Vulnerability & Patch Management Deep Dive - V1.0

ID	Requirements	Reference
VulPat_01	Continuously assess cyber threats and ICT vulnerabilities relevant to ICT-supported business functions, information assets, and ICT assets.	DORA
VulPat_02	As part of the ICT risk management framework, financial entities shall have comprehensive documented policies for patches and updates.	
VulPat_03	Maintain capabilities and staff to gather information on vulnerabilities and cyber threats and analyze their potential impact on digital operational resilience.	
VulPat_04	Implement crisis communication plans to ensure responsible disclosure of major vulnerabilities to clients, counterparts, and, when appropriate, the public.	
VulPat_05	Include vulnerability assessments and scans in the digital operational resilience testing program.	
VulPat_06	Central securities depositories and central counterparties shall perform vulnerability assessments before the deployment or redeployment of applications, infrastructure components, or ICT services supporting critical or important functions.	
VulPat_07	Develop, document, and implement a vulnerability management procedure as part of the ICT security procedures.	RTS risk management
The vulnerability management procedure shall include provisions		
VulPat_08	to identify and update reliable information sources to maintain awareness of vulnerabilities.	
VulPat_09	for performing automated vulnerability scanning and assessments on ICT assets, with frequency and scope based on asset classification and the overall risk profile of the ICT asset, and at least weekly for assets supporting critical or important functions.	
VulPat_10	to verify that ICT third-party service providers manage vulnerabilities in their services, report critical vulnerabilities and trends promptly, and investigate, determine root causes, and apply appropriate mitigating actions.	
VulPat_11	to track the usage of third-party and open-source libraries employed by ICT services supporting critical or important functions, and to collaborate with the ICT third-party provider to monitor and manage their versions and updates.	
VulPat_12	to track the usage of ICT services developed by the financial entity itself or specifically customized or developed by an ICT 3P-provider.	
VulPat_13	to track the usage of third-party and open-source libraries, to the extent possible, for acquired off-the-shelf ICT assets, such as hardware, operating systems, and standard software, used for non-critical or non-important ICT services."	
VulPat_14	for the responsible disclosure of vulnerabilities to clients, counterparties, and the public.	
VulPat_15	provisions to prioritize the deployment of patches and mitigation measures to address identified vulnerabilities, considering their criticality, asset classification, and the risk profile of the affected ICT assets.	
VulPat_16	provisions to monitor and verify the remediation of vulnerabilities.	
VulPat_17	requirements to record any detected vulnerabilities and to monitor their resolution.	
VulPat_18	Develop, document, and implement a patch management procedure as part of the ICT security procedures.	
The patch management procedures shall include provisions		
VulPat_19	to identify and evaluate available software and hardware patches and updates using automated tools.	
VulPat_20	for emergency procedures for patching and updating ICT assets.	
VulPat_21	to test and deploy patches, ensuring compliance with requirements for separating production from development and testing environments and obtaining approvals for exceptions as needed.	
VulPat_22	related to deadlines for installing software and hardware patches and updates, as well as escalation procedures for missed deadlines.	