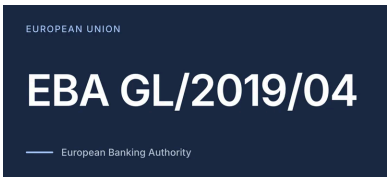
SmartSuite

Framework / Cybersecurity / Other

EBA/GL/2019/04

EBA/GL/2019/04 set ICT and security risk expectations for banks and payment firms; since May 20, 2025 only Guideline 3.8 on payment user relationships remains, and DORA covers the rest.



What it is

EBA/GL/2019/04, the European Banking Authority's Guidelines on ICT and security risk management, was written in 2019 to set out how credit institutions, investment firms and payment service providers manage ICT and security risk, but since May 20, 2025 only its Guideline 3.8 on payment service user relationship management remains in force; the rest was deleted by EBA/GL/2025/02 because DORA now covers it. The Guidelines applied from June 30, 2020 and replaced the 2017 guidelines on security measures under PSD2 (EBA/GL/2017/17).

At a glance

PUBLISHER
European Banking Authority (EBA)

TYPE
Guidance

VERSION
EBA/GL/2019/04, as amended by EBA/GL/2025/02 (applies from May 20, 2025)

EFFECTIVE
June 30, 2020 (original); amendments from May 20, 2025

DOMAIN
Cybersecurity

FAMILY
Other

REGION
European Union

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management

Why it matters

- **A clear status** As of May 20, 2025 paragraphs 1 to 91 (sections 3.1 to 3.7) are deleted and Guideline 3.8 is the part that remains.
- **DORA replaced the ICT risk content** The EBA found that DORA and its technical standards cover the ICT risk management, incident, testing and third-party content, so it narrowed the Guidelines instead of keeping a parallel set.
- **User-facing security still applies** Paragraphs 92 to 98 ask payment service providers to give users guidance, control over functionalities, spending limit options, alerts and support.
- **Useful history for mapping** The original structure, from governance to business continuity, still shows what supervisors expected before DORA and helps when mapping old controls.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports EBA GL/2019/04

Guideline 3.8 Requirement Register

Track paragraphs 92 to 98 for each payment service with owner, status and evidence.

User Guidance and Awareness

Keep the security guidance given to users and the dates it was updated for new threats (paragraphs 92 and 93).

Function and Limit Controls

Record the user options to disable functions and to adjust spending limits (paragraphs 94 and 95).

Alerts and Notices

Track alert settings, failed attempt notices and security procedure update messages (paragraphs 96 and 97).

Support and Anomaly Handling

Log support requests on security matters and response times (paragraph 98).

Legacy Control Mapping

Map controls originally built on sections 3.1 to 3.7 to the DORA requirements that now apply, with the retirement date.

Common framework mappings

CIS Controls v8.1 | EU DORA | GDPR | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SWIFT CSCF

Official resources

EBA Guidelines on ICT and Security Risk Management

Describes requirements for managing ICT and security risks in financial institutions.

eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

EBA Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/05)

How competent authorities assess ICT risk within the supervisory review and evaluation process.

eba.europa.eu/sites/default/files/documents/10180/1954038/0d11223d-d682-4bd9-bb82-72b81ba6282e/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29_EN.pdf

EBA Cyber Resilience Framework

Outlines strategies to enhance cyber resilience among EU financial entities.

eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management

EBA Guidelines on ICT and security risk management

Defines procedures for reporting ICT incidents as per EBA requirements.

eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management

Frequently asked questions

Are the EBA ICT and security risk management Guidelines still in force?

Only in part. EBA/GL/2025/02 deleted paragraphs 1 to 91, which were sections 3.1 to 3.7, with effect from May 20, 2025. Guideline 3.8 on payment service user relationship management (paragraphs 92 to 98) remains.

Why were most of the Guidelines deleted?

The EBA found that DORA, which applies from January 17, 2025, and its regulatory technical standards cover the ICT risk management, incident, testing and third-party content. Keeping a parallel set for the same entities would run against DORA's objectives.

What does Guideline 3.8 require?

Payment service providers give users assistance and guidance on security risks, update it for new threats, let users disable specific payment functions, adjust agreed spending limits, receive alerts on initiated or failed payment attempts, learn about security procedure updates and get support on security matters (paragraphs 92 to 98).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Who are the Guidelines addressed to now?

Competent authorities and financial institutions that are payment service providers under Article 1(1), points (a), (b) and (d) of PSD2, which are credit institutions, electronic money institutions and payment institutions, including exempted ones.

Where do banks find ICT risk requirements now?

In DORA and its regulatory technical standards for the entities within DORA's scope, which have applied since January 17, 2025.

License included / downloadable: Yes The Guidelines are published free by the European Banking Authority and are included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/eu-eba-gl-2019-04-guidelines-on-ict-and-security-risk-management