Appendix II — Main tasks stemming from the implementation of Part-IS, including mapping to NIST CSF 1.1 competencies and ISO/IEC 27001 clauses and controls

ED Decision 2023/010/R

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Establish and operate an information security management system (ISMS)	Management	IS.AR.200(a)	IDENTIFY	ID.RM	4 6.1.1		
Establish the scope of the ISMS according to Part-IS requirements	Management	IS.AR.205(a)	IDENTIFY	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implement and maintain an information security policy	Management	IS.AR.200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1	A5.1
Identify and review information security risks	Management	IS.AR.200(a)(2) IS.AR.205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implement security risk treatment measures	Management	IS.AR.200(a)(3) IS.AR.210	PROTECT	PR.PT	6.1.3 8.1 8.3		
Implement measures to detect information security events and identify those related to aviation safety	Management	IS.AR.200(a)(4) IS.AR.215	DETECT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7	A7.2 A8.15 A5.28
Monitor compliance with this Regulation and report findings to top management	Operational	IS.AR.200(a)(8)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Protect confidentiality of exchanged information	Operational	IS.AR.200(a)(9)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
Communicate to the Agency changes regarding capability and responsibilities	Operational	IS.AR.200(a)(10)				A6.1.3	A5.5
Share information to assist other competent authorities, agencies and organisations	Operational	IS.AR.200(a)(11)	IDENTIFY	ID.RA-2 ID.BE-2		A6.1.4	A5.6
			PROTECT	PR.IP-8			
			RESPOND	RS.CO-3 RS.CO-5			
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.AR.200(b) IS.AR.235	IDENTIFY	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1	A5.1 A5.28 A5.29 A5.35
			PROTECT	PR.IP-7 PR.IP-10			
			DETECT	DE.DP-5			
			RESPOND	RS.MI-3 RS.IM-2			
			RECOVER	RC.IM-2			
Document and maintain all key processes, procedures, roles and responsibilities	Management	IS.AR.200(c)	IDENTIFY	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1	A5.1 A5.2
			PROTECT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12			
			DETECT	DE.DP-1			
			RESPOND	RS.CO-1 RS.AN-5			
Identify all elements which could be exposed to information security risks	Management	IS.AR.205(a)	IDENTIFY	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	A8.1.1	A5.9
Identify the interfaces with other organisations which could result	Management	IS.AR.205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
in exposure to information security risks							
Identify information security risks and assign a risk level	Management	IS.AR.205(c)	IDENTIFY	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2		
Review and update the risk assessment based on certain criteria	Operational	IS.AR.205(d)	IDENTIFY	ID.RM	8.2		A5.7
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.AR.210(a)	PROTECT	PR.IP PR.PT	6.1.3 8.3		
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.AR.210(b)	IDENTIFY	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1		
			PROTECT	PR.IP-7			
			DETECT	DE.AE-2 DE.AE-3 DE.AE-5			
Implement measures to detect in processes and operations information security events which may have a potential impact on aviation safety	Operational	IS.AR.215(a)	DETECT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5	A7.2 A8.8 A8.15 A8.16 A5.24 A5.25 A5.26 A6.8
			PROTECT	PR.PT-1			
Implement measures to respond to information security events that	Operational	IS.AR.215(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5	A5.26

Part-IS main task	Activity type	Reference					
	Management, Operational	**Part-IS**	**NIST CSF Version 1.1**		**ISO/IEC 27001**		
			Function	**Category**	**Paragraph Clause**	**Annex A Control**	
						:2013	**:2022**
may cause a security incident			🟥				
Implement measures to recover from information security incidents	Operational	IS.AR.215(c)	RECOVER	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6	A5.26 A5.27
Manage risks associated with contracted activities with regard to the management of information security	Management	IS.AR.220	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Define a person with the authority to establish and maintain the organisational structures, policies, processes, and procedures necessary to implement this Regulation	Management	IS.AR.225(a)	IDENTIFY	ID.AM-6	7.1	A6.1.1	A5.2
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.AR.225(b)	IDENTIFY	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding	Management	IS.AR.225(c)	IDENTIFY PROTECT	ID.AM-5 ID.AM-6 PR.AT-1	7.2	A7.2.2	A6.3

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
information security management							
Create and maintain a process to ensure that the personnel acknowledge the responsibilities associated with the assigned roles and tasks	Management	IS.AR.225(d)	IDENTIFY	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2
Verify the identity and trustworthiness of personnel who have access to information systems	Management	IS.AR.225(e)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
Archive, protect and retain records traceability for a specified time	Operational	IS.AR.230	IDENTIFY	ID.RA-4	7.5	A8.2.2 A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3	A5.10 A5.13 A7.3 A7.5 A8.6 A8.10 A8.13 A8.15
			PROTECT	PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1			
			RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5			
			RECOVER	RC.CO-3			
Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.AR.235(a)			9	A5.1.2 A12.7.1 A16.1.6	A5.1 A5.27 A8.34
Take actions to improve the ISMS if required. Reassess	Operational	IS.AR.235(b)			10	A5.1.2	A5.1

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control	
						:2013	:2022
the implemented measures of the ISMS elements.							