	STANDARDISATION						REGULATION				1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status																			
ATM/ANS	Interoperability of Flight Data Processing (Air Traffic Control - Air Traffic Control) for application under the Single European Sky - Interoperability Regulation EC 552/2004	CEN/TS 16071	CEN	2010	Published	ISO/IEC												x											Technical Specification
ATM/ANS	Security Certification and Declaration of ATM ANS Ground Systems	ED-205A	EUROCAE WG-72	2022	Published	RTCA / DO-393					x			x	x	x	x	x							x	x		x	
ATM/ANS	Security Management Handbook - A Framework	Edition 1.0, May 2008	EUROCONTROL	2008	Published										x			x							x				
ATM/ANS	ICT Security Guidance	Edition 1.0, May 2008	EUROCONTROL	2008	Published						x			x	x	x								x	x	x			
ATM/ANS	ATM Security Risk Management Toolkit - Guidance Material	Edition 1.0, September 2010	EUROCONTROL	2010	Published										x			x								x			
ATM/ANS	ATM Security Risk Management Toolkit - Guidance Material - Appendices	Edition 1.0, September 2010	EUROCONTROL	2010	Published										x			x								x			
ATM/ANS	Manual for National ATM Security Oversight	Edition 3.0, December 2016	EUROCONTROL	2016	Published									x				x											
ATM/ANS	ATM Security Policy - Guidelines for Implementation		EUROCONTROL/NATO	2015	Published	NATO									x			x								x			ATM Security Coordination Group, (NEASCOG)
ATM/ANS	Security Risk Assessment Methodology for SESAR 2020 (SecRAM 2.0 + corresponding catalogue)		SESAR 2020	TBC	Published						x				x	x		x				x				x	x		Internal S2020 standard
TRANSVERSAL																													
Transversal	Supplement 3 to ARINC REPORT 667: GUIDANCE FOR THE MANAGEMENT OF FIELD LOADABLE SOFTWARE	ARINC 667 Supplement 3	ARINC	2022	Draft														x	x		x	x						A667-3 will include requirements for securely managing operation of dataloaders and handling software
Transversal	Supplement 1 to ARINC Report 645: Common Terminology and Functions for Software Distribution and Loading	ARINC 645 Supplement 1	ARINC	2021	Published											x			x	x		x	x						Applies to manufacturers and operators. A645-1 includes definition and technical requirements for secure dataloaders.
Transversal	Electronic Distribution of Software by Crate (EDS Crate)	ARINC 827	ARINC	2010	Published												x		x	x		x	x						
Transversal	Standard Guide for Cybersecurity and Cyberattack Mitigation	ASTM F3286-17	ASTM	2017	Published																						x		
Transversal							ESCP - Regulatory Processes Work Stream	EASA	2021/4Q	Ongoing	x	x		x	x	x	x	x	x	x		x			x	x	x	x	Coordinating the discussion about Rule Making Task.0720 (aka "horizontal rule") - Implementing Rule NPA June 2019, Opinion 2Q2020
Transversal							ESCP - Regulatory Processes Work Stream	EASA	2021/4Q	Ongoing	x	x		x	x	x	x	x	x	x		x			x	x	x	x	Coordinating the discussion about Rule Making Task.0720 (aka "horizontal rule") - AMC
Transversal	Guidance On Security Event Management	ED-206	EUROCAE WG-72	2022	Published	RTCA DO-392										x		x								x	x	x	x	ED-XXX ISEM will provide more detailed guidance than F3286-17 and tailloring toward proposed regulation. F3286-17 "Standard Guide for Cybersecurity and Cyberattack Mitigation" by ASTM was published 09-Jul-05.
Transversal	Aeronautical Information System Security (Aiss) Framework Guidance	ED-201A	EUROCAE WG-72	2021	Published	RTCA DO-391					x	x			x	x	x	x	x	x		x	x			x	x	x	

