CORE®

ZAIT - Comparison with BAIT

Out of 12 chapters 6 identical in content, 5 considerably and 1 extensively expanded

Dr. Waldemar Grudzien
Liubov Khomutovskaya

December 2021

Key Facts

- Chapter 9 on outsourcing has been greatly expanded
- The other changes in five chapters are of a medium nature and should not pose any major challenges to technology-savvy institutions capable of change
- BaFin thus takes account of the trend towards outsourcing IT infrastructure and white-labelling of bank licences.
- ZAIT introduces additional fine-grained specifications, a framework with target formulations and the freedom of implementation with appropriate measures increasingly becomes a catalogue of measures
- The further technologization of the banking business shows the advantages of an existing functional ISMS, as most of the requirements of ZAIT are already addressed by a comprehensive ISMS according to common standards.

Introduction

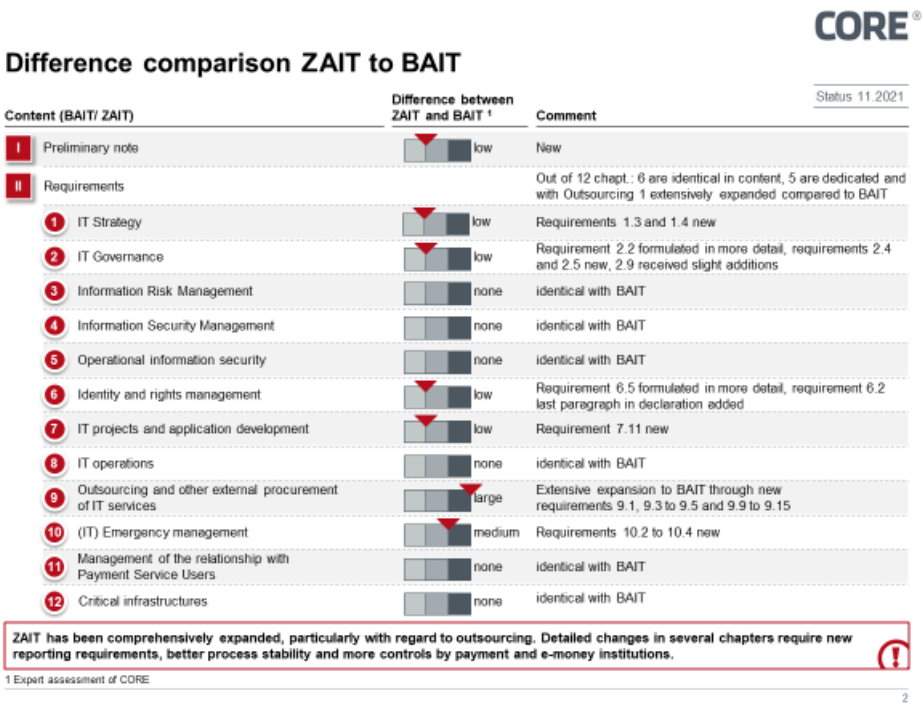
In mid-August 2021, BaFin also updated the "Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Meld-Instituten - ZAIT" (Payment Services Supervisory Requirements for the IT of Payment and Electronic Money Institutions). The circular specifies the IT requirements specifically for these institutions. The requirements are very close to the already existing IT requirements for banks (BAIT) and include in particular the EBA requirements from the EBA Guidelines on ICT and Security Risk Management (GL/2017/17) and the EBA Guidelines on Outsourcing (GL/2019/02). Of the 12 chapters, six remain identical in content to BAIT:

- Information Risk Management,
- Information Security Management,
- Operational Information Security,
- IT Operations,
- Management of relationships with payment service users, and
- Critical Infrastructure.

Five chapters underwent minor to moderate expansions:

- IT Strategy,
- IT Governance,
- Identity and rights management,
- IT projects and application development and
- IT Emergency Management.

The chapter "9 Outsourcing and Other External Procurement of IT Services" has been extensively expanded compared to the BAIT. The following figure provides a summary of the differences.



