Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

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

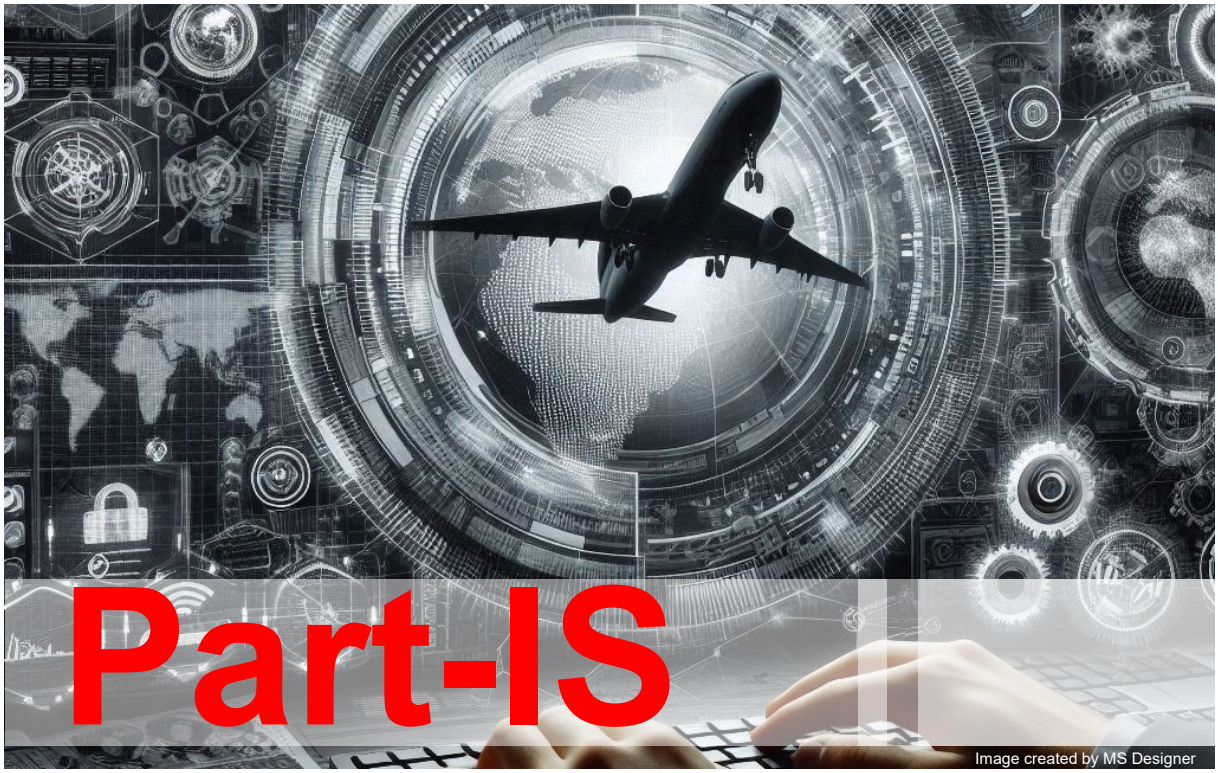
Federal Office of Civil Aviation FOCA
Safety Divisions

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
Valid from	01.04.2025
Version	ISS 01 / REV 00

Business object	033.1-1/152/1/3
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)

List of Effective Chapters

List of Abbreviations

LoA ISS 1 / REV 0 / 01.04.2024

The following abbreviations are within this GM/INFO:

