

INFORMATION SECURITY(IS) (EASA PART IS) (UNDERSTANDING

WHAT IS INFORMATION SECURITY (PART IS):

In simple terms:

**Management of information (and cyber) security risks
with a potential impact on aviation safety**

Currently a next safety net is introduced:

PART IS – Information Security

EASA PART IS becomes applicable for Part 21J/G organizations on 16 October 2025
(for Maintenance and Continuing Airworthiness Management 22 February 2026).

The application date is in the future, but not too far away.

Workshops from EASA and national authorities currently scheduled.

[Easy Access Rules for Information Security \(Regulations \(EU\) 2023/203 and 2022/1645\)](#)

[Delegated regulation - 2022/1645 - EN - EUR-Lex](#)

WHY INFORMATION SECURITY (PART IS):

- Most aviation processes, equipment and communication network are **now digitized**
- Airlines and the aviation industry as a whole find **information security (including cybersecurity) of great importance** - the entire process from safety, passenger comfort to the business may be impacted if they go wrong or jeopardized.
- The aviation industry has seen a surge in **ransomware attacks** in recent years and cyber incidents are a serious threat to business continuity.
- Not including all events of Information Security, Data shows **cyber attacks** alone rose by 131% between 2022 across the aviation industry.



PART IS (INFORMATION SECURITY)

Feb 2026

WHAT IS THE ORIGIN OF PART IS (IN THE DIGITAL AGE WE LIVE IN)

- Before the introduction of radio communication, aircraft communicated with ground crews and other aircraft using visual and auditory signals
- Until radio communication was introduced in 1915
- Most of office files were in hard copy
- Then computers were introduced and all information held in digital files
- Pilots would carry their hard copy flight manuals in heavy bags
- And then we went to the digital age with the EFB (Electronic Flight Bag)
- Use of electronic equipment in offices, airplanes, airports, air traffic has created risks that can seriously affect aviation safety
- **LIKE SYSTEMS IN BUSINESS, SUPERMARKETS, HOSPITALS ETC, THIS HAS BROUGHT ON RISKS WHICH IN AVIATION IS DESCRIBED AS "INFORMATION SECURITY" AND THEREFORE THESE RISKS HAVE TO MITIGATED**



Earliest communication was visual signalling



Aircraft radio communication first used 1915



We used hard copy papers



Then we had computers since 1980s



Pilots carried flight manual in a bag



Now it is compressed in an Electronic Flight Bag (EFB)



WITH MOST AVIATION PROCESSES AND EQUIPMENT DIGITIZED, THIS CAN LEAD TO IN SERVICE SAFETY RISKS





INCIDENTS LIKE THESE LEADS TO THE CONCERN OF INFORMATION SECURITY AND HENCE THE REGULATORS FEEL THE NEED TO INTRODUCED A “PART IS” THROUGH REGULATIONS

