ENISA implementation guidance on Commission Regulation (EU) 2024/2690 of 17.10.2024

Comment No.	Reviewer name	Line number	Document Page	Section	Comment	Proposed change
1	ECSO	161	6	Introduction	“This is mandatory and must be implemented in its entirety by the relevant entities.” In reference to the Implementing Act paragraphs (5) principle of proportionality and (6) Certain technical and methodological requirements set out in the Annex to this Regulation should be applied by the relevant entities where appropriate, where applicable, or to the extent feasible.	The sentence must be revised to reflect the language of the Implementing Act.
2	ECSO	205	8	Topic Specific Policies	“In addition to this overarching corporate policy the following topic-specific, documented policies are required:” There should not be an enforcement for entities to define requirements in documents called “policy” or that there should be a specific document for those requirements.	There should be a clarifying comment that the requirement is to define certain requirements in mandatory/binding documentation.
2	ECSO	224	9	1.1.1	No definition of security objectives in the proposal, should be added.	
3	ECSO	265	10	1.1.2	Risk analysis should be enumerated, maybe first	
4	ECSO	274	10	1.1.2	Risk analysis should be enumerated, maybe first	
5	ECSO	320	11	1.1.2	No definition of security objectives in the proposal, should be added.	
6	ECSO	335	12	1.2	The section on roles, responsibilities, and authorities is comprehensive but could include a clear example of how an organizational chart might be structured to segregate conflicting duties.	Provide a sample template for documenting security roles and responsibilities to standardize implementation across different organizations or an example of an RACI chart.
7	ECSO	345 - 346	12	1.2	We welcome the reference to the ECSF in the context of defining roles, responsabilities and authorities within entities. The European Cybersecurity Skills Framework (ECSF) is a very valuable tool to support a the identification of and articulation of skills, competences, tasks and knowledge linked to cybersecurity professionals, fostering a common EU-wide understanding and helping firms fill critical skills gaps.	
8	ECSO	442	15	2.1	Section covers risk treatment and residual risk. Should include gross risk, risk after existing security measures, residual risk and difference to risk appetite, approval of risk appetite, mechanism for provisioning of resources for approved risk treatment plans (to reduce residual risk below risk appetite). Also, should include risk metrics.	
9		773	26	3	The guidance on incident handling lacks comprehensive protocols for developing and implementing effective incident response strategies. Clear steps for incident detection, containment, eradication, recovery, and lessons learned should be outlined, along with defined roles and responsibilities during an incident. This would help organizations better prepare for and respond to cybersecurity incidents.	
10	ECSO	774	26	3.1	The guidance on incident categorization could specify examples of severity levels and their corresponding responses.	Provide a decision tree or flowchart for incident handling to clarify the escalation process.
11	ECSO	1084	34	3.3.1	Usually a security event is lower than a security incident, the definition here points to a security incident and the difference can create confusion about what needs to be reported. Maybe a clarification that security event is used equivalent to security incident is useful.	
12	ECSO	1531	48	4.2	Provisions for cloud operations should be considered by employing replication in availability zones, backup saved in other availability zones, encryption etc.	
13	ECSO	1743	54	4.3.3	As recongised in the guidance it is critical to ensure that the point of contact with the CSIRT possess adequate knowledge with regards to incidents and threat intelligence. In section 2.3.1 line 693, the guidance rightly presents the possession of relevant professional certifications as a relevant indicator of the competences of independent auditors and gives concrete examples of widely used, state-of-the-art certifications in the field. The standard expectations should be the same for all those who have a sensitive role that required a specific, skilled profile (whether internal or external, whether auditors or threat intelligence specialists or other roles) - this also has a basis in the NIS2 legal text. For this reason, examples of evidences in this regard should include relevant professional certifications (with concrete examples in this case as well) for this role.	Add "evidences of that the point of contact has sufficient knowledge concerning incidents and threat intelligence. This can include for example professional certifications like CRISC, ISSMP, CSX-P".
14	ECSO	1811	57	5.1	Provide specific examples of risks and mitigation strategies for supply chain vulnerabilities, such as third-party software dependencies or hardware procurement risks.	e.g. Unpatched Vulnerabilities - Vulnerability Scanning:/ Code Review and Testing - Vendor Assurance Programs.
15	ECSO	3227 - 3228	99 - 100	8.1.2	We are pleased with the Cybersecurity Skills Academy being referenced as a source to consult when implementing the awareness raising program. The academy is a crucial initiative to foster cybersecuirty training in the EU and it is important to increase its visibility and expand on it (as is in line with ENISA's priorities).	
16	ECSO	3262 - 3263	101	8.2	Welcomes the reference to the ECSF also in the context of planning security training for employees.	
17	ECSO	3538	109	10.1	We welcome that the technical guidance calls on firms to put in place processes and best practices to ensure human resource security. This is also in line with the NIS2 text in its broader goal of fostering the monitoring of entities' maturity level and network and information security. This is crucial to ensure state-of-the art cybersecurity. For this reason, the use of relevant frameworks or models to integrate cybersecurity best practices in a given firm should be listed alongside other relevant metrics such as training material and mechanisms for hiring hired professionals . To better guide firms, concrete examples of models should be given as well as exaples of relevant evidence (as concrete examples of professional certifications have been given elsewhere in the guidance)	Add "use of cybersecurity frameworks, quality management and maturity models e.g. CMMI, NIST, ISO 9001"
18	ECSO	3728	116	11	Device attestation for conditional access should be added to increase security.	