Abbreviation	Definition
CAP	Corrective Action Plan
EASA	European Aviation Safety Agency
ED	Executive Director
FOCA	Federal Office of Civil Aviation
GM/INFO	Guidance Material / Information
ISMS	Information Security Management System
SMS	Safety Management System
ISMM	Information Security Management Manual
OMM	Organisation's Management Manual
CL	Certification Leaflet
IJ	Implementing Journal
ATO	Approved Training Organisation
FSTD	Flight Simulation Training Device
BITD	Basic Instrument Training Device
FNPT	Flight Navigation Procedures Trainer
FTD	Flight Training Device
CAMO	Continuing Airworthiness Management Organisation
CVSS	Common Vulnerability Scoring System
SPO	specialised operations
AOC	air operator certificate
NCC	non-commercial air operations with complex motor-powered aircraft
MOA	maintenance organisation approval
POA	production organisation approval
ATM	Air Traffic Management
ANS	Air Navigation Services
ICAO	International Civil Aviation Organisation
EU	European Union
AeMC	Aero Medical Centres
USSP	U-Space Service Providers
CAME	Continuing Airworthiness Management Exposition
MOE	Maintenance Organisation Exposition
POE	Production orgnisation Exposition
MOPSC	Maximum Operational Passenger Seating Configuration
ELA 2	European Light Aircraft
CMPA	Complex Motor Powered Aircraft

Table of Contents (ToC)

ToC ISS 1 / REV 0 / 01.04.2025

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 0 / 01.04.2025

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

0.2 Legal References

Ch. 0.2 ISS 1 / REV 0 / 01.04.2025

Basic Regulation (EU) 2018/1139

Commission Implementing Regulation (EU) 2023/203

Commission Delegated Regulation (EU) 2022/1645

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

ED Decision 2023/008/R

ED Decision 2023/009/R

0.3 Purpose of this GM/INFO

Ch. 0.3 ISS 1 / REV 0 / 01.04.2025

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 as part of their regular oversight activities.

In addition, this document should serve to identify and evaluate a possible derogation within the organisation and also 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 of 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 0 / 01.04.2025

Before notifying FOCA about any changes[3], 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 the approved process

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

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 0 / 01.04.2025

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.

[3] Prior approval and NOT requiring prior approval

- 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 in 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 0 / 01.04.2025

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 who is responsible for communication, investigation, and resolution.

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.I.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, data flows, and third-party services that support daily activities.

Part-IS.I/D.OR 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.I/D.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 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 documented and integrated into the overall Information Security Management System (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.

Incident detection, response and recovery

Setting up robust mechanisms for 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 from 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 fators and processes.

Even though, a profound IT-knowledge is required in many aspects in 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 training is a crucial component of the Information Security Management System (ISMS) outlined in Part-IS.I/D.OR.

In the initial implementation phase, it is essential to develop a comprehensive training programme that covers all aspects of information security relevant to your organisation. This programme 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. Especially 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.I/D.OR.230. This ensures transparency and compliance with legal requirements, helping to build trust with regulatory bodies and stakeholders.

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 0 / 01.04.2025

If the organisation choses to establish a separate ISMM, the initial issue shall be approved by FOCA as required by Part-IS point IS./D.OR.250(b). However, as described under point 2, the preferred method is to integrate the content of an ISMM into other expositions (e.g. OMM) already held by the organisation.

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).

2.3 Submission of application documents

Ch. 2.3 ISS 1 / REV 0 / 01.04.2025

FOCA expects that all concerned organisations submit the documentation sufficiently, at least a minimum of 8 weeks in advance, of the applicability date of Part-IS through the applicable FOCA processes. Because of the high volume of applications expected, it might not be possible for FOCA to process the submissions before the applicability date.

3 Derogation

Ch. 3 ISS 1 / REV 0 / 01.04.2025

The FOCA recognises the possibility of an organisation to obtain an approval not to implement the requirements of Part-IS in accordance with IS.I/D.OR.200(e) and will support an application wherever possible and appropriate. In doing so, the FOCA relies not only on the regulation but also on the additional guideline issued by the EASA for the application of derogation, where it is adequate and applicable for the Swiss civil aviation landscape (see Online Resources and References).

Without prejudice to the obligation to comply with the reporting requirements laid down in Commission Regulation (EU) No 376/2014(1) and the requirements of point IS.I/D.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.I/D.OR.205 to IS.I/D.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 the information security, which must be carried out by the organisation or a third party in accordance with point IS.I/D.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. 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**. Despite the fact, that 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.