Difference comparison ZAIT to BAIT

Status 11.2021

Content (BAIT/ ZAIT)	Difference between ZAIT and BAIT [1]	Comment
I Preliminary note	low	New
II Requirements		Out of 12 chapt.: 6 are identical in content, 5 are dedicated and with Outsourcing 1 extensively expanded compared to BAIT
1 IT Strategy	low	Requirements 1.3 and 1.4 new
2 IT Governance	low	Requirement 2.2 formulated in more detail, requirements 2.4 and 2.5 new, 2.9 received slight additions
3 Information Risk Management	none	identical with BAIT
4 Information Security Management	none	identical with BAIT
5 Operational information security	none	identical with BAIT
6 Identity and rights management	low	Requirement 6.5 formulated in more detail, requirement 6.2 last paragraph in declaration added
7 IT projects and application development	low	Requirement 7.11 new
8 IT operations	none	identical with BAIT
9 Outsourcing and other external procurement of IT services	large	Extensive expansion to BAIT through new requirements 9.1, 9.3 to 9.5 and 9.9 to 9.15
10 (IT) Emergency management	medium	Requirements 10.2 to 10.4 new
11 Management of the relationship with Payment Service Users	none	identical with BAIT
12 Critical infrastructures	none	identical with BAIT

ZAIT has been comprehensively expanded, particularly with regard to outsourcing. Detailed changes in several chapters require new reporting requirements, better process stability and more controls by payment and e-money institutions.

1 Expert assessment of CORE

2

Figure 1: Difference comparison ZAIT to BAIT

Individual examination of chapters with minor to medium changes

- Preliminary note
- Chapter 1: IT Strategy,
- Chapter 2: IT Governance,
- Chapter 6: Identity and rights ranagement,
- Chapter 7: IT projects and application development and
- Chapter 10: IT Emergency management.

The preliminary remarks of BAIT (4 preliminary remarks) and ZAIT (5 preliminary remarks) are similar in their core statements in that they define the respective group of users, set out the legal framework, commit themselves to the principle of proportionality and, in the design of the IT systems and the associated IT processes, are generally based on common standards.

Two new requirements 1.3 and 1.4 have been included in chapter "1. IT Strategy". In 1.3, BaFin prescribes a PDCA cycle for strategy processes, while requirement 1.4 requires the institution to pass on and discuss the IT strategy with the supervisory body, not only once, but also in the event of adjustments. In both requirements 1.1 and 1.2, the consistency of the IT strategy with the business strategy has been moved from 1.2 in the BAIT to 1.1 in the ZAIT, otherwise both requirements have remained identical in content.

In chapter "2. IT Governance", requirement 2.2 is formulated in more detail, requirements 2.4 and 2.5 are new, and requirement 2.9 has been supplemented slightly. Requirement 2.2 has been expanded to include the obligation to effectively implement processes from the IT structure and IT process organization. Only the two requirements 2.4 (ensuring the quality level of employees)

and 2.5 (missing employees must not disrupt the operational process) are new. Requirement 2.9 has been supplemented by the last sentence (suitability of the IT systems and IT processes to achieve the protection objectives must be checked by the employees with functional and technical responsibility). The comments on 2.9 have been expanded to include PCI-DSS in the standards for the design of IT systems. All other requirements on IT governance of the ZAIT can be traced back to various requirements and explanations on the chapter of the same name in the BAIT.

The "Identity and rights management" (Chapter 6) has two changes to BAIT: For requirement 6.2, the last paragraph has been added to the statement. This can be summarized as "Authorizations must correspond to the organizational assignment". The second change relates to requirement 6.5, which is now formulated in more detail, and can be summarised with two central statements:

- Authorizations must be adjusted in a timely manner
- Recertifications must take place at least
    - semi-annually: particularly critical authorizations such as those of administrators
    - annual: essential entitlements
    - every three years: all others

Chapter 7 "IT projects and application development" has only one change with requirement 7.11. According to this requirement, IT systems must be tested and accepted before they are used for the first time and after significant changes (whereby an indication of the assessment of the significance of the change is given in the declaration). A rule process must be established for this purpose; the mandatory separation of production and test environments is also called for. In the explanations, a valuable reference is made to third-party test certificates, such as certifications; these do not completely replace the institute's own acceptance. An institution must incorporate further expertise of its own into the assessment of the suitability and appropriateness of the IT systems.

