BAIT (Banking Supervision Requirements for IT) is implemented to ensure that information technology in banks and other financial institutions in Germany is secure and reliable. The standard guidelines require operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities. ARCON's highly mature Identity and Access Management (IAM) along with enterprise risk remediation solutions can help the enterprises to comply with the BAIT mandates.

Table of Content

Overview

At the end of 2017, the German Federal Financial Supervisory Authority (BaFin) published the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT, BAIT) - a binding set of rules for safeguarding IT infrastructure in the finance industry of Germany. The main objective is to ensure the secure design of IT systems and processes and to create transparent governance. It supplements the MaRisk (Minimum Requirements for Risk Management) compliance standards and is divided into various areas that provide detailed regulations and recommendations for dealing with IT security in the organizations of the financial sector.

Understanding the BAIT compliance standards

The BAIT is the compliance standard that defines the statutory requirements of Section 25A of the German Banking Act (Kreditwesengesetz, KWG). Accordingly, the supervisory authority's catalog of requirements explains how financial institutions must set up appropriate technical and organizational resources for their IT systems. In terms of content, the BAIT is built on MaRisk and specifies them in greater detail. However, the MaRisk requirements remain unaffected by the BAIT and thus retain their validity. BaFin particularly emphasizes the consideration of information security requirements and an appropriate contingency plan. In addition, BAIT also addresses Section 25b KWG since companies in the finance industry are increasingly outsourcing IT services as other external procurement, non-material, or material outsourcing. Overall, BaFin sees BAIT as the principal component for IT supervision in the banking sector in Germany.

What are the requirements to comply with BAIT compliance standard?

The BAIT has a modular structure and is originally comprised of nine chapters. It is intended to provide the necessary flexibility for future adjustments and the implementation of new subject areas of IT security standards. After the amendments in August 2021, the BAIT has a principle-based structure and is intended to create IT risk awareness by presenting the requirements in a transparent manner.

The guidelines issued by BaFin, the German Federal Financial Supervisory Authority are designed to ensure that financial institutions maintain robust IT systems and processes. Here are the key requirements for BAIT compliance:

1. **IT Strategy:** Organizations must have a concrete and well-defined IT strategy that aligns IT operations.
2. **IT Governance:** Institutions must have a clear IT governance framework that aligns with their overall business strategy.
3. **Information Risk Management:** Effective management of information risks, including identification, assessment, and mitigation of IT-related risks.
4. **Information Security Management:** Implementation of comprehensive information security measures to protect data integrity, confidentiality, and availability.
5. **Operational Information Security:** It is crucial for maintaining the overall security posture of an organization and ensuring that its information assets are protected against various IT threats.
6. **Identity Access Management:** IAM is a framework of policies and technologies that ensures the right individuals have the right access to the right technology resource.

The requirements of BAIT follow the principles of methodological freedom and dual proportionality to ensure proportionality. This means that BaFin defines regulatory guard rails which guide the institutions in the specific design of the measures. In addition, the supervisory authority considers the risk profile of the respective company, whereby the business model and the complexity of the risks play a role in addition to the volume of business.

Who should follow BAIT Compliance?

BAIT compliance is primarily aimed at financial institutions operating in Germany. This includes:

- **Banks:** All types of banks, including commercial banks, savings banks, and cooperative banks.
- **Insurance Companies:** Firms providing insurance services.
- **Financial Service Providers:** Companies offering financial services, such as investment firms and payment service providers.
- **Outsourced Service Providers:** Third-party vendors that provide IT services to financial institutions must also adhere to BAIT requirements to ensure the overall compliance of the institution they serve.

These guidelines help ensure that these entities maintain robust IT systems and processes to protect against risks and ensure the integrity and security of financial operations.