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

3.1 Air Operations, Aircrew and Aero medical Centres

Ch. 3.1 ISS 1 / REV 0 / 01.04.2025

Likelihood of approval[4]	Condition	Affected Approvals
A request on derogation is most likely denied by FOCA	• The organisation is systemically relevant at the federal level: a. Monopoly/systemically important (aviation policy = international accessibility), e.g. Flag Carriers b. 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**

[4] 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.

3.2 Products, part and appliances

Ch. 3.2 ISS 1 / REV 0 / 01.04.2025

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* assessment).	**1. Safety-related or critical services and products of the organisations are not provided by digital processes and informations**	
	1.A No digital controlled shelf-life of materials, components or maintenance intervals	**POA / MOA**
	1.B No field loadable software (or provision of those)	**MOA / CAMO**
	1.C. No digital maintenance records	**MOA / CAMO**
	2. OT systems are not or only minimally interconnected with IT systems and are not connected to the public network	
	2.A No interconnected calibration tools and test stands	**MOA / POA**
	2.B CNC production systems for critical and structural A/C parts and HVAC systems for manufacturing floors are not connected to the internet	**POA (partly MOA, if applicable)**
	2.C The organisation does not operate any web applications that have a direct or indirect influence on its productive systems	**POA, MOA, CAMO**

* **Case-by-case basis:** 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.

3.3 Aerodromes

Ch. 3.3 ISS 1 / REV 0 / 01.04.2025

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, LSGS) are not in scope of Part-IS. Therefore is no need to issue a derogation request.	**ICAO airports**

3.4 Air Traffic Management

Ch. 3.4 ISS 1 / REV 0 / 01.04.2025

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).	**USSP**

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

4 Reporting of information Security Incidents and Vulnerabilities

Ch. 4 ISS 1 / REV 0 / 01.04.2025

As mentioned in the key requirements under point 2.1., maintaining comprehensive records of information security incidents and actions taken is essential for the effectiveness of your Information Security Management System.

4.1 Internal Reporting

Ch. 4.1 ISS 1 / REV 0 / 01.04.2025

Establish clear internal processes and procedures for staff to report observed or suspected security events. Procedures and responsibilities should be defined for evaluation of events and decision of 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.

4.2 External Reporting

Ch. 4.2 ISS 1 / REV 0 / 01.04.2025

Notify FOCA about significant incidents, especially those with potential safety impacts, within specified timeframes. Procedures to identify which incidents and vulnerabilities have to be reported through the external reporting system should 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 an 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.
- Passenger Data Breach: Cyberattacks targeting passenger data can lead to identity theft and other security concerns, indirectly affecting overall aviation 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.

Reporting of vulnerabilities

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).

- Common known vulnerabilities within a critical information system (operating system, application) which renders a CVSS Score of 9.0 or higher and which cannot be patched within a reasonable time or within the standard vulnerability management process.
- 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.
- Outdated systems: Legacy systems may lack modern security features, making them more susceptible to cyberattacks.
- Insecure supply chains: Compromised components or software from suppliers can introduce vulnerabilities into aviation systems

First notification & Report

The way and tool to use to notify and report is currently under clarification with NCSC in order to minimize the reporting effort for the orgnizations.

4.3 Collaboration Across Stakeholders

Ch. 4.3 ISS 1 / REV 0 / 01.04.2025

Share relevant incident information with other entities in the aviation ecosystem to enhance collective security resilience.

All the staff involved have to be properly trained about the respective procedures and processing/handling of reports.

5 ISO/IEC 27001 Certification

Ch. 5 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.

6 Online Resources and References

Ch. 6 ISS 1 / REV 0 / 01.04.2025

- EASA Guidelines ISO/IEC 27001 vs Part-IS
- EASA Implementation guidelines for Part-IS derogation
- EASA Guidelines Part-IS oversight approach
- Easy Access Rules for Information Security
- EASA - Cyber Security
- EASA - FAQ General Cyber Security
- EASA - FAQ Part-IS
- EASA - Part-IS Training
- European Centre for Cybersecurity in Aviation, ECCSA
- FOCA - Aviation Cybersecurity
- National Cyber Security Centre Switzerland, NCSC
- FOCA GM/INFO CL Management System

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