation and supplier compromise
ISMS Manager, Enterprise Architect, System Owners	Asset, process and dependency mapping	Maintain inventory of critical systems, interfaces, services, data flows, suppliers and operational dependencies
Security Architect, IT/OT Engineering Lead	Security architecture	Design secure IT/OT/cloud/network architecture, segmentation, secure remote access and resilience
IAM / PAM Manager	Identity and access management	Define and operate IAM, MFA, privileged access management, account lifecycle and access reviews
SOC Lead	Security monitoring and detection	Define logging strategy, SIEM use cases, SOC procedures,

		alert triage and detection coverage
Incident Response Manager	Incident response	Lead cyber incident handling, crisis coordination, containment, eradication and recovery
Safety Manager, ISMS Manager, Incident Response Manager	Aviation occurrence reporting	Determine whether information security events require aviation safety reporting and coordinate with safety reporting channels
Vulnerability / Patch Manager	Vulnerability management	Operate vulnerability scanning, patch prioritisation, exception handling and remediation verification
Supplier Security Manager, Procurement, Legal	Supplier and subcontractor security	Define contractual security requirements, assess suppliers, monitor outsourced services and manage interface risks
Change Manager, Security Architect, System Owners	Secure change management	Ensure IT, OT, software, cloud, network and supplier changes are assessed for safety-relevant security impact
Training / Awareness Lead, ISMS Manager	Training and competence management	Define awareness, role-specific training, competence records and refresher cycles
CISO, ISMS Manager	Management reporting	Provide risk posture, incidents, KPIs, control effectiveness and resource needs to senior management
ISMS Manager, CISO, Compliance Monitoring	Continuous improvement	Conduct lessons learned, update risk assessments, improve controls and maintain ISMS maturity

7.3 Competence Level by role

Ch. 7.3 ISS 1 / REV 2 / 10.07.2026

Role	Small / low-complex organisation	Complex organisation
Accountable Manager	Awareness / decision-making competence	Strategic oversight and risk governance competence
Information Security Responsible Person	Broad working knowledge across ISMS, risk, suppliers, incidents and controls	Usually replaced by dedicated ISMS / Part-IS Manager and CISO structure
CISO / Head of Information Security	Usually not required as separate role	Expert competence in security governance, risk, resources and strategy
ISMS / Part-IS Manager	May be combined with Safety or Compliance Manager	Practitioner / expert competence in Part-IS implementation
Safety Manager	Working knowledge of cyber-safety links	Strong competence in integrating cyber risk into SMS
Compliance Monitoring	Basic audit and evidence review	Independent assurance and regulatory audit competence
IT / Technical Security	Often outsourced; practitioner competence required from provider	Internal expert teams for infrastructure, cloud, OT, IAM, SOC and engineering
Supplier Manager	Basic contractual and oversight competence	Specialist supplier security and third-party risk management
SOC / Detection	May be external or simplified monitoring	Dedicated detection, SIEM, SOC and response competence
Incident Response	Simple escalation and external support	Dedicated incident response, crisis management and forensic readiness
All Staff	Awareness	Awareness plus role-specific training for critical functions

8 ISO/IEC 27001 Certification

Ch. 8 ISS 1 / REV 0 / 01.04.2025

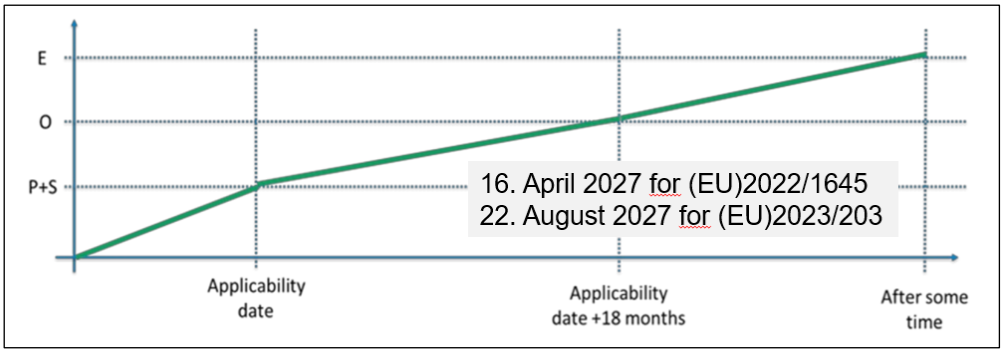
An organisation with a current ISO/IEC 27001 certification is **not** automatically compliant to the requirements of Part-IS, even though the requirements for an ISMS that are specified by Part-IS are in most parts consistent and aligned with ISO/IEC 27001.