	STANDARDISATION						REGULATION				1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	**Standardisation activity**	**Reference**	**Standardisation organisation**	Target date for standard publication	Status	**Joint activity**	**Regulatory activity**	**Regulatory organisation**	**Target date for regulatory material publication**	**Status**																			
Transversal	Security Services for Aeronautical Communications	Doc. 10090	ICAO	2022	Draft																								Information to be completed.
Transversal	Secure Dialog Service Tech Manual / ConOps / Guidance	Doc. 10094	ICAO	2022	Draft																								Information to be completed.
Transversal	PKI SecurityPolicy	Doc. 10095	ICAO	2022	Draft																								Information to be completed.
Transversal	Security Risk Assessment for Aeronautical Comm	Doc.10145	ICAO	2022	Draft																								Information to be completed.
Transversal	Considerations for Digital Twin Technology and Emerging Standards	NIST IR 8356	NIST	2021	Draft							x										x	x						
Transversal	Security and Privacy Controls for Information Systems and Organizations	US NIST 800-53 rev.5	NIST	2020	Published						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Transversal	Security and Privacy Controls for Federal Information Systems and Organizations	US NIST 800-53 rev.4	NIST	2015	Published						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
Transversal	Cyber Physical Systems Security Engineering Plan	JA7496	SAE G-32 Cyber Physical Systems Security	2022	Published						x				x		x		x			x	x		x	x	x		A cross sector Standard for assessing and addressing vulnerabilities of a cyber physical system to ensure security and reslience throghout the lifecyle of the system.
Transversal	Cyber Physical Systems Security Hardware Assurance	JA6801	SAE G-32 Cyber Physical Systems Security	2022	Draft						x				x		x		x			x	x		x	x	x		
Transversal	Cyber Physical Systems Software Assurance.	JA6678	SAE G-32 Cyber Physical Systems Security	2022	Draft						x				x		x		x			x	x		x	x	x		
	OTHER AVAILABLE STANDARDS																												
Other available standards	mobile networks security; 3G, 4G, 5G	all security work 3G and beyond	.3GPP SA3		Published												x						x						
Other available standards	Standard Guide for Credentialing for Access to an Incident or Event Site	ASTM E2842-14	ASTM	2014	Published									x												x	x		
Other available	Protection profiles for secure signature creation device - Part 1: Overview	EN 419211-1	CEN	2014	Published						x																		European Standard
Other available standards	Protection profiles for secure signature creation device - Part 2: Device with key generation	EN 419211-2	CEN	2013	Published										x	x	x					x			x		x		European Standard
Other available standards	Protection profiles for secure signature creation device - Part 3: Device with key import	EN 419211-3	CEN	2013	Published											x	x					x			x		x		European Standard

	STANDARDISATION						REGULATION				1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status																			
Other available standards	Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application	EN 419211-4	CEN	2013	Published											X	X					X			X		X		European Standard
Other available standards	Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application	EN 419211-5	CEN	2013	Published											X	X					X			X		X		European Standard
Other available standards	Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application	EN 419211-6	CEN	2014	Published											X	X					X			X		X		European Standard
Other available standards	Security requirements for device for authentication - Part 1: Protection profile for core functionality	EN 419251-1	CEN	2013	Published											X	X					X			X		X		European Standard
Other available standards	Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application	EN 419251-2	CEN	2013	Published											X	X					X			X		X		European Standard
Other available standards	Security requirements for device for authentication - Part 3: Additional functionality for security targets	EN 419251-3	CEN	2013	Published											X	X					X			X		X		European Standard
Other available	Protection profile for trustworthy systems supporting time stamping	FprEN 419231	CEN	2019	Ongoing											X	X					X			X		X		European Standard
Other available standards	Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016)	EN ISO/IEC 27000	CEN and CENELEC	2017	Published	ISO/IEC					X																		European Standard
Other available standards	Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)	prEN ISO/IEC 27000 rev	CEN and CENELEC	2019	Ongoing	ISO/IEC					X																		European Standard
Other available standards	Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)	EN ISO/IEC 27001	CEN and CENELEC	2017	Published	ISO/IEC						X			X	X	X		X	X		X			X		X		European Standard
Other available standards	Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)	EN ISO/IEC 27002	CEN and CENELEC	2017	Published	ISO/IEC						X			X	X	X		X	X		X			X		X		European Standard
Other available standards	Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)	EN ISO/IEC 27037	CEN and CENELEC	2016	Published	ISO/IEC						X			X	X	X		X	X		X			X		X		European Standard
Other available standards	Information technology - Security techniques - Specification for digital redaction (ISO/IEC 27038:2014)	EN ISO/IEC 27038	CEN and CENELEC	2016	Published	ISO/IEC						X			X	X	X		X	X		X			X		X		European Standard