PART IS (INFORMATION SECURITY) SOME MITIGATING ACTIONS

No	Date	Problem	Mitigating action
1	Oct 2006	A330/340 Blanking of flight deck Display Units in flight	first reset/reboot , next software change
2	From 2000	PED Interference with flight deck instruments	PEDs switch off take off landing,. Pre flight safety warnings- Flight crew prepared with appropriate equipment
3	Jan 2022/2023	"5G" Mobile phone use, concerns may affect aircraft instruments including altimeter. Disruption of flights into US	FAA ruled that operators equip with either 5G C – Band tolerant rad altimeters or approved filters
4	Feb 2024	EFB (Electronic Flight Bags -tablets with lithium battery) used by Pilots in Cockpit, which carries risk of fire (like in the cabin)	Use of integrated EFB, or follow the EASA guidelines in case of using tablets and holders for EFB
5	2022/2023	Passenger using Computer Apple "AirDrop" sends frightening messages to other passengers on plane – flight disruption	Immediate arrest of passengers – clear deterrent message to attackers that they are breaking the law and will not try this. Also Apple computer advised of their system to ensure better data control
6	Current	Data control for Aviation Design, Production and Maintenance Organisations (-incorrect (technical) classifications , unauthorized data modification or approval, supplier & data integrity issues, significant in-service findings linked to the design, design data stolen or subject to cyberattack , unauthorized data transmittal or deletion)	Data security control systems , like firewall blocking of risk data , internal audit and external regulatory EASA audit of company's system. Important for immediate notification to sender and recipient – to ensure that aviation secure systems are in place
7	Aug 2022	Global "safety alert for operators" US FAA an issue with Boeing's Onboard Performance Tool (OPT), a mobile app that pilots can use to make safety calculations before take-off and landing. Possible flaw meant hackers could tamper with critical data and trick pilots into using the wrong settings, potentially causing a crash.	Software change
8	2023/2025	GPS Spoofing/Interference – Can cause Aircraft navigation problems	Mitigation possible to guard against interference - like AIM(advanced interference monitoring mitigation) NovAtel GRIT (GMSS Resilience and Integrity Technology etc
9	Aug 2024/ Dec 2024	Regulators FAA/EASA (and ICAO) concerns on Information Security (Cyber Security) Introduce Regulation Changes Some practical examples may be: -incorrect (technical) classifications , unauthorized data modification or approval, supplier & data integrity issues significant in-service findings linked to the design, design data stolen or subject to cyberattack , unauthorized data transmittal or deletion	Introduction of Regulation Change – EASA Part IS . Organisations Design , Production and Maintenance to have an ISMS (Information Security Management System) 2025/206 Information Security (Regulations (EU) 2023/203 and 2022/1645)

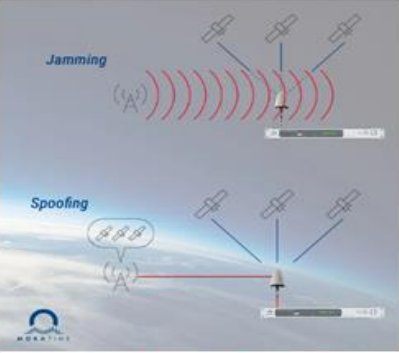
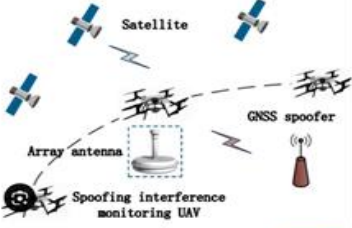


PART IS (INFORMATION SECURITY) SOME MITIGATING ACTIONS IN DETAIL

No	Date	Problem	Mitigating action
1	Oct 2006	A330/340 Blanking of flight deck Display Units in flight 	First reset/reboot , next software change/upgrade 
2	From 2000	PED Interference with flight deck instruments  	PEDs switch off take off landing.. Pre flight safety warnings- Flight crew prepared with appropriate equipment. Passengers are warned Not to use PEDs in flight  
3	Jan 2022/2023	“5G” Mobile phone use, concerns may affect aircraft instruments including altimeter. Disruption of flights into US  	FAA ruled that operators equip with either 5G C –Band tolerant rad altimeters or approved filters 
4	Feb 2024	EFB (Electronic Flight Bags -tablets with lithium battery) used by Pilots in Cockpit, which carries risk of fire (like in the cabin) 	Use of integrated EFB, or follow the EASA guidelines in case of using tablets and holders for EFB  