However, Part-IS introduces provisions that are specific to the context of aviation safety. If an ISO/IEC 27001-based ISMS is already operated by an entity for a different scope and context, it can be adapted and extended to the scope and context of Part-IS based on an analysis of the scope and gaps. In order to take credit from ISO/IEC 27001 certifications to achieve compliance with Part-IS, aviation safety needs to be included in the organisational risk management, with the relevant risk acceptance level determined by the applicable requirements. Moreover, for a mapping between the main tasks required under Part-IS and the clauses and associated controls in ISO/IEC 27001, refer to Appendix II of the published Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS.

A reference to a dedicated document can be found in chapter Online Resources and References.

9 Part-IS Development Phase 2026-2027

Ch. 9 ISS 1 / REV 2 / 10.07.2026



The FOCA decided to follow the EASA's proposed 18 month transition period to allow organsations to achieve operational maturity level in their ISMS implementation.

This transition period has the following characteristics

- The FOCA acknowledges that organisations will need this time to develop their Information Security Management System from a present and suitable maturity level to a fully operational level.
- Organisations should make best use of this development period to progress towards an operational status.
- It is not to be understood as a grace period, it is to be understood as a development period.
- The FOCA will not perfom any dedicated Part-IS audits during this time, but may very likely assses the progress of the implementation of the ISMS during regular oversight activities. Consequently, findings may be raised if an inspector considers that progress in implementing the requirements of Part-IS is insufficient, or if there is no implementation plan in place demonstrating that implementation will be complete by the end of the transition period.
- The FOCA will not conduct Part-IS audits, as long as the ISMM has not been approved.

10 Online Resources and References

Ch. 10 ISS 1 / REV 2 / 10.07.2026

EASA

- EASA Easy Access Rules for Information Security
- EASA Part-IS Implementation Task Force - Deliverables
- EASA Guidelines ISO/IEC 27001 vs Part-IS
- EASA Guidelines Part-IS oversight approach
- EASA Guidelines Part-IS proportional implementation
- EASA - Cyber Security
- EASA - FAQ General Cyber Security
- EASA - FAQ Part-IS
- European Centre for Cybersecurity in Aviation, ECCSA

FOCA

- FOCA - Aviation Cybersecurity
- FOCA – EU regulation on information security (Part-IS)

National Cyber Security Center, NCSC

- National Cyber Security Centre Switzerland, NCSC
- Information and onboarding to the Cyber Security Hub

Please report broken links to cybersecurity@bazl.admin.ch.

11 Annex

Ch. 11 ISS 1 / REV 1 / 30.06.2025

11.1 Part-IS Compliance Matrix

Ch. 11.1 ISS 1 / REV 2 / 10.07.2026

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FOCA PART-IS COMPLIANCE ASSESSMENT

Please fill only cells below

At this stage, the goal is for FOCA to assess whether the organisation has demonstrated that the foundation elements of the ISMS are established, and the organisation is in a position to operate the ISMS. Most of the evidence that the organisation should provide for the authority's assessment of a present and suitable implementation of the ISMS is expected to be part of the Information Security Management Manual (ISMM), whereas the remaining evidence may only be reviewed during an audit of the organisation.

