CORE®

BANKING SUPERVISORY REQUIREMENTS FOR IT (BAIT) HAVE ENTERED INTO FORCE FOLLOWING PUBLICATION BY BAFIN

Christian Everts
Holger Friedrich
Dr. Waldemar Grudzien

November 2017
COREtechmonitor | Blogpost

Key Facts

- BAIT entered into force on November 6, 2017, with minor amendments compared to the consultation status in June 2017
- Principles-based approach and proportionality principle in line with MaRisk, MaComp, and MaSan
- Scope for possible amendments thanks to modular structure
- Role of IT security officers strengthened
- BSI (German Federal Office for Information Security) and BaFin still reviewing the option of incorporating a critical infrastructure module into BAIT; BAIT highly likely to serve as a template for Insurance Supervisory Requirements for IT (VAIT)

Report

Summary of BAIT

Just like the Minimum Requirements for Risk Management (MaRisk) applicable to banks, the latest version of which BaFin published in late October, BAIT also interprets the legal requirements of Sect. 25 (1) Clause 3 (4) and (5) of the German Credit Act (Kreditwesengesetz). BAIT serves as a regulatory explanation of what constitutes suitable technological/organizational specifications for IT systems, paying particular regard to information security requirements and an appropriate disaster recovery plan. In light of the growing share of IT services provided by third parties, particularly as part of functional outsourcing, BAIT serves to flesh out the requirements of Sect. 25b of the Credit Act.

By means of BAIT, BaFin is making it clear to institutions what it expects in terms of robust supervision. In order to maintain the proportionality principle – i.e. consideration of the different risk situations of banks according to size, business model, and appetite for risk, for example – the requirements are formulated in a principle-based way. Therefore, technological neutrality is also preserved (the objective is specified, not how to get there): Institutes have to observe "current standards" and "factor in" the state of the art.

Its modular structure affords the flexibility necessary for amendments or additions that may be required in the future; by its very nature, an IT-related regulatory framework is not exhaustive. For example, a review is currently being carried out as to whether amendments are required in light of the implementation of "G7 fundamental elements of cybersecurity." Moreover, work is being carried out in conjunction with the German Federal Office for Information Security (BSI) as to whether a special "critical infrastructure" model (KRITIS) needs to be developed and incorporated into BAIT. This module would only contain the requirements necessary for critical infrastructure operators in the financial and insurance sectors as per Sect. 2 (10) of the Act on the Federal Office for Information Security in order to satisfy the applicable provisions of said Act.

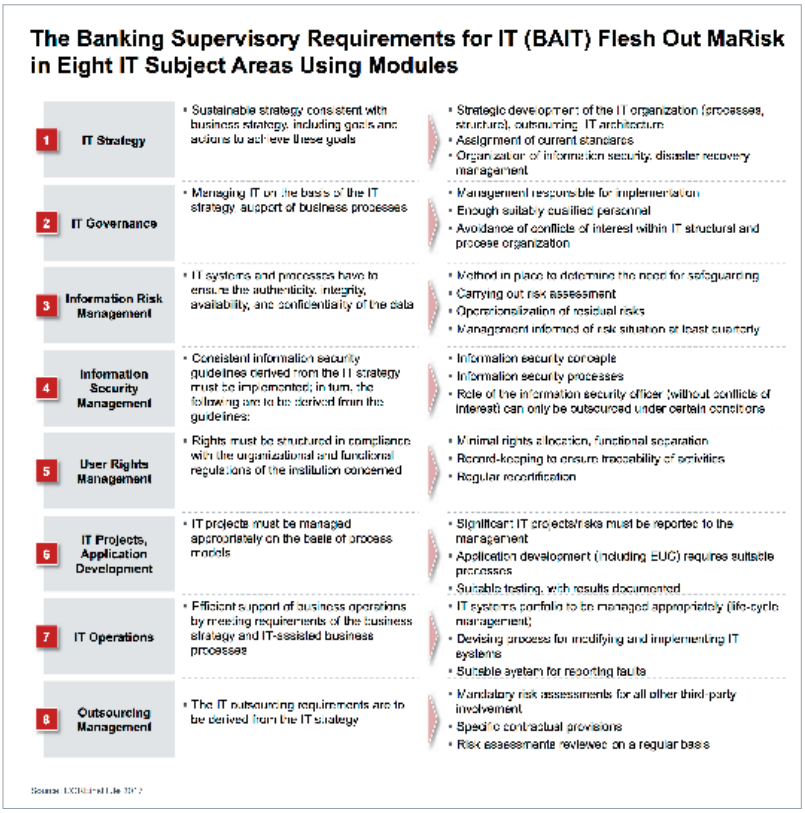

Figure 1: BAIT comprises eight modules

Special Topics

Role of IT Security Officers Strengthened

BAIT considerably strengthens the role of IT security officers, who are now finally on the same level as second-line risk functions.