STANDARDISATION							REGULATION																																
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status	1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Other available standards	Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)	EN ISO/IEC 27041	CEN and CENELEC	2016	Published	ISO/IEC						x			x	x	x		x	x		x			x		x		European Standard
Other available standards	Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015)	EN ISO/IEC 27042	CEN and CENELEC	2016	Published	ISO/IEC						x			x	x	x		x	x		x			x		x		European Standard
Other available standards	Information technology - Security techniques - Incident investigation principles and processes (ISO/IEC 27043:2015)	EN ISO/IEC 27043	CEN and CENELEC	2016	Published	ISO/IEC						x			x	x	x		x	x		x			x		x		European Standard
Other available standards	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	EN IEC 62443-4-1:2018	CENELEC	2018	Published	IEC						x			x	x	x					x			x		x		European Standard
Other available standards	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	FprEN IEC 62443-4-2	CENELEC	2019	Published	IEC						x				x	x					x			x		x		European Standard
Other available standards	Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design	prEN 62443-3-2	CENELEC	2020	Published	IEC						x				x	x					x			x		x		European Standard
Other available standards	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	prEN IEC 62443-3-3	CENELEC	2014	Published	IEC						x				x	x					x			x		x		European Standard
Other available standards	Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers	prEN 62443-2-4	CENELEC	2017	Published	IEC						x			x	x	x					x			x		x		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 1: Terminology and basic concepts	EN 61069-1	CENELEC	2016	Published	IEC					x																		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 2: Assessment methodology	EN 61069-2	CENELEC	2016	Published	IEC									x	x									x		x		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 3: Assessment of system functionality	EN 61069-3	CENELEC	2016	Published	IEC									x	x									x		x		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 4: Assessment of system performance	EN 61069-4	CENELEC	2016	Published	IEC									x	x									x		x		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 5: Assessment of system dependability	EN 61069-5	CENELEC	2016	Published	IEC									x	x									x		x		European Standard