REGULATORY REQUIREMENTS		Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ORGANISATION ASSESSMENT		
			Yes/No	Reference to internal company procedure	Comment
ORGANISATIONAL STRUCTURE	IS.I/D.OR.240	a) Has the structure been updated to reflect the ISMS (e.g. appointment of an information security manager, reporting structure)?	No		
		o Is there a link between safety, security and information security functions?	No		
		b) Where the organisation has decided to appoint a CRP (Common Responsible Person), does the person have sufficient capacity and delegated authority to effectively implement Part IS in the organisation?	No		
		c) Has the organisation developed a framework/policy to address the different levels of trustworthiness of the workforce? Have the current staff been already assessed for trustworthiness?	No		
		d) Has the organisation developed a competence framework and evaluation process? Have the current staff been already assessed for competence?	No		
INFORMATION SECURITY POLICY	IS.I/D.OR.200(a)(1)	a) Has the organisation developed a clearly defined information security policy?	No		
		o Is the purpose of the policy clearly stated?	No		
		o Are the information security objectives defined?	No		
		o Is the concept of aviation safety an integral part of the policy?	No		
		o Is the content of the policy appropriate to the complexity of the organisation?	No		

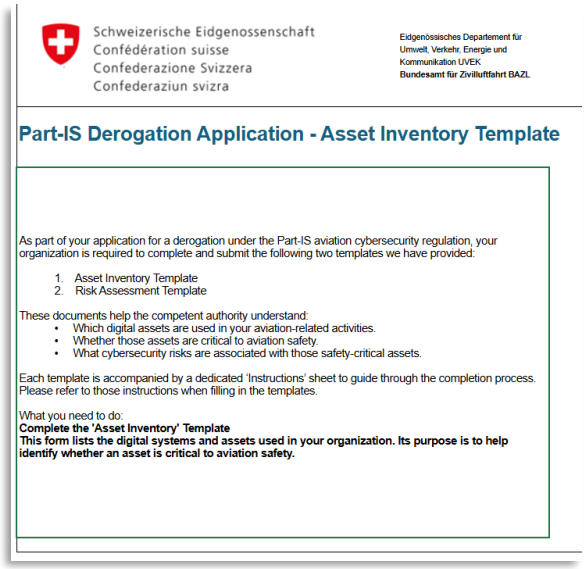
The template is available on the FOCA Website – Information Security under the "Publication" tab.

11.2 ICT-Asset Inventory and Risk Assessment for Derogation

Ch. 11.2 ISS 1 / REV 2 / 10.07.2026

The purpose of an ICT asset inventory is to provide a comprehensive, up-to-date record of all ICT assets within an organisation to help assessing the decision of a derogation application. That inventory helps the FOCA to understand, which digital assets are used in your aviation related activities, and whether those assets are critical to aviation safety.

As per IS.OR.200(e) a decision on a derogation approval shall be based on a documented information security risk assessment carried out by the applicant organisation or an assigned third party. In accordance with IS.OR.205(c), this information security risk assessment shall identify the information security risks which may have a potential impact on aviation safety. The purpose of that document is to assist the organsation in this task.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Zivilluftfahrt BAZL

Part-IS Derogation Application - Asset Inventory Template

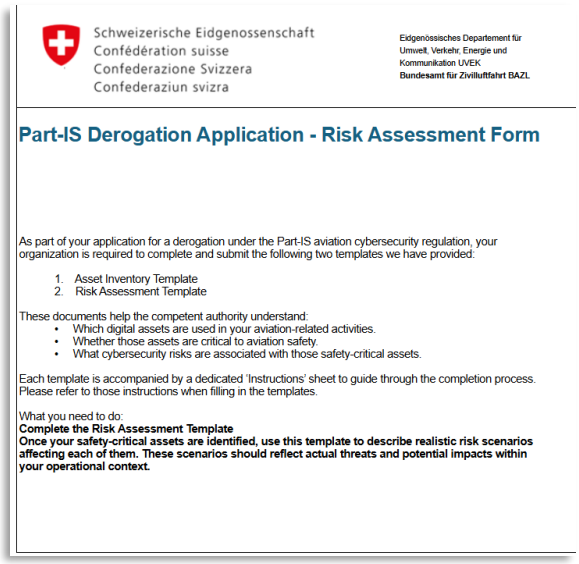
As part of your application for a derogation under the Part-IS aviation cybersecurity regulation, your organization is required to complete and submit the following two templates we have provided:

1. Asset Inventory Template
2. Risk Assessment Template

These documents help the competent authority understand:
- Which digital assets are used in your aviation-related activities.
- Whether those assets are critical to aviation safety.
- What cybersecurity risks are associated with those safety-critical assets.

