VAIT Update 2022

High reuse share from BAIT and ZAIT

Dr. Waldemar Grudzien
Nadine Hofmann

April 2022
Blogpost

Key Facts

- The share of new content in text paragraph counting is less than 8% compared to BAIT and ZAIT, a further 16% of the text paragraphs were slightly complemented
- In the case of outsourcing, VAIT does not follow ZAIT, but remains largely faithful to the lean approach of BAIT for outsourcing
- IT emergency concept must be updated on an ad hoc basis and regularly, but not annually as with BAIT and ZAIT
- Insurance companies may explicitly write the IT strategy as part of the business or risk strategy; a separate document is not necessary
- Unification of BAIT, VAIT and ZAIT into sectoral IT requirements catalogue with sector-specific additions in view of the equal shares offered for bundling the personnel and organisational resources of BaFin and the Bundesbank

Introduction

At the beginning of March 2022, BaFin published Circular 10/2018 as amended on 03.03.2022 "Insurance Supervisory Requirements for IT (VAIT)" and replaced the VAIT as amended on 20.03.2019. Following Circulars 10/2017 (BAIT) and 11/2021 (ZAIT) of 16 August 2021, the triad of supervisory requirements for IT of the three groups of financial market players - insurance companies, banks as well as payment and e-money institutions - was updated.

With the new version, BaFin is adapting the VAIT to the "Guidelines on Security and Risk Management for Information and Communication Technology (ICT) " published in October 2020 by EIOPA.[1]

In our following remarks, the analysis of VAIT follows, also in the context of BAIT and ZAIT.

Technical analysis

The updated VAIT consists of two parts, "I. Preliminary Remarks" and "II. Requirements", with 11 chapters in the second part and a total of 104 text paragraphs.

Section I "Preliminary remarks" consists of 12 text paragraphs and thus, compared to BAIT (4) and ZAIT (6), of significantly more content which, moreover, has five new text paragraphs. Seven text paragraphs were adopted from BAIT and ZAIT. In addition to insurance-specific content (text paragraphs 3 and 5), the new five text paragraphs contain self-evidence (text paragraphs 10 to 12):

- Text paragraph 3: Circular also applies to groups of insurance and reinsurance companies domiciled in Germany
- Text paragraph 5: Ensuring compliance with the requirements in outsourcing agreements with IT service providers

[1] European Insurance and Occupational Pensions Authority

- Text paragraph 10: Determination that risk profile is dependent on structures, IT systems or processes
- Text paragraph 11: Determination that a risk profile continues to apply if there are no changes
- Text paragraph 12: Assignment of the overall responsibility from the Circular to all members of the Executive Board, this cannot be delegated and dismissed from among themselves

Text paragraph 5 marks the importance of chapter 9 (with a focus on outsourcing). Text paragraphs 10 and 11 are intended to further explain the principle of proportionality described in paragraphs 7 to 9. Text paragraph 5 would be better placed in chapter 9 (focus on outsourcing). Text paragraphs 10 and 11 are probably intended to explain the principle of proportionality described in text paragraph 7 to 9.

The **second section** has been expanded on two chapters "Chapter 5: Operational Information Security" and "Chapter 10: IT Emergency Management" compared to the previous version of the VAIT. Figure 1 illustrates the equal parts and differences in content between the three requirement catalogues of VAIT, BAIT and ZAIT. The three sets of requirements were compared from several perspectives: Equality of content, equality of interpretation and equality of effect of the implemented requirement.

The x-axis shows the chapters of the two sections, which in turn are divided into the individual text paragraphs. For a better understanding of Figure 1, two reading examples follow:

- Field "II 2.X/10": VAIT text paragraph 2.10 is a complemented content transfer of text paragraphs 3.1 in Section II Chapter 3 and from text paragraphs 3 in Section I of the BAIT
- Field "II 7.X/16": VAIT text paragraphs 7.16 is a content transfer of text paragraphs 7.14 in Section II Chapter 7 from BAIT and text paragraphs 7.15 in Section II Chapter 7 from ZAIT.