	STANDARDISATION						REGULATION																											
											1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status																								
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 6: Assessment of system operability	EN 61069-6	CENELEC	2016	Published	IEC									X	X									X		X		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 7: Assessment of system safety	EN 61069-7	CENELEC	2016	Published	IEC									X	X									X		X		European Standard
Other available standards	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 8: Assessment of other system properties	EN 61069-8	CENELEC	2016	Published	IEC									X	X									X		X		European Standard
Other available standards	Global Cyber Security Ecosystem	Doc. Nb. TR 103 306 Ver. 1.3.1	ETSI /TC CYBER	2018	Published						X																				
Other available standards	Privacy; introductory guide	TR 103 370	ETSI /TC CYBER	2019	Published								X																		
Other available standards	Privacy; Attribute-based encryption for Attribute Based Access Control	TS 103 532	ETSI /TC CYBER	2018	Published								X				X														
Other available standards	Privacy; Attribute-based encryption for data protection on smart devices, cloud and mobile services	TS 103 458	ETSI /TC CYBER	2018	Published								X				X														
Other available standards	Privacy; Mechanisms for privacy assurance and verification	Doc. Nb. TS 103 485	ETSI /TC CYBER	2019	Ongoing								X																		
Other available standards	Privacy; Identity management and naming schema protection mechanisms	Doc. Nb. TS 103 486	ETSI /TC CYBER	2019	Ongoing								X																		
Other available standards	Protection measures for ICT in the context of Critical Infrastructure	Doc. Nb. TR 103 303 Ver. 1.1.1	ETSI /TC CYBER	2016	Published																						X				
Other available standards	Critical Infrastructure; ICT Metrics for Identification of CI	Ref. DTR/CYBER-0024	ETSI /TC CYBER	2020	Ongoing																						X				
Other available standards	Critical Security Controls for Effective Cyber Defence;	Doc. Nb. TR 103 305-1 Ver. 3.1.1	ETSI /TC CYBER	2018	Published																						X				
Other available standards	Critical Security Controls for Effective Cyber Defence;	**Doc. Nb. TR 103 305-2 Ver. 4.1.2**	ETSI /TC CYBER	2022	Published																						X				
Other available standards	Critical Security Controls for Effective Cyber Defence;	Doc. Nb. TR 103 305-3 Ver. 2.1.1	ETSI /TC CYBER	2018	Published																						X				
Other available standards	Critical Security Controls for Effective Cyber Defence;	Doc. Nb. TR 103 305-4 Ver. 2.1.1	ETSI /TC CYBER	2018	Published																						X				
Other available standards	Critical Security Controls for Effective Cyber Defence;	TR 103 305-5	ETSI /TC CYBER	2018	Published																						X				

	STANDARDISATION						REGULATION																																
												1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status																													
Other available standards	Secure by Default - platform security technology	Doc. Nb. TR 103 309 Ver. 1.1.1	ETSI /TC CYBER	2015	Published																		X	X												
Other available standards	Structured threat information sharing	Doc. Nb. TR 103 331 Ver. 1.1.1	ETSI /TC CYBER	2016	Published																													X	
Other available standards	Design requirements ecosystem	Doc. Nb. TR 103 369 Ver. 1.1.1	ETSI /TC CYBER	2016	Published																			X											
Other available standards	Network Gateway Cyber Defence	Doc. Nb. TR 103 421 Ver. 1.1.1	ETSI /TC CYBER	2017	Published																		X												
Other available standards	Middlebox Security Protocol	TS 103 523-1	ETSI /TC CYBER	2019	Ongoing													X																	
Other available standards	Middlebox Security Protocol	Doc. Nb. TS 103 523-2	ETSI /TC CYBER	2019	Ongoing													X																	
Other available standards	Middlebox Security Protocol	TS 103 523-3	ETSI /TC CYBER	2018	Published													X																	
Other available standards	Implementation of the Network and Information Security (NIS) Directive	Doc. Nb. TR 103 456 Ver. 1.1.1	ETSI /TC CYBER	2017	Published											X														X		X		X	
Other available standards	Quantum Computing Impact on security of ICT Systems;	Doc. Nb. EG 203 310 Ver. 1.1.1	ETSI /TC CYBER	2016	Published																										X				
Other available standards	Quantum-Safe Cryptography	All published work	ETSI /TC CYBER	2018	Published										X									X											
Other available standards	Quantum-Safe Cryptography	ongoing work	ETSI /TC CYBER	2019	Ongoing										X									X											
Other available standards	Methods and protocols; Threat, Vulnerability, Risk Analysis	Doc. Nb. TS 102 165-1 Ver. 5.2.3	ETSI /TC CYBER	2017	Published											X								X											
Other available standards	Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures	Doc. Nb. TS 102 165-2	ETSI /TC CYBER	2019	Ongoing																			X					X						
Other available standards	Specifying a common interface to transfer sensitive functions to a trusted domain.	Doc. Nb. TS 103 457	ETSI /TC CYBER	2018	Published													X													X				
Other available standards	Security techniques for protecting software in a white box model	TR 103 642	ETSI /TC CYBER	2018	Published																			X											
Other available standards	Cyber Security for Consumer Internet of Things	TS 103 645	ETSI /TC CYBER	2019	Published																			X											
Other available standards	Techniques for assurance of digital material used in legal proceedings.	TS 103 643	ETSI /TC CYBER	2019	Ongoing								X							X															
Other available standards	Cryptography: Guide to Identity Based Encryption	DTR/CYBER-0045	ETSI /TC CYBER	2020	Ongoing													X						X											