BaFin is also fleshing out the requirements connected with the outsourcing of IT security officers, who will now only be eligible for outsourcing within specific group or association structures, or at small institutions without their own IT infrastructures (although a responsible contact has to be named in instances where they are outsourced within institutions).

Evaluating the Integration of a Critical Infrastructure Module

It is the opinion of the authors that BAIT contains all significant IT-related security requirements for banks and – by virtue of the proportionality principle, the principle-based approach, and, last but not least, the modular structure – the necessary structural flexibility to accommodate future amendments. In our view, there is no need for any further requirements in the shape of a critical infrastructure model that would transfer the requirements of MaRisk and the German IT Security Act (IT-Sicherheitsgesetz) into BAIT.

Furthermore, any harmonization would be difficult on account of the differences. The IT Security Act sets out two main requirements: the attainment of a minimum security standard and notification of any serious IT security incidents. It addresses all operators of critical infrastructures, i.e. a larger group than financial institutions, and imposes set thresholds, with operators who exceed these thresholds falling within the scope of the Act. By contrast, BAIT sets out a minimum security standard through the eight modules and the need to observe the state of

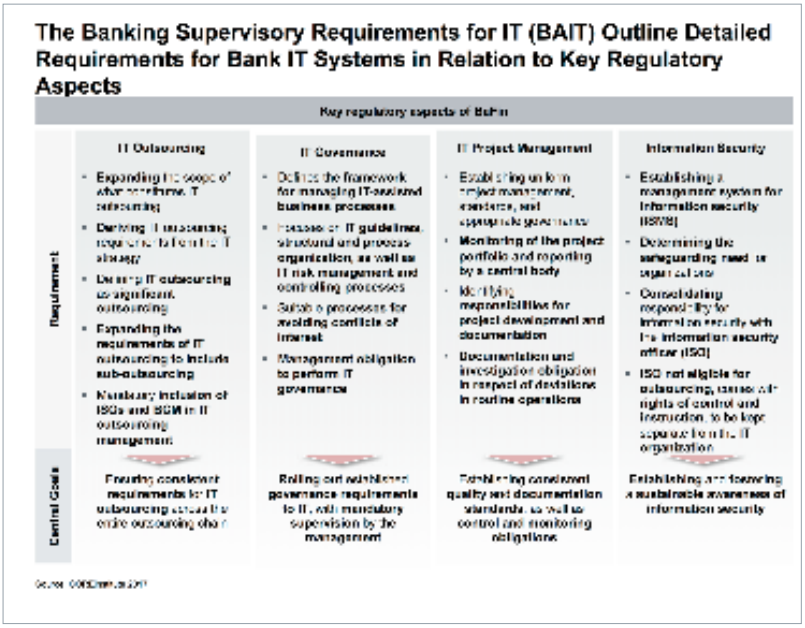

Figure 2: Key regulatory aspects of BAIT

the art; furthermore, it includes no reporting mechanism, as this is already provided for in the banking sector by means of MaSI and its successor PSD II.

As BAIT is applicable to banks, whereas the IT Security Act pertains to infrastructures identified as critical, this raises the question of how both regulatory systems can be unified in a single BAIT critical infrastructure model and how this should be drafted in practice. Would it even be possible for a non-critical bank (as per the IT Security Act) to drift into the scope of IT Security Act regulation through the back door as a result of BAIT, which is applicable to all banks?

How would the different threshold regimes as per BAIT (proportionality) and critical infrastructure regulation (set thresholds) be combined? When you consider the seven-year development period of the IT Security Act (including the B3S sector-specific security standard), these initial questions already give an idea of how long the development and implementation of a critical infrastructure module could drag on for. Two stable regulatory frameworks in the shape of BAIT and the IT Security Act are better for all market players than any attempt to unite both regulatory systems in a BAIT module.