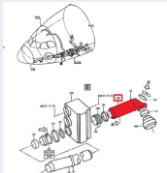
PART IS (INFORMATION SECURITY) SOME MITIGATING ACTIONS IN DETAIL

No	Date	Problem	Mitigating action
5	2022/2023	<p>Computer Apple "Air Drop" frightening messages Passengers send "AirDrop" to <u>send frightening</u> messages to other passengers on plane – flight disruption <u>AirDrop</u> has become a powerful and easy tool for cyberattacks in the aviation industry. The risks to the flight's safety may be minimal, but they are real and can cause considerable financial damage to airlines.</p>  <p>Typical Air Drop message</p>	<p>1.Immediate arrest of passengers – clear deterrent message to attackers that they are breaking the law and will not try this. <u>Also</u> Apple computer advised of their system to ensure better data control 2.Airlines <u>to ensure</u> that pilots and flight crew are properly trained and informed of this potential vulnerability to quickly mitigate and solve such situations, as they will only increase over time. 3The pilot QHR (Quick Reference Handbook) has no reference or checklist to handle such scenarios. Airlines have no instructions or mitigation to overcome such events, and so, every pilot handled the situation mentioned above as they felt. <u>It strongly</u> suggest that pilots must be trained to handle constantly evolving cyberattacks to prevent this situation. 4.Passenger advised to turn off <u>AirDrop</u> or set it to "Receiving off" in the</p> <p><u>PED setting.</u> </p> <p>5.<u>Legal Consequences.</u>, including fines and potential prison sentences</p> 
6	Current	<p>Data Control for Aviation Design, Production and Maintenance <u>Organisations</u> (-incorrect (technical) <u>classifications</u>, <u>unauthorized data modification</u> or approval, <u>supplier & data integrity issues</u>, <u>significant in-service findings</u> linked to the design, <u>design data stolen</u> or <u>subject to cyberattack</u>, <u>unauthorized data transmittal</u> or <u>deletion</u>) Fake documentation</p> 	<p>Data security control <u>systems</u>, like firewall blocking of risk data , internal audit and external regulatory EASA audit of company's system. Important for immediate notification to sender and recipient – to ensure that aviation secure systems are in place (sender will not repeat). Legal prosecution</p>  <p>Legal action Prank message "On my way to blow up the plane (I'm a member of the Taliban)." -Audit</p>
7	Aug 2022	<p>Hacking of Boeing's Onboard Performance Tool (OPT). US FAA identifies an issue with Boeing's Onboard Performance Tool (OPT), a mobile app that pilots can use to make safety calculations before take-off and landing. Possible flaw meant hackers could tamper with critical data and trick pilots into using the wrong settings, potentially causing a crash.</p> 	<p>FAA Global Safety Alert</p>  <p>U.S. Department of Transportation Federal Aviation Administration</p> <p>SAFO Safety Alert for Operators</p> <p>SAFO 22002 DATE: 07/25/22 Flight Standards Service Washington, DC</p> <p>Recommended action: 1.Operators using OPT for iOS should obtain copy of applicable MOM and any subsequent communication from Boeing 2.Operators should identify and verify the OPT software version on any electronic flight bag (EFB) hosting OPT for iOS software and take any necessary corrective measures as identified by MOM</p> <p>Hackers will be aware of this and not try to continue to cyber attack</p>

PART IS (INFORMATION SECURITY) SOME MITIGATING ACTIONS IN DETAIL (CONTD)

No	Date	Problem	Mitigating action
8	2023/2025	<p><u>GPS Spoofing/ Jamming (Interference) –</u> Can cause Aircraft navigation problems</p> 	<p>Mitigation possible to guard against interference - like AIM(advanced interference monitoring mitigation) NovAtel GRIT (GMSS Resilience and Integrity Technology/monitoring etc</p>  <p>Localization of GNSS Spoofing Interference Source Based on a...</p>
9	Aug 2024/ Dec 2024	<p><u>Information Security (Cyber Attacks etc) General</u> Regulators FAA/EASA (and ICAO) concerns on Information Security (Cyber Security etc) Introduce Regulation Changes Some practical examples may be: <i>-cyber attacks, incorrect (technical) classifications, unauthorized data modification or approval, supplier & data integrity issues significant in-service findings linked to the design, design data stolen or subject to cyberattack, unauthorized data transmittal or deletion</i> General:</p> 	<p>Introduction of Regulation Change – EASA Part IS, Organisations Design, Production and Maintenance to have an ISMS (Information Security Management System) 2025/206 Information Security (Regulations (EU) 2023/203 and 2022/1645)</p> 