	STANDARDISATION						REGULATION																												
												1. Cybersecurity Terminology	2. Trustworthiness	3. Privacy	4. Oversight	5. Risk assessment	6. Cyber resilience requirements	7. Transorganisational security requirements and interfaces	8. Civil-military interoperability, secure data exchange	9. Supply chain cyber security	10. Maintenance (MRO) Security	11. Cloud security	12. Development & Production Process Security	13. Product security	14. Cyber security verification	15. Risk and vulnerability management	16. Operation security	17. Security Incident, Event Management, Incidence Response and Recovery Management	18. Information sharing	Comment
Domain	Standardisation activity	Reference	Standardisation organisation	Target date for standard publication	Status	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status																									
Other available standards	Information Security Indicators	All published work	ETSI/ISG ISI	2019	Published																							X	X				
Other available standards	Digital signatures: creation and validation (formats, procedures, sign policies)	All published work	ETSI/TC ESI	2019	Published												X		X			X										
Other available standards	Digital signatures: formats conformance checkers (free access)	Sign format conformance checkers	ETSI/TC ESI	NA	Published																	X										
Other available standards	Digital signatures; Trust Service Providers Supporting Digital Signatures (audit req, conformity assessment, protocols for remote signature creation and validation)	All published work	ETSI/TC ESI	2019	Published												X															
Other available standards	Digital signatures: Cryptographic suites	TS 119 312	ETSI/TC ESI	2019	Published												X						X									
Other available standards	Digital Signatures: registered eDelivery services	All published work	ETSI/TC ESI	2019	Published												X															
Other available standards	Digital Signatures: registered electronic mail services	All published work	ETSI/TC ESI	2019	Published												X															
Other available standards	Digital Signatures: ongoing work (formats, preservation…)	ongoing work	ETSI/TC ESI	TBC	Ongoing												X															
Other available standards	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations	ISO/IEC 20243-1	ISO/IEC	2018	Published								X							X												
Other available standards	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018	ISO/IEC 20243-2	ISO/IEC	2018	Published	IEC							X							X												
Other available standards	Information technology — Security techniques —Vulnerability disclosure	ISO/IEC 29147	ISO/IEC	2014	Published	IEC																					X				ED-206 ISEM is intended to include vulnerability disclosure programme guidance. ED-206 ISEM is intended to provide aviation-specific VDP guidance and this ISO standards provides good interum guidance.
Other available standards	Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security	ISO/IEC 27036-3	ISO/IEC	2013	Published	IEC														X												
	UAS																																		
UAS																																		See U-RDP at EUSCG.EU

DOMAIN AND CATEGORY SCOPES

Scope of Domain	To facilitate access to the relevant documents, the standards and regulations have been divided into mutually exclusive domains. Domains are common user group or base for standards that has similar lifecycle and environment; these are loosely aligned with organisational approvals. These domains are: 'Aerodrome', 'Aircraft', 'ATM/ANS', 'Transversal' (i.e. across aviation) and Other available standards (i.e. non-aviation). 'Air Operators' may become a future domain once its scope is defined and potentially relevant documents are proposed.
Scope of Category	To facilitate access as well as the identification of gaps, the standards and regulations are associated with one or more categories. These categories are used to identify topics addressed by the standards and regulations. This categorisation is also used to identify common topics where security standardisation is needed.
Information Security scope in the RDP	In this context and with view to use a scope as broad as possible: • "The practice of defending information from unauthorised access, use, disclose, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)" (ER-013). • Information security includes here information technology, operational technology and embedded systems. • Information security here also includes the impact on safety, security and continuity of civil aviation.

