EBA/GL/2019/04
(consolidated version)

19 May 2026

O

EBA Guidelines on ICT and security risk management

Guidelines on ICT and security risk management		Application date
➢ O		30.06.2020
➢ Amended by:		
➢ A1	EBA/GL/2025/02	20.05.2025
	EBA/GL/2019/04 (consolidated version)	19.05.2026

Compliance and reporting obligations

Status of these guidelines

O

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010 [1]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how European Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 and to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

A1

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by 20.05.2025. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/2025/02'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

O

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

Subject matter, scope and definitions

Subject matter

A1

5. These guidelines are based on the mandate to issue guidelines under Article 95(3) of Directive (EU) 2015/2366 and cover aspects of payment user relationship management.

6. These guidelines complement the risk management measures under Digital Operational Resilience Act (DORA) and the related Regulatory Technical Standards that payment service providers referred to in paragraph 5 above must take, in accordance with Article 95(1) of PSD2, to manage the operational and security risks relating to the payment services they provide.

Scope of application

A1

7. These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that payment service providers must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide.

Addressees

A1

8. These guidelines are addressed to competent authorities as defined in Article 4 point (2) point (vii) of Regulation (EU) No 1093/2010 and to financial institutions as defined in Article 4(1) of Regulation No 1093/2010, which are payment service providers as defined in Article 1(1) point (a), point (b) and point (d) of Directive (EU) 2015/2366, including natural or legal persons benefiting from an exemption pursuant to Article 32 or 33 of Directive (EU) 2015/2366 and legal persons exempted under Article 9 of Directive 2009/110/EC.

Definitions

[Deleted]

Implementation

Date of application

⮛A1

9. These guidelines apply from the latest by 20.05.2025.

Repeal

⮛A1

[deleted]

Guidelines on ICT and security risk management

3.1. Proportionality

⮟A1

[deleted]

3.2. Governance and strategy

⮟A1

[deleted]

3.3. ICT and security risk management framework

⮟A1

[deleted]

3.4. Information security

⮟A1

[deleted]

3.5. ICT operations management

⮟A1

[deleted]

3.6. ICT project and change management

⮟A1

[deleted]

3.7. Business continuity management

⮟A1

[deleted]

3.8. Payment service user relationship management

GO

92. Payment service providers should establish and implement processes to enhance payment service users' awareness of the security risks linked to the payment services by providing payment service users with assistance and guidance.

93. The assistance and guidance offered to payment service users should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the payment service user.

94. Where product functionality permits, payment service providers should allow payment service users to disable specific payment functionalities related to the payment services offered by the payment service provider to the payment service user.

95. Where, in accordance with Article 68(1) of Directive (EU) 2015/2366, a payment service provider has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the payment service provider should provide the payer with the option to adjust these limits up to the maximum agreed limit.

96. Payment service providers should provide payment service users with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.

97. Payment service providers should keep payment service users informed about updates in security procedures that affect payment service users regarding the provision of payment services.

98. Payment service providers should provide payment service users with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. Payment service users should be appropriately informed about how such assistance can be obtained.