PART IS (INFORMATION SECURITY) TYPICAL APPLICATIONS (LARGE AND SMALL DOAS)

Problem	IS Action	DOA
<p>"5G" concerns may affect aircraft instruments including altimeter. Disruption of flights into US</p> 	<p>FAA ruled that operators equip with either 5G C – Band tolerant rad altimeters or approved Fitment of Filters</p> 	<p>Large DOAs <u>Operation:</u> Mitigate against attacks/interference, like cyber attacks. With the appropriate EASA approved scope will issue Change (STC) to install 5G resistant Rad Altimeters. In addition to identify any IS risks and issue mitigating action for risks <u>Typical Consideration</u> <u>Data/Documentation Control:</u> For the change protect/mitigate against: <i>-incorrect (technical) classifications ,unauthorized data modification or approval,supplier & data integrity issues,significant in-service findings linked to the design,design data stolen or subject to cyberattack, unauthorized data transmittal or deletion) Fake documentation</i></p>
<p>Installation of any change , related to or unrelated to IS Like fitment of an air condition duct .</p>	<p>Typical minor change, an air condition duct , low or no probability of impacting information security (IS)</p> 	<p>Small DOAs <u>Operation:</u> Confirm change(mod) has no impact on operation IS (i.e cyber attacks , EMI interference etc) <u>Data/Documentation Control :</u> As above (see page 8)</p>


PART IS (INFORMATION SECURITY) ASSESSMENT OF POTENTIAL RISKS (PART OF SMS) (FOR TYPICAL MINOR CHANGE PER PAGE 12)


	HAZZARD/RISK IDENTIFIED	HAZZARD/RISK DESCRIPTION	RISK CLASSIFICATION- RED/YELLOW/GREEN (apply /matrix below)	MITIGATION MEANS FOR RISKS CLASSIFSSIFIED RED OR YELOW
*	Information Security	Check the extent Part IS to be considered introduced with this change.	B2	<ol style="list-style-type: none"> 1. All change documents are exchanged between stake holders in secure pdf format, hence there is low risk of external parties (cyber attack) access the documents to alter any information with the intension of jeopardising the process. 2. Certification and compliance documents like manufacturing drawings etc, /are forwarded to the customer in a controlled manner ., where IP intellectual Property and sensitive data cannot be used by any non approved company to make fake imitation parts, that could be inferior get on to the airplane and jeopardise safety levels. 3. All design documents for signature go through a Design Assurance (management) check and balance system with multiple signature levels...hence any incorrect/ misleading/errors in the information is picked up and corrected. In addition the ISM internal quality monitoring system and EASA auditors oversee the documents. 4.All design document projects are stored and well guarded IT ERP system. 5.The company IT communication through email system is protected with a strong security sensitive firewall system that blocks incoming mail which are in unfavorable and outdated formats. There are attempts to enhance/improve the system further with more pronounced alerting system in “best practices”when files are blocked in order to improve the efficiency and smooth running of two way communication. 6.Exchanges between stakeholders for certification of the documents are exchanged and recorded in a document called Comments Sheet (CF), hence to ensure the accuracy of the information and a record in the unlikely event later in in an investigation , clarification can be obtained by referring to the CF sheet.