DOMAINS

Domain	Agreed scope
Aerodrome	A defined area on land or in water (including buildings, installations and equipment) intended to be used either wholly or in part for the arrival, departure and movement of aircraft (ICAO). The domain includes all documents that provide requirements, specifications, guidelines or characteristics related to the design, construction and operation.
Aircraft	An aircraft is any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface (ICAO). The domain includes all documents that provide requirements, specifications, guidelines or characteristics related to the design, production and MRO.
ATM/ANS	**Air traffic management** is an aviation term encompassing all systems that assist aircraft to depart from an aerodrome, transit airspace, and land at a destination aerodrome, including Air Traffic Services (ATS), Airspace Management (ASM), and Air Traffic Flow and Capacity Management (ATFCM). **Air Navigation Services** is a term that includes air traffic management (ATM), communications, navigation and surveillance systems (CNS), meteorological services for air navigation (MET), search and rescue (SAR) and aeronautical information services (AIS). These services are provided to air traffic during all phases of operations (approach, aerodrome and en-route). The domain includes both ATM and ANS as defined above and comprises all documents that provide requirements, specifications, guidelines or characteristics to ensure that materials, products, processes and services are fit developed for all systems that assist aircraft to depart from an aerodrome, transit airspace, and land at a destination aerodrome.
Transversal	The domain includes all documents that could have a horizontal and/or vertical effect on specifications, guidelines or characteristics across two or more domains.
Other available standards	The domain includes all non-aviation standards that may be relevant to one or more domains and provided for information only. Where gaps in the categories exist for a particular domain, the available standards can be used directly, if appropriate, otherwise they can be modified with a supplement or used as a template for creating aviation standards.
Future domain	
Air Operators	*Scope to be characterised in a second stage, with the proposition of related regulatory and standardisation documents.*

CATEGORIES

Category	Scope agreed
1. Cybersecurity Terminology	Terminology either defined by standards being developed or already existing. Common recognition of definitions either used in or relevant to the field of cybersecurity or information security as used in the relevant domain.
2. Trustworthiness	The ability to be relied on as honest or truthful and to handle with best intent. In technology this refers to the application of appropriate procedures, processes and standards which allows it to be perceived as reliable by a human or another technical system. For example, and without limitation: Standards that establish trust in personnel and organisations such that credit can be taken for certification purposes, includes both technical means such as encryption and digital signatures, operational means such as policies, procedures and contracts, as well as external agreements.
3. Privacy	Set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems (ISO/IEC 29100) For example, and without limitation: Standards related to particular security aspects related to privacy
4. Oversight	Standards providing the means of consistently ensuring oversight in an economically viable manner including certification (by authorities and/or trusted third parties), auditing and inspection (by contracting organisation or trusted third party)
5. Risk assessment	Overall process comprising a risk analysis and a risk evaluation (ISO/IEC Guide 73). For example, and without limitation: procedure for identifying all threat conditions, ranking of threat conditions, harmonising severity of threat conditions, use of threat catalogues, use of likelihood or probability, use and harmonisation of attacker profiles.
6. Cyber resilience requirements	**Cyber resilience** refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. Refers to procedures, processes and standards an organisation, stakeholder or system must fulfil for cyber resilience assurance. For example, and without limitation: providing best practices for hardening parts and services

