

EBA/GL/2019/04

EBA Guidelines set ICT and security risk management requirements to strengthen operational resilience and protect EU financial institutions' information systems.



What it is

EU EBA GL/2019/04 — Guidelines on ICT and Security Risk Management is a regulatory framework that provides financial institutions with requirements and best practices to identify, manage, and mitigate information and communication technology (ICT) and security risks. The guidelines aim to enhance operational resilience, safeguard sensitive data, and strengthen protections against cyber threats and disruptions.

Published by the European Banking Authority (EBA), this framework applies to credit institutions, investment firms, and payment service providers across the European Union. It covers a broad range of areas, including cybersecurity controls, risk assessment methodologies, incident response planning, business continuity management, and regulatory compliance with digital operational resilience requirements.

At a glance

PUBLISHER European Banking Authority (EBA)	TYPE Guidance	VERSION EBA/GL/2019/04
EFFECTIVE June 30, 2020	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>

Why it matters

- **Strengthen ICT governance** Establish clear policies and accountability for managing technology and security risks across the organization.
- **Enhance regulatory alignment** Support compliance with EU financial sector requirements by aligning internal controls to supervisory expectations and obligations.
- **Promote operational resilience** Enable organizations to anticipate, withstand, and recover from ICT-related disruptions and cyber threats more effectively.
- **Improve incident response planning** Ensure that processes for identifying, escalating, and managing security incidents are structured, documented, and regularly tested.

How SmartSuite supports EBA GL/2019/04

ICT Risk Requirement Library Organize governance, security, and resilience expectations with clear ownership.	ICT Risk Assessments and Treatment Run periodic assessments and track mitigations with approvals and timelines.	Outsourcing and Vendor Oversight Manage provider due diligence, contract controls, and ongoing monitoring evidence.
Incident Response and Escalation Workflow Track incident handling, classification, and reporting readiness with documentation.	Control Testing and Assurance Schedule testing, monitoring, and evidence capture for key ICT controls.	Supervisory Readiness Reporting Provide leadership and regulator-ready reporting on posture, gaps, and actions.

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 ICT Risk Assessment Methodology Provides methods for assessing ICT-related risks in alignment with EBA guidelines. eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management
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 Incident Reporting Guidelines Defines procedures for reporting ICT incidents as per EBA requirements. eba.europa.eu/regulation-and-policy/internal-governance/incident-reporting-guidelines

Frequently asked questions

What is EU EBA GL/2019/04 used for?

EU EBA GL/2019/04 is designed to help financial institutions identify, manage, and mitigate ICT and security risks. Its goal is to strengthen operational resilience, protect sensitive data, and prevent cyber threats and disruptions in the EU financial sector.

Is compliance with EU EBA GL/2019/04 mandatory?

Yes, compliance is mandatory for EU credit institutions, investment firms, and payment service providers under EBA's regulatory oversight. Firms must align their risk management and ICT security practices with the guidelines to fulfill legal and supervisory requirements.

Which organizations are in scope for EU EBA GL/2019/04?

The guidelines apply to credit institutions, investment firms, and payment service providers operating within the European Union. Third-party service providers may be covered indirectly through contractual requirements and risk management obligations.

What are the key requirements of EU EBA GL/2019/04?

Key requirements include establishing ICT governance frameworks, performing regular risk assessments, implementing technical and organizational security controls, managing third-party risks, and maintaining incident response and business continuity plans. Documentation and continuous monitoring are also essential parts of compliance.

How does an organization implement the EBA Guidelines on ICT and Security Risk Management?

Implementation involves conducting comprehensive ICT risk assessments, developing and updating ICT policies, mapping controls to specific requirements, formalizing incident handling, and integrating business continuity measures. Organizations are expected to document their approach, assign responsibilities, and test the effectiveness of controls regularly.

How does EU EBA GL/2019/04 relate to other frameworks like DORA or ISO 27001?

EU EBA GL/2019/04 aligns closely with the Digital Operational Resilience Act (DORA), ISO 27001, and NIST standards, ensuring harmonization of cybersecurity and operational risk practices. Organizations commonly map controls and requirements across these frameworks to leverage synergies and ensure comprehensive compliance.

What are the ongoing compliance and monitoring requirements under EU EBA GL/2019/04?

Ongoing compliance requires institutions to perform continuous monitoring, regular control testing, updating of risk and incident records, and periodic review of ICT governance structures. Firms must also collect evidence of compliance, address audit findings, and adapt controls based on evolving threats and regulatory updates.

How would SmartSuite support EU EBA GL/2019/04?

SmartSuite enables organizations to operationalize EU EBA GL/2019/04 by facilitating risk tracking, control management, and evidence collection. The platform supports compliance monitoring, audit readiness, incident and third-party tracking, and robust reporting to ensure effective governance and streamlined regulatory adherence.

License included / downloadable: Yes The EBA ICT and Security Risk Management Guidelines are publicly available through the European Banking Authority.

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