Role of IAM in complying with BAIT

Identity and Access Management (IAM) plays a crucial role in complying with BAIT (Bankaufsichtliche Anforderungen an die IT) requirements. The top areas where IAM contributes to BAIT compliance are:

- **Access Control:** BAIT mandates strict control over access to IT systems. IAM ensures that only authorized personnel can access sensitive information and systems, reducing the risk of unauthorized access and data breaches.
- **User Authentication and Authorization:** IAM systems provide robust authentication mechanisms, such as multi-factor authentication (MFA), to verify user identities. They also manage user permissions, ensuring that users have access only to the resources necessary for their roles.
- **Audit and Monitoring:** BAIT requires continuous monitoring and logging of access to IT systems. IAM solutions facilitate detailed logging of user activities, which can be audited to detect and respond to suspicious activities.
- **Identity Governance:** IAM helps in managing the lifecycle of user identities, from creation to deletion. This includes regular reviews and updates of user roles and permissions, ensuring compliance with BAIT's requirements for information security and risk management.
- **Incident Response:** In case of a security incident, IAM systems can quickly revoke access or adjust permissions to mitigate risks, aligning with BAIT's requirements for effective incident response and contingency management.

By implementing a robust IAM framework, financial institutions can ensure they meet BAIT's stringent requirements for IT governance, information security, and risk management.

BAIT Compliance Checklist and Role of ARCON

BAIT requirements	Does ARCON help?	Which ARCON solution and its feature addresses it?
The IT systems, the related IT processes and the other components of the information domain shall ensure the integrity, availability, authenticity, and confidentiality of the data. The institution shall define and coordinate the tasks, competencies, responsibilities, controls, and reporting channels required for the management of information risks.		▪ ARCON EPM ▪ ARCON FIM (File Integrity Monitoring) ▪ ARCON PAM
5.1 - Appropriate monitoring and steering processes shall be established for IT risks, comprising the definition of IT risk criteria, the identification of IT risks, the determination of the protection requirement, protective measures for IT operations derived from it, and the definition of measures to manage and mitigate risks.		▪ ARCON PAM ▪ ARCON EPM
6.2 - User access rights concepts shall ensure that users are assigned access rights according to the need-to-know and least privilege principles, that the segregation of duties is observed across user access rights concepts and that conflicts of interest are avoided. User access rights concepts shall be reviewed regularly and, on an event, -driven basis and updated if necessary.		▪ ARCON PAM • Access control • Identity Governance • Virtual Grouping • Just-In-Time (JIT) • ITSM • Dynamic workflows

6.4 - Approval and control processes shall ensure compliance with the requirements contained in the user access rights concept when setting up, changing, deactivating, or deleting access rights for users. The responsible organizational unit shall be appropriately involved, thus enabling it to fulfil its organizational responsibilities		▪ ARCON PAM • Dynamic workflows • Just-In-Time (JIT) • Access control • Identity Governance • ITSM
6.5 - The control bodies responsible for setting up, changing, deactivating, or deleting access rights shall be involved in reviewing whether access rights granted are still required and whether these comply with the requirements contained in the user access rights concept (recertification).		▪ ARCON PAM • Identity Governance • Access control • Just-In-Time (JIT)
6.6 - The setting up, changing, deactivating, and deleting of access rights and recertification shall be documented in a way that facilitates comprehension and analysis.		▪ ARCON PAM • Identity Governance • Access control • Just-In-Time (JIT)
6.7 - The organization shall set up logging and monitoring processes consistent with the protection requirements and the target requirements that enable checks to be carried out to ensure that access rights are used only in the manner intended. Owing to the associated far-reaching intervention options, the institution shall set up appropriate processes to log and monitor the activities with privileged (particularly critical) access rights.		▪ ARCON PAM • SIEM (Security Information and Event Management) • Audit logs • Access logs • Just-In-Time (JIT) • Session management • ITSM • Dynamic workflows • Identity Governance

Conclusion

ARCON's IAM solutions enables security and risk management leaders to –

- Comply with BAIT cybersecurity guidelines
- Ensure robust identity and access management posture
- Mitigate unauthorized access and chances of data breach incidents
- Ensure continuous monitoring and logging of access to different IT systems
- Help with identity governance and manage dynamic workflow of identities

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us