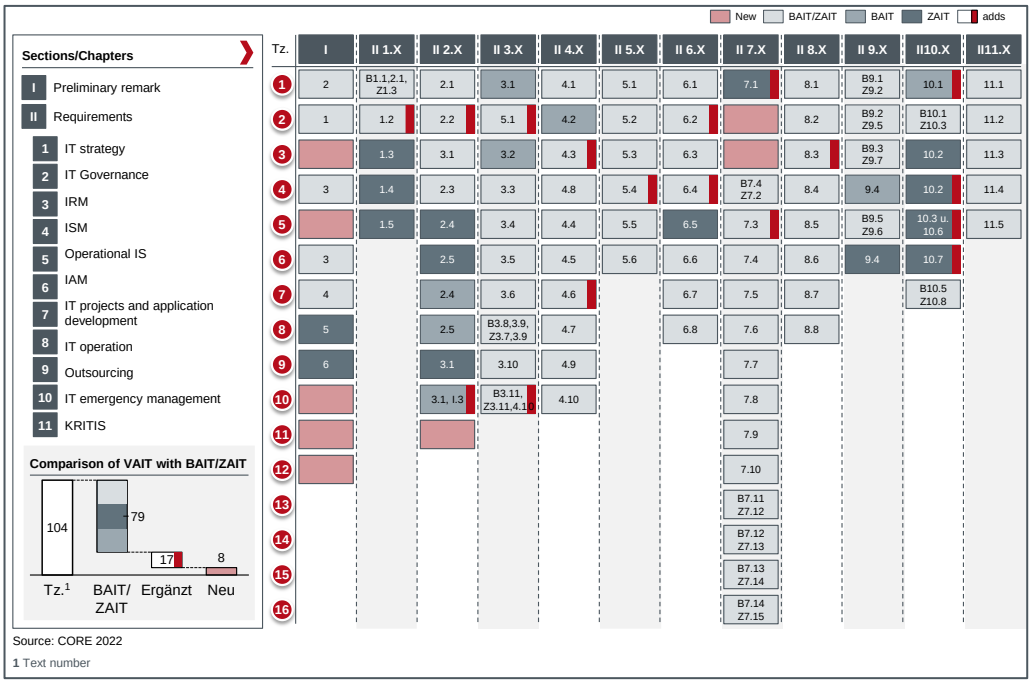

Figure 1 : Comparison of VAIT (version of 03.03.22) with BAIT and ZAIT (both version of 16.08.2021)

The equal proportions (all three shades of grey) are immediately obvious, because VAIT consists for the most parts of content from BAIT and ZAIT: Of 104 text paragraphs of VAIT 8 text paragraphs were newly formulated, 96 text paragraphs are either unchanged (79) or - mostly slightly - complemented (17). In percentages, 76% of the VAIT consists of the same content as the BAIT and ZAIT, 16.3% of complemented text paragraphs and 7.7% of new content compared to the BAIT and ZAIT. BAIT and ZAIT were updated in August last year and were ahead of VAIT with the two chapters "Chapter 5: Operational Information Security" and "Chapter 10: IT Emergency Management". BaFin has corrected this with the new VAIT. However, not all of the new contents of the ZAIT (compare CORE blog post ZAIT - Comparison with BAIT) were included in the VAIT, which is surprising in the case of outsourcing (Chapter 9: "Outsourcings of IT services and other service relationships in the area of IT services").

Chapter 1 "**IT Strategy**":

The sentence "The management must ensure the implementation of the IT strategy." in text paragraph 1.1 is a commonplace and was taken from MaRisk, which was also published on 16 August 2021.

Addition to point 2.1: In the explanations (right-hand column), VAIT explicitly grants insurance companies the freedom to draft the IT strategy as a subchapter of the business strategy or risk strategy. Usually, the IT strategy is prepared as a separate document. There are no statements on this in BAIT and ZAIT.

The authors of the VAIT applied the strategy process from the ZAIT (the BAIT does not describe an IT strategy process, but this is described in MaRisk, which prescribes the BAIT as a minimum requirement).

Chapter 2 "**IT Governance**":

Chapter 2.2 was complemented by the following sentence: "These guidelines [on the IT structure and IT process organisation] are to be determined in the company according to the risk profile."