It can be assumed that strong political influence is being exerted by the stakeholders involved, the Federal Ministry of the Interior (for the Federal Office for Information Security) and the Federal Ministry of Finance (for the Federal Financial Supervisory Authority). Specialist knowledge and technical evaluation are taking a step back as politically motivated regulatory costs rise.

Assessment of the Model Status of BAIT for Corresponding Insurance Requirements (VAIT)

In the fourth quarter of 2017, BaFin once again used the proven approach of a specialist committee to begin work on developing Insurance Supervisory Requirements for IT (VAIT).

Even for the sake of equal treatment alone, BaFin has to apply the same requirements to insurance companies as it does to

banks. Furthermore, the business models of both types of institution are based on the collection and processing of sensitive data, which, as a result, has to be handled securely by banks and insurers alike. In light of the chain of banking regulation comprising the Credit Act (Sect. 25a), MaRisk and BAIT, the regulatory chain for insurance would have to comprise Sect. 23 (1) of the German Insurance Supervision Act (Versicherungsaufsichtsgesetz), MaGo and VAIT. When you also consider that MaGo (Supervisory Minimum Requirements on the Business Organization of Insurance Companies) deals with the issue of IT to much less of an extent that MaRisk, it is possible to come to the converse conclusion that VAIT may contain (even) more statements on the topic of IT than BAIT. With a questionnaire entitled "Questions on handling cyber risks," which all insurers had to respond to by November 3, BaFin is, on the one hand, getting a picture of the facilities and capabilities of insurers' IT systems in terms of information security; on the other hand, they are closing the delta between MaGo and MaRisk.

Therefore, it can be assumed, first of all, that VAIT will adopt the eight-module structure of BAIT and, secondly, that it will contain far more IT content than BAIT. The transfer of the high regulatory standards of banking IT to the IT systems of insurance companies has already been partly initiated. This honors the significance of insurance as an IT-based industry and, consequently, the relevance of insurance companies as an economic factor.

Conclusion

As with the consultation for the MaRisk amendment, the BAIT consultation period lasted about 18 months. This length of time reflects the regulation's high degree of complexity and seems to be establishing itself as the "standard" time frame for solid regulation. After all, it can be assumed that the regulatory framework is a sophisticated one that can withstand market needs.

The final published version of BAIT is to be welcomed without reservation. Although a fleshing out of the regulations concerning cloud services would have been desirable, and although the joint BSI and BaFin review on the possible integration of a critical infrastructure module within BAIT should, in our view, be ended (as the redundancy and mixing of different regulatory regimes will not lead to enhanced regulation and supervision), this does not diminish the strength of the structure, the structural openness, or the content. With BAIT, the regulator has also created a template for VAIT and, moreover, for all supervisory areas and entities that fall within BaFin's remit.

Sources

INTERNET:

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1710_BAIT_anschreiben.html

PREVIOUS POSTS IN THE SERIES

COREinstitute 2016/2017

https://www.coretechmonitor.com/de/marisk-novelle-der-bafin-final-veroeffentlicht/

https://www.coretechmonitor.com/de/schwerpunkte-der-aufsicht-und-pruefung-der-bank-it-informationsveranstaltung-it-aufsicht-der-bafin/

https://www.coretechmonitor.com/de/it-sicherheitsgesetz-neue-anforderungen-an-kritische-betreiber/

NEWSPAPER:

BÖRSEN-ZEITUNG, SEPTEMBER 28, 2017, “SUPERVISORY BODY LOOKS AT REGTECH”

Authors

Christian Everts is a Transformation Manager at CORE and is particularly experienced in the field of regulation. Prior to joining CORE, Christian worked for several banks as a compliance manager, where he primarily implemented regulatory requirements in German and international investment and universal banks.

Mail: christian.everts@core.se

Christian Everts

Holger Friedrich has been in charge of our consulting unit since 2010. He was one of the founding members of the Institute for Theoretical Computer Science at the University of Potsdam (HPI). Before founding CORE, he set up a technology company and was a partner in a leading international strategic consulting firm**.**

Mail: holger.friedrich@core.se

Holger Friedrich

Dr. Waldemar Grudzien is a Transformation Engineer at CORE and focused on the security regulations of the financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial industries he was a specialist for retail banking and banking technologies. He graduated in electrical engineering at the TU Berlin.

Mail: waldemar.grudzien@core.se

Dr. Waldemar Grudzien

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae