ESMA_QA_2103

Submission Date
11/02/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Subject Matter
EUC, EULA and Shadow IT

Question
For complying with the regulatory provisions envisaged by the DORA Regulation, Financial Entities should consider End User Computing (EUC) tools, End User License Agreements (EULA), and the conditions of Shadow IT.
Would it be possible to obtain the regulatory references for these areas?

ESMA Answer

11-02-2024

Original language

According to the broad definition of ICT asset under Article 3(7) of DORA, EUC tools are considered ICT assets since they are software or hardware used in the network and information systems of the financial entity. The same apply for the software governed by the EULA and the ICT systems developed and managed by users outside the ICT function (shadow IT). Therefore, all management, security, and risk assessment provisions of DORA related to ICT assets should apply to EUC tools, software governed by EULAs and Shadow IT. This includes identifying, documenting, and managing these assets to mitigate any associated risks.

In addition, According to Article 11, Paragraph (2), point (c) of the Commission Delegated Regulation (CDR) (EU) 2024/1774 (RTS on RMF), a financial entity should identify the security measures to ensure that only authorised software is installed in ICT systems and endpoint devices. This means that all ICT systems implemented need to be authorised; the financial entity should implement all necessary technical and organizational measures to this effect.

Also, Article 16, Paragraph (9) of the RTS on RMF emphasizes that procedures related to ICT systems' acquisition, development, and maintenance must also apply to ICT systems developed or managed by users outside the official ICT function, using a risk-based approach. Under DORA, all ICT assets must be identified, documented, and managed to ensure they meet the entity's ICT risk management requirements. This means financial entities must ensure that their ICT risk management and control processes cover the ICT systems developed and managed by users outside the ICT function and EUC practices, ensuring all software and hardware is implemented in an authorised way and is securely integrated and operated within the organization's ICT infrastructure The risks that such a practice can pose should be also appropriately identified and managed, as per the Article 6 and Article 8 Paragraph (2) of DORA respectively.

Regarding the EULA, if an EULA is a contractual agreement between a third-party service provider, as defined by Article 3(19) of DORA and the financial entity, and the software governed by this EULA is installed on an ICT asset of the financial entity or used to support business functions of the financial entity, then all provisions of Regulation (EU) 2022/2554 regarding ICT risk management, including third-party risk management, apply. This scenario includes the use of authorised software governed by the EULA even if the terms of the EULA are accepted by the employee of the financial entity on behalf of the financial entity.

We understand there could be cases where the EULAs is not subject to specific third-party risk management provisions as above. Nevertheless, they would be anyway subject to the ICT risk management requirements, because the software provided under these agreements is often customised and maintained internally by the financial entity or involves minimal interaction with external service providers. The emphasis is on managing ICT risks directly related to the software's use and all the relevant DORA provisions should apply.