Chapter 2.10 was expanded to include the process of assigning rights with the naming of a possible role model. Furthermore, the 1LoD[2] obligation to check the suitability of IT systems and IT processes to achieve the protection goals is mentioned. The section on the allocation of rights should be moved to Chapter 6.

The new chapter 2.11 establishes the requirement for workflow descriptions (also called organisational guidelines or work instructions). This requirement corresponds to largely lived practice and thus codifies a necessary best practice.

Chapter 3 "**Information risk management**":

The statement in text paragraph 3.2 is new and describes requirements for the definition of risk criteria and the factors determining them.

Chapter 3.10 was amended with the last sentence to include reporting frequencies of a status report. The status report "contains, for example, the assessment of the risk situation" and differs from the "written report with results of the risk analysis" mentioned in the same chapter by an assessing part complementing the descriptive part of the written report.

Chapter 4 "**Information security management**":

This chapter records only two additions: In chapter 4.3, the last sentence in the explanation section was added: "The results of information risk management include the defined target measures (cf. 3.7)." Here, BaFin once again emphasises the importance of underpinning risks with measures for their treatment.

Chapter 4.7 sets in the explanatory section the requirements in the event of outsourcing for the role of the information security officer himself as well as his functional segregation in the event of outsourcing of IT-related business activities forth.

Chapter 5 "**Operational information security**":

Chapter 5 has also undergone only a few changes compared to BAIT and ZAIT. Chapter 5.4, for example, has a new sentence in the explanation section: "The rules must be suitable for recognising anomalous activities and threats." This is a reference to the obviousness of operating a SIEM with a sensible set of rules and alerts, for example. Then in chapter 5.5 there is a surprise,

[2] 1st Line of Defence

not by addition, but by omission: The reference to a SOC (Security Operations Centre) is missing. While both the BAIT and the ZAIT contain this sentence in the same place - "Prompt analysis and response may require a permanently staffed central office, e.g., in the form of a Security Operation Centre (SOC)." - this was not included in the VAIT. A SOC is mentioned in BAIT and ZAIT as an example of a possible area and is therefore not specifically required. Perhaps the authors of the VAIT wanted to avoid vagueness in the interpretation. Perhaps a SOC is not seen as the first priority of measures in the mostly non-time-critical activities of an insurance company.

Chapter 6 "**Identity and rights management**":

In Chapter 6.2, the sentence "Within the framework of the principle of economy, the access rights of each individual technical user are to be limited to the absolute minimum and user accounts that are not required are to be deleted." underlines the "need-to-know" and "least privilege" principles in IAM.

A second addition is found in Chapter 6.4 in form of a new sentence in the explanation section: "The prior consent of the responsible body is required for the setting up and changing of authorisations; in the case of deactivation or deletion, it must be informed promptly." These are actually self-evident facts, but for the first time they have been put in written form for insurance companies.

Chapter 7 "**IT projects and application development**":

Chapter 7 has new content in comparison to BAIT and ZAIT in 7.2 and 7.3, and two text paragraphs have been added. Chapter 7.1 was complemented by the last three sentences. These impose on insurance companies the obligation to also involve the "independent risk control function, the compliance function and the actuarial function in IT projects and application developments, provided that the company must establish the respective functions by law. The internal audit function may be involved in an advisory capacity. "Furthermore, chapter 7.1 also applies to the "first-time use and significant changes of IT systems".

The new paragraph 7.2 deals with the testing of IT systems prior to production operation and prescribes the separation of the operating environment from development and testing, so that the three classic software environments of development, testing and production are now effectively codified.

Chapter 7.3 addresses the difficult topic of IDP[3] by referring to four other paragraphs - 2.9 and 2.10 on technical and organisational equipment, 3.2 on risk criteria and 7.2 on testing and distinguish environments for development, testing, and operation. In addition, there is a reference to the protection requirement for data processed by IDP to derive appropriate measures.

Chapter 7.5 has been complemented to take account of change management: "If major changes to processes with an impact on information security are required as part of IT projects,

[3] Individual data processing

corresponding change requests must be made and processed." The reference to complete documentation of the change is missing.

Chapter 8 "**IT Operations**"

The only difference to BAIT and ZAIT is found in chapter 8.3 with two complemented sentences on hardware components: These must be disposed of when they are no longer in use. In the explanation section, "in particular data carriers" are added to hardware components.

Chapter 9 "**Outsourcing of IT services and other service relationships in the area of IT services":**

This chapter poses a puzzle. It corresponds to BAIT and ZAIT but does not address the major expansion of ZAIT compared to BAIT in August 2021 (compare CORE blog post ZAIT - Comparison with BAIT).

Reminder: The ZAIT addresses topics in the corresponding chapter 9 and detailed descriptions in the following text paragraphs that are not found in the VAIT or not in the same depth of detail:

- 9.3: Remaining minimum knowledge in the outsourcing company
- 9.8: Results of risk analyses in contracts
- 9.9: Continuation of business after termination of outsourcing
- 9.10: Contents of the outsourcing contract
- 9.11: Onward transfers in the outsourcing contract
- 9.12: Central Outsourcing Officer
- 9.13: Reports on outsourcing
- 9.14: Joint emergency concepts of IT bonds
- 9.15: Outsourcing register

Chapter 9.1 ZAIT applies specifically to payment service providers.

Chapter 10 "**IT emergency management**":

Chapter 10 adopted largely content from BAIT and ZAIT and were complemented in four text paragraphs. Text paragraph 10.1 contains a note that IT emergency management should also be considered in the case of outsourcing.

Text paragraph 10.2 contains a minor detail in comparison to the ZAIT, but it can mean an enormous reduction in effort for insurance companies compared to payment and e-money institutions: While BAIT and ZAIT require the IT contingency plan to be updated "annually" or on an ad hoc basis, this only has to be done "regularly" or on an ad hoc basis for insurance companies. From the authors' point of view, this is a plus for VAIT compared to BAIT and ZAIT, as it is much more practical for insurance companies.

Text paragraph 10.4 has an addition in the declaratory part, which explains the results of impact analyses and risk analyses up to the determination of measures.

Text paragraph 10.5 is supplemented in the declaratory part by two details: Firstly, IT contingency plans should contain the conditions for their activation, and secondly, alternative options should be included if the establishment of normal operations is not possible in the short term.

Text paragraph 10.6 additionally requires the written documentation of the results of emergency tests, the analysis of deficiencies and their reporting to the management.

Chapter 11 "**Critical infrastructures**"

Complies with BAIT and ZAIT.

Conclusion

The changes in VAIT compared to BAIT and ZAIT can be described as marginal. The VAIT does not adopt the requirements for outsourcing relationships presented by the ZAIT in Chapter 9 and thus follows the "default" of the BAIT; the proximity of banking supervision to insurance supervision as well as the underlying supervisory objects manifests itself here. Apart from the additions identified and analysed in the text, in view of the contents in BAIT, VAIT and ZAIT, the question arises of a unification of the IT requirements into common sectoral IT requirements catalogue for banks, insurance companies as well as payment and e-money institutions with the then focused sector-specific additions in three sub-chapters of supervisory requirements for IT, subsumed into XAIT. This standardisation would be the first step towards a bundled IT supervision for all supervisory objects and thus towards a concentration of the forces of BaFin and the Bundesbank and the resulting increase in the technical expertise and personnel strength of the audit. The supervisory objects themselves would have the advantage of an improved audit situation in terms of duration and quality of the audit. XAIT would also provide the sector with a good technical basis for developing a national implementation circular for the upcoming DORA[4] .

[4] Digital Operational Resilience Act

Author

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

Mail: waldemar.grudzien@core.se

Nadine Hofmann is Expert Manager at CORE. She graduated in aerospace engineering in Braunschweig and Dresden. Her consulting expertise focuses on technical data protection and information security (focus on IAM, SOC/SIEM, management of risks, ISO27001 and GDPR). She supports clients in structuring and setting up financial compliance systems. She holds the position of a Deputy ISO.

Mail: nadine.hofmann@core.se

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

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

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

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

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