Chapter 10 "Emergency management" has undergone more adjustments: Requirement 10.1 is shortened compared to 10.1 of the BAIT, the "missing" parts were distributed in the ZAIT to other requirements in chapter 10. Requirement 10.2 prescribes the performance of impact analyses and risk analyses for the identification of time criticalities. The former analysis examines impaired activities and processes with regard to their impact on business operations, while the risk analysis examines activities and processes identified as time-critical with regard to their impairment of business processes.

Requirement 10.3 prescribes both business continuity and recovery plans for the emergency concept. Thus, as with BAIT, only the standard BCMS is preferred as one of three possible BCMS models of BSI Standard 200-4. In the case of outsourcing, the emergency plans must be coordinated with each other. The descriptive part of the requirement stipulates at least the following scenarios for consideration in the emergency plan:

- (Partial) failure of a site
- significant failure of IT systems or communication infrastructure
- Loss of a critical number of employees

- Failure of service providers

Requirement 10.4 prescribes the regular review of the effectiveness and adequacy of the emergency concept. Regular for time-critical activities and processes means to be demonstrated at least annually[1] and on an as-needed basis. The reviews must include, but are not limited to:

- Test of the technical precautionary measures
- Communication, crisis management and alerting exercises
- Emergency or full-scale exercises

Description of changes in Chapter 9 on outsourcing and other IT-related matters

In principle, BAIT refers to AT.9 MaRisk for outsourcing and only specifies requirements for other external procurement. The ZAIT always addresses outsourcing and other external procurement without reference to its own separate minimum requirements.

The ZAIT recodifies Chapter 9 in large parts. Four requirements of the BAIT are also reflected in the ZAIT:

- ZAIT 9.2 corresponds to BAIT 9.1
- ZAIT 9.6 corresponds to BAIT 9.5
- ZAIT 9.7 corresponds to BAIT 9.3
- ZAIT 9.8 corresponds to BAIT 9.4

Requirements 9.1, 9.3 to 9.5 and 9.9 to 9.15 are new and their most important statements are presented below in cursory form:

Requirement 9.1:

- emphasises the fact that responsibility for outsourcing remains with the institution
- Management tasks of the executive board cannot be outsourced
- In the case of outsourcing outside the EEA, supervision of the outsourcing entity by the competent supervisory authorities in the third country must be ensured. The outsourcing institution must ensure that a cooperation agreement is in place between the supervisory authorities responsible for the supervision of the institution and the supervisory authorities responsible for the supervision of the outsourcing entity.

  The last addition is entirely new and could pose a question mark and at least time delays for institutions, at least as long as no standardised and already numerous cooperation agreements between authorities exist.

Requirement 9.3:

[1] and occasion-related (this is only mentioned once here, as all documents must be updated when the occasion arises)

- An institution must continue to have sufficient knowledge and experience to ensure effective monitoring of the IT service provided
- In the event that the outsourcing relationship is terminated or the group structure is changed, it must be possible to continue orderly operations in these areas

Institutions are thus obliged to maintain their own resources that can guarantee a sufficient assessment of the services of the service providers, both in terms of expertise and in the key compliance areas. It is questionable whether the institutions must be able to provide the outsourced area themselves in an emergency or whether, for example, a sufficiently detailed analysis of the provider landscape and the possibility of a rapid change of provider is sufficient. For services with a wide choice of providers and low migration costs, this probably does not mean a requirement to provide sufficient resources for internalisation. This would also contradict point 9.9, which calls for consideration in contingency planning in the absence of options for action, without making more specific specifications here.

Requirement 9.4:

- Definition for outsourcing that cannot be excluded by contractual agreements
- Giving examples of the distinction between outsourcing and other external procurement
- Maintenance and software support services are not to be classified as outsourcing, unless the software is used to identify, assess, manage, monitor and communicate risks or is essential for the performance of payment services business tasks.