7. Transorganisational security requirements and interfaces	Refers to the set of procedures, processes and standards designed to provide information security assurance affecting the organisations which are part of the aviation functional chain thus, are required to exercise a level of risk management that results in (acceptable) levels of risks which are acceptable for other organisations.
8. Civil-military interoperability, secure data exchange	Standards relating to particular needs of civil-military interfaces
9. Supply chain cyber security	It refers to the set of procedures, processes and standards designed to provide information security assurance for organisations acting as suppliers for research, design, development, production, maintenance, repair, overhaul, operations and decommission of assets For example, and without limitation: documents related to securing risks to supply chain - either internal manufacturing or outsourced suppliers of software and hardware taking into consideration the relationship between the contracting organisations.
10. Maintenance (MRO) Security	MRO Security refers to the set of procedures, processes and standards designed to provide information security assurance across organisations involved in aviation maintenance, repair and overhaul thus, including relevant supply chain organisations.
11. Cloud security	Cloud computing security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment with the objective of preserving the confidentiality, integrity and availability of information. Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered (public, private or hybrid delivery model). For example, and without limitation: documents that establish the best practices and requirements when using cloud technologies in aviation.
12. Development & Production Security	Development & Production Security refers to the set of procedures, processes and standards designed to provide information security assurance across organisations involved in the design, development and production of assets for aviation thus, including relevant supply chain organisations. For example, and without limitation: specific enterprise needs for development of certified parts and securing of Operational Technology used to produce aviation parts.

13. Product security	*Product security* refers to the set of procedures, processes and standards designed to provide information security assurance of a product or asset through documents providing requirements, specifications, guidelines fit developed for application security, infrastructure security, and incident response. For example, documents that establish the best practices and requirements for aviation products.
14. Cyber security verification	**Cyber security verification** is intended to check that a product, service, or system (or portion thereof, or set thereof) intended to ensure cyber security meets a set of (design) specifications. For example, and without limitation: Standards providing the processes for performing various forms of security testing to uncover vulnerabilities and assess security architecture and implementation of security requirements as well as the means for assessing the quality and coverage of testing performed.
15. Risk and vulnerability management	Risk management is the identification, evaluation, and prioritisation of risks followed by coordinated and economical application of resources to minimise, monitor, and control the probability or impact of unfortunate events or to maximise the realisation of opportunities. **Vulnerability Management:** Vulnerability management is a security practice specifically designed to proactively mitigate or prevent the exploitation of IT vulnerabilities which exist in a system or organization. The process involves the identification, classification, remedy, and mitigation of various vulnerabilities within a system. It is an integral part of computer and network security and is practiced together with risk management as well as other security practices. For example, and without limitation: continuously identifying vulnerabilities throughout lifecycle through automated means, private or public vulnerability disclosures, testing and ranking or scoring of vulnerabilities to identify and harmonise vulnerabilities posing risks that need to be remediated immediately, can be deferred or accepted
16. Operation security	It refers to the set of procedures, processes and standards designed to provide information security assurance across an organisation's operations. For example, and without limitation: documents providing means of consistently applying operational security controls for which credit can be taken

17. Security Incident, Event Management Incidence Response and Recovery Management	'Information security event' means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of security controls, or a previously unknown situation that can be security relevant; "information security incident' means a single or a series of unwanted or unexpected information security events which could potentially affect aviation safety," security and continuity of civil aviation. Documents providing requirements, specifications, guidelines developed for the process of identifying, monitoring, recording and analysing security events or incidents as defined above. **Incident response** is the methodology an organization uses to respond to and manage an Information Security Incident. An incident response aims to reduce this damage and recover as quickly as possible. **Recovery Management** involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Recovery management focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery can therefore be considered as a subset of business continuity. For example, and without limitation: cleaning of malware, forensics.
18. Information sharing	Information sharing describes the exchange of data between various organizations, people and technologies through documents providing requirements, specifications, guidelines related to the act of passing information, electronically or through other systems. For example, and without limitation: setting the framework for establishing the trust necessary to share sensitive security information