Each template is accompanied by a dedicated 'Instructions' sheet to guide through the completion process. Please refer to those instructions when filling in the templates.

What you need to do:
Complete the 'Asset Inventory' Template
This form lists the digital systems and assets used in your organization. Its purpose is to help identify whether an asset is critical to aviation safety.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Zivilluftfahrt BAZL

Part-IS Derogation Application - Risk Assessment Form

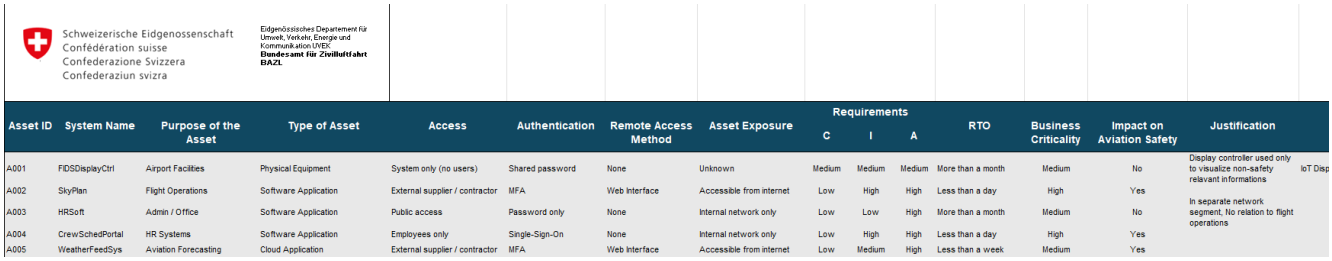
As part of your application for a derogation under the Part-IS aviation cybersecurity regulation, your organization is required to complete and submit the following two templates we have provided:

1. Asset Inventory Template
2. Risk Assessment Template

These documents help the competent authority understand:
- Which digital assets are used in your aviation-related activities.
- Whether those assets are critical to aviation safety.
- What cybersecurity risks are associated with those safety-critical assets.

Each template is accompanied by a dedicated 'Instructions' sheet to guide through the completion process. Please refer to those instructions when filling in the templates.

What you need to do:
Complete the Risk Assessment Template
Once your safety-critical assets are identified, use this template to describe realistic risk scenarios affecting each of them. These scenarios should reflect actual threats and potential impacts within your operational context.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Zivilluftfahrt BAZL

Asset ID	System Name	Purpose of the Asset	Type of Asset	Access	Authentication	Remote Access Method	Asset Exposure	Requirements			RTO	Business Criticality	Impact on Aviation Safety	Justification	
								C	I	A					
A001	FIDSDisplayCtrl	Airport Facilities	Physical Equipment	System only (no users)	Shared password	None	Unknown	Medium	Medium	Medium	More than a month	Medium	No	Display controller used only to visualize non-safety relavant informations	IoT Disp
A002	SkyPlan	Flight Operations	Software Application	External supplier / contractor	MFA	Web Interface	Accessible from internet	Low	High	High	Less than a day	High	Yes		
A003	HRSoft	Admin / Office	Software Application	Public access	Password only	None	Internal network only	Low	Low	High	More than a month	Medium	No	In separate network segment, No relation to flight operations	
A004	CrewSchedPortal	HR Systems	Software Application	Employees only	Single-Sign-On	None	Internal network only	Low	High	High	Less than a day	High	Yes		
A005	WeatherFeedSys	Aviation Forecasting	Cloud Application	External supplier / contractor	MFA	Web Interface	Accessible from internet	Low	Medium	High	Less than a week	Medium	Yes		

The template is available on the [FOCA Website – Information Security] under the “Publication” tab.