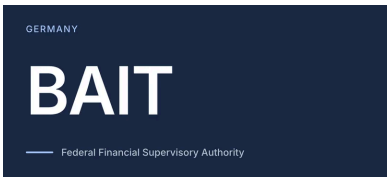
SmartSuite

Framework / Cybersecurity / Other

Bankaufsichtliche Anforderungen an die IT (BAIT) – BaFin Rundschreiben 10/2017 (BA), version of 16 December 2024

BAIT is BaFin Circular 10/2017 (BA), the IT requirements for German institutions outside DORA since 17 January 2025; BaFin repeals it at the end of 31 December 2026.



What it is

BAIT (Bankaufsichtliche Anforderungen an die IT) is BaFin Circular 10/2017 (BA) of 3 November 2017, the supervisory requirements for IT that German credit and financial services institutions have applied under section 25a(1) of the German Banking Act (KWG). It is being phased out: since 17 January 2025 institutions that must run ICT risk management under Articles 5 to 15 or Article 16 of DORA are excluded from BAIT, and BaFin will repeal the circular completely at the end of 31 December 2026.

At a glance

PUBLISHER
Federal Financial Supervisory Authority (BaFin)

TYPE
Regulation

VERSION
Circular 10/2017 (BA) in the version of 16 December 2024

EFFECTIVE
November 3, 2017 (version of December 16, 2024 applies from January 17, 2025; repealed at the end of December 31, 2026)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Germany

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html

Why it matters

- **Binding supervisory expectations** Issued on the basis of section 25a(1) KWG, BAIT is what BaFin and the Deutsche Bundesbank examine in the institutions it still covers.
- **A named security function** Paragraph 4.4 requires management to establish the information security officer function, organizationally independent under paragraph 4.5.
- **Protection needs decide the controls** Paragraph 3.4 requires a protection needs assessment for integrity, availability, confidentiality and authenticity, owned by the business units.
- **Tested emergency plans** Paragraph 10.4 requires IT emergency tests at least annually covering every IT system that supports time-critical activities and processes.

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

How SmartSuite supports BAIT

BAIT Control Library with Chapter Numbers

Hold each paragraph of chapters 1 to 12 as a control with owner, MaRisk reference, status and evidence, and flag the paragraphs that DORA now covers.

Protection Needs and Information Network Register

Record the information network components (3.3), their dependencies and the protection needs for integrity, availability, confidentiality and authenticity (3.4), owned by the business units.

Information Security Officer Reporting

Track the security policy (4.2), the officer's tasks and independence (4.4, 4.5), testing policy results (4.8) and awareness program completion (4.9) for management reporting.

Access Rights and Recertification

Run authorization concepts (6.2), attribute every access to a responsible person (6.3) and schedule the periodic rights reviews with approvals.

IT Outsourcing and Cloud Risk Assessments

Keep the contract overview of paragraph 9.3, run the pre-procurement risk assessments of 9.2 and link cloud services to AT 9 MaRisk outsourcing records.

Emergency Plans and Annual Tests

Maintain IT emergency plans with restart, emergency operation and recovery parameters (10.3) and record the annual test results and follow-ups (10.4).

Common framework mappings

EU DORA | GDPR | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0

Official resources

BAIT (Bankaufsichtliche Anforderungen an die IT)

Defines IT requirements for German banks and financial service providers.

bafin.de/EN/Aufsicht/BankenFinanzdienstleister/ITaufsicht/BAIT/bait_node_en.html

Frequently asked questions

Does BAIT still apply after DORA?

Only to institutions outside DORA. The preliminary remark of the 16 December 2024 version excludes, from 17 January 2025, every institution that must run ICT risk management under Articles 5 to 15 or Article 16 of DORA. BaFin will repeal BAIT completely at the end of 31 December 2026; the FinmadiG brings financial services institutions under DORA from 1 January 2027.

What is the legal basis of BAIT?

Section 25a(1) of the German Banking Act (KWG), which requires a proper business organization including adequate technical and organizational resources, and section 25b KWG for outsourcing. BAIT concretizes the MaRisk circular for IT; the MaRisk requirements remain unaffected (preliminary remark 2 and 3).

What are the chapters of BAIT?

IT strategy, IT governance, information risk management, information security management, operational information security, identity and access management, IT projects and application development, IT operations, outsourcing and other procurement of IT services, IT emergency management, a repealed chapter 11 on payment service users, and critical infrastructures.

What does BAIT require of the information security officer?

Management must establish the function (paragraph 4.4), which is responsible for all information security matters inside the institution and toward third parties, and must make it organizationally and procedurally independent (4.5), with its own job description, resources and training budget to avoid conflicts of interest. Reporting to management follows BT 3.2 MaRisk.

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

How does BAIT treat cloud services?

Paragraph 9.1 treats cloud services, meaning IT provided over a network and billed dynamically through defined interfaces, as outsourcing under AT 9 MaRisk. Any other procurement of IT services needs a prior risk assessment (9.2) and must be managed through a complete contract overview (9.3).

License included / downloadable: Yes The circular is published free of charge by BaFin (German text) and by the Deutsche Bundesbank, and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/germany-banking-supervisory-requirements-for-it-bait