PART IS (INFORMATION SECURITY) ASSESSMENT OF POTENTIAL RISKS (PART OF SMS)

Risk classification matrix:

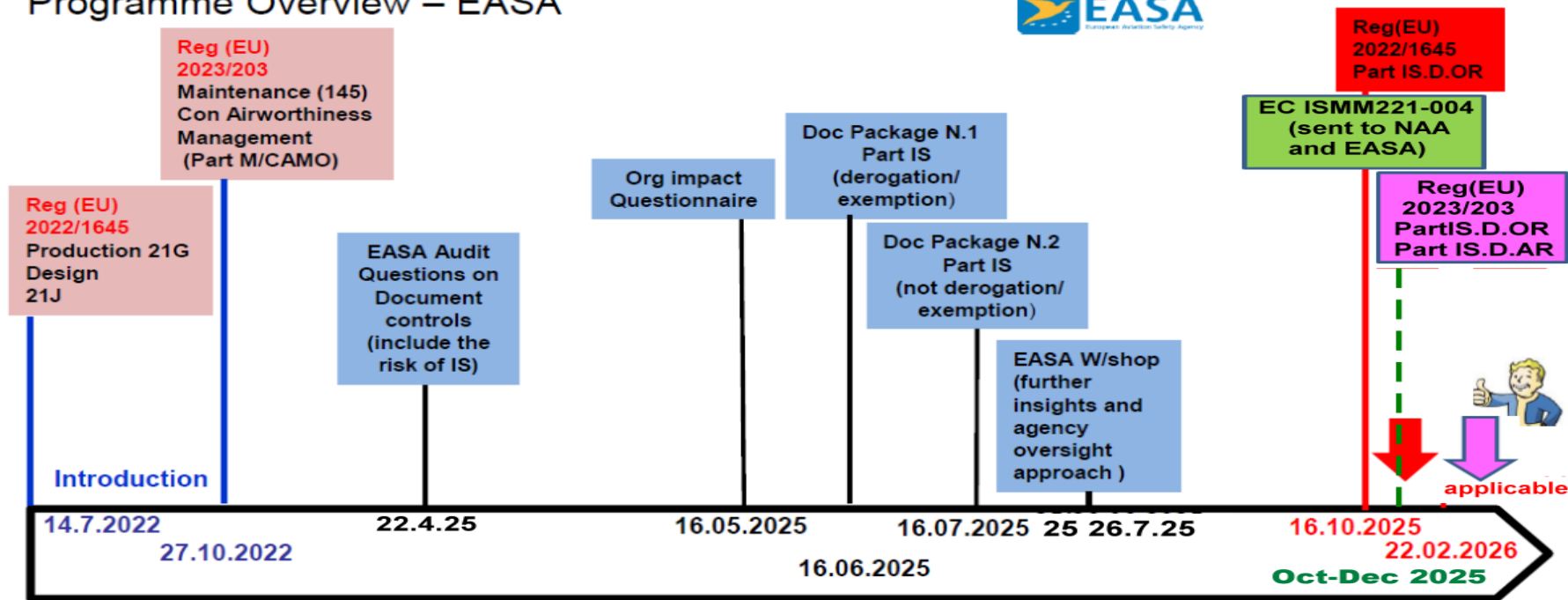
RISK PROBABILITY / RISIKO WAHRSCHEINLICHKEIT	RISK SEVERITY / SCHWEREGRAD DES RISIKOS				
	5 (catastrophic/ katastrophal)	4 (hazardous/ gefährlich)	3 (major/ groß)	2 (minor/ gering)	1 (negligible/ unbedeutend)
E (frequent/ häufig)	E5	E4	E3	E2	E1
D (occasional/ gelegentlich)	D5	D4	D3	D2	D1
C (remote/ gering)	C5	C4	C3	C2	C1
B (improbable/ unwahrscheinlich)	B5	B4	B3	B2	B1
A (extremely improbable/ sehr unwahrscheinlich)	A5	A4	A3	A2	A1

 unacceptable risks area with risk control actions/
Bereich mit inakzeptablem Risiko - Kontrollmaßnahmen erforderlich

 risk area under monitoring for actions if necessary/
risikobehafteter Bereich zur weiteren Überwachung - ggf. Maßnahmen treffen

 acceptable risks area without risk control actions/
Bereich mit akzeptablem Risiko - keine weiteren Maßnahmen erforderlich

Programme Overview – EASA



PART IS JOURNEY