Requirement 9.5:

- Obligation to carry out a preliminary assessment of the outsourcing of IT activities and IT processes or external procurement by means of a risk analysis.
- Identification of significant outsourcing on the basis of the risk analyses
- Preparation of frameworks for risk analysis
- From the declarations, extensive, detailed specifications are to be taken into account in risk analysis with regard to risk consideration, participating responsible functions and
- In the case of outsourcing of IT activities or IT processes with significant consequences, it must be intensively examined whether and how the outsourced IT activities and IT processes can be included in risk management.

Unfortunate is the introduction of the term "substantial consequence", which, in addition to "materiality", does not contribute to simplification.

Requirement 9.9:

- Commitment to the preparation of an exit strategy and its regular review
- If there are no options for action, the exit option must be taken into account in the context of contingency planning.

Requirement 9.10:

- Detailed specifications for minimum contents of the outsourcing contract, including "agreed service quality with clearly defined performance targets" and ensuring data

protection-compliant processing, support for the institution by the old outsourcing company in the event of transfer from the old outsourcing company to the new outsourcing company
- Delimitation of the obligation to agree on rights to issue instructions
- Granting of information and audit rights to BaFin in the case of outsourcings

It is helpful to note that an explicit agreement on rights to issue instructions in favour of the institution can be dispensed with if the service to be provided by the outsourcing company is specified sufficiently clearly in the outsourcing agreement. This is often a difficult point of negotiation. Furthermore, the internal audit function of the outsourcing institution may refrain from carrying out its own audit procedures if an audit activity carried out elsewhere, e.g. in the form of group audits, satisfies the supervisory requirements.

Internal preparatory actions and documentation must include consideration of the internal level of acceptance of any poor performance.

Requirement 9.11:

- Granting of information and consent rights to the institution in the event of onward transfers to be included in the outsourcing agreement
- Subcontracting agreement must correspond to agreements of the original outsourcing agreement
- Institute has to assess quality of outsourced services on a regular basis

Requirement 9.12:

- Obligation to establish the function of the central outsourcing officer (zAB), who is to be supported by a central outsourcing management depending on the type, scope and complexity of the outsourcings
- Requirements for the direct subordination of the zAB to management
- Specifications of the minimum tasks of outsourcing management

Requirement 9.13:

- Preparation of a report on material outsourcing at least annually and on an ad hoc basis (exception: smaller, less complex institutions)
- Derivation of a statement whether outsourcing should be continued

Requirement 9.14:

- Facilitation for financial alliances such as
    - Risk-mitigating consideration of effective precautions at group level, in particular uniform and comprehensive risk management as well as rights of access in the case of group- and association-internal outsourcing of IT activities and IT processes in the preparation and adjustment of the risk analysis
    - Setup of a central outsourcing management on group or association level possible
    - Waiver of the creation of exit processes and options for action

- common contingency plans

Requirement 9.15:

- Keeping an up-to-date outsourcing register with information on all outsourcing agreements
- minimum content requirements for the outsourcing register for all outsourcings in point 54 and for material outsourcings in point 55 of the EBA Guidelines on Outsourcing (EBA/GL/2019/02).
- The outsourcing register shall cover all outsourcing agreements, including outsourcing agreements with outsourcing entities within a group of institutions or a financial network.
- In the case of further outsourcing of material outsourcing, the outsourcing institution must determine whether the part to be further outsourced is material and material parts must be recorded in the outsourcing register

Authors

Waldemar Grudzien is Expert Director at CORE. He holds a PhD in electrical engineering and a diploma in economics. His work focuses on information security and data protection - in theory and practice, including his work as an ISB and DPO in various client structures.

Mail: waldemar.grudzien@core.se

Liubov Khomutovskaya is a Senior Legal Expert at CORE. She is a business lawyer and focuses on the negotiation and drafting of IT contracts as well as on information security issues.

Mail: liubov.khomutovskaya@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany14109
https://core.se/
Phone: +49 30 263 440 20
office@core.seoffice@core.se

COREtransform GmbH
Am Sandwerder 21-23
Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20

COREtransform Ltd.
Limmatquai 1Canary
8001 Zurich | HelvetiaLondon
https://core.se/
Phone: +41 44 261 0143
office@core.seoffice@core.se

COREtransform Ltd.
Wharf, One Canada Square
E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61

COREtransform Consulting MEA Ltd.
DIFC - 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se

