

BAIT (BaFin, 2017)

BAIT is a German supervisory framework requiring banks and financial institutions to implement IT security, governance, and risk-management controls.



What it is

Germany Banking Supervisory Requirements for IT (BAIT) is a regulatory framework that sets forth specific requirements for information technology security, governance, and risk management within German financial institutions. The framework aims to ensure that banks and financial service providers implement effective IT controls to protect critical systems, data, and processes from cyber threats and operational risks.

Published by the Federal Financial Supervisory Authority (BaFin), BAIT applies to banks, credit institutions, and other regulated financial entities operating in Germany. It addresses areas such as IT governance, information security management, access controls, data protection, outsourcing oversight, and incident response, aligning with broader European banking and cybersecurity regulations.

At a glance

PUBLISHER Federal Financial Supervisory Authority (BaFin)	TYPE Regulation	VERSION BAIT — Banking Supervisory Requirements for IT
EFFECTIVE January 1, 2018	DOMAIN Cybersecurity	FAMILY BSI IT-Grundschrift
REGION Germany	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/ITAufsicht/BAIT/bait_node_en.ht

Why it matters

- **Strengthen cybersecurity oversight** Enhance management visibility over IT risks and security controls, contributing to proactive threat identification and mitigation.
- **Enhance regulatory alignment** Support adherence to BaFin and European banking regulations, reducing compliance gaps and regulatory enforcement risks.
- **Promote operational resilience** Ensure continuity of critical banking functions by requiring structured IT risk management and robust incident response processes.
- **Increase audit readiness** Facilitate the documentation and review of IT controls, making it easier to demonstrate compliance during official audits and examinations.

How SmartSuite supports BAIT

IT Governance and Control Management

Centralize IT policies, governance documentation, and technology control ownership.

Cybersecurity Risk Assessment and Tracking

Identify technology risks, track mitigation actions, and monitor cybersecurity controls.

Access and Identity Governance

Manage user roles, privileged access approvals, and authentication policies.

IT Operations and Incident Management

Track IT incidents, remediation tasks, and operational risk events affecting technology systems.

Outsourcing and Vendor Risk Oversight

Evaluate third-party technology providers and monitor compliance with regulatory expectations.

BAIT Regulatory Reporting and Audit Readiness

Provide dashboards and reporting showing IT risk posture and BAIT compliance status.

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

What is BAIT used for?

BAIT (Bankaufsichtliche Anforderungen an die IT) is used to define specific requirements for IT security, governance, and risk management within German banks and financial institutions. It aims to ensure these organizations establish effective controls to safeguard critical systems, data, and business processes against cyber threats and operational risks.

Is BAIT mandatory for financial organizations in Germany?

Yes, BAIT is mandatory for banks, credit institutions, and other regulated financial service providers operating in Germany. Compliance is required under the supervision of the Federal Financial Supervisory Authority (BaFin) and is subject to ongoing regulatory review and audits.

Who does the BAIT framework apply to?

BAIT applies to all banks and financial services institutions regulated by BaFin in Germany, including both domestic and EU-licensed foreign entities operating in the German market. Its requirements extend to internal IT operations as well as outsourced IT services.

What are the key concepts and artifacts required by BAIT?

Key concepts under BAIT include documented IT strategy, comprehensive information security management, change and release management, access controls, operational resilience, and incident response. Required artifacts often consist of security policies, risk assessment documentation, incident logs, outsourcing contracts, and audit trails.

How do organizations implement BAIT requirements?

Organizations implement BAIT by integrating its requirements into their internal control systems, developing IT governance structures, performing risk and gap analyses, and regularly updating security policies. Continuous monitoring, documentation, and ongoing training also play crucial roles in practical compliance.

How does BAIT relate to other frameworks like ISO 27001?

BAIT aligns with international standards such as ISO 27001, particularly in its approach to information security management and risk assessment. While ISO 27001 can provide a foundation, BAIT includes additional supervisory expectations tailored for the German financial sector, requiring further specific controls.

What are the ongoing compliance obligations for BAIT?

Ongoing compliance with BAIT includes regular supervisory assessments, periodic risk evaluations, continuous improvement of IT processes, and the timely reporting of incidents. Financial institutions must ensure documentation is up-to-date and controls remain effective as technology and risks evolve.

How would SmartSuite support Germany Banking Supervisory Requirements for IT (BAIT)?

SmartSuite can help organizations manage BAIT by building a control library aligned to BAIT requirements, tracking risks, governing documentation, and facilitating evidence collection for audits. It supports remediation workflows, vendor assessments, ongoing monitoring, and offers customizable reporting dashboards to demonstrate compliance and prepare for supervisory reviews.

License included / downloadable: Yes BAIT guidance is publicly available through Germany's Federal Financial Supervisory Authority (BaFin).

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