BaFin's Supervisory Requirements for IT in Financial Institutions

German financial services supervisor clarifies supervisory requirements on IT systems, processes and governance in financial institutions

This Client Alert is part of series of briefings on supervisory guidance on conduct of business and organizational requirements in the financial services sector issued by the German Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin). Please see our further coverage on inter alia "The German BaFin's changes to MaRisk and the impact on market participants" and the "Revised MaComp" on our Eurozone Hub website.

BAIT as "core component" for IT supervision in the financial services sector

The rapidly expanding provision of IT-based financial services as well as banks' and financial institutions' increasing internal reliance on IT processes put new challenges on supervisors. To keep pace with this development, the BaFin has introduced a range of supervisory measures.[1]

Amongst them and as "the core component for IT supervision of all credit and financial institutions in Germany",[2] the BaFin has published the Circular on Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT) at the beginning of November 2017.[3] The BAIT clarifies the supervisor's expectations for firms' compliance with the requirements on secure IT systems and associated IT processes (as regard the integrity, availability, authenticity and confidentiality of data) as well as on IT governance.[4]

Significant impact

Though the BAIT does not set forth legally binding requirements, it specifies the BaFin's expectations on compliance with IT requirements in financial institutions. In this regard the BAIT has a significant impact on the market: In-scope firms will want to implement and adhere to the principles-based requirements of the BAIT as non-compliance might bring them into the supervisor's focus. This is even more true as the BaFin stressed in its letter to the associations (Anschreiben an die Verbände), which accompanied the publication of the BAIT, that IT governance and information security are of "equal importance" as firms' compliance with capital and liquidity.[5]

Irrespective of the BAIT's significance for the local German financial services sector, the BAIT is likely to also impact on the further development of supervisory requirements for IT in financial institutions on an EU scale. In this regard, the BaFin has already announced in the January 2018 edition of its monthly journal, that it will "actively put forward in the discussion" the BAIT as regards the planned EU-wide harmonization of requirements on the management of IT risks.[6]

Scope

The BAIT further details statutory requirements of the German Banking Act (Gesetz über das Kreditwesen (Kreditwesengesetz – KWG)) on the proper business organization (ordnungsgemäße Geschäftsorganisation) of institutions and the outsourcing of activities and processes from an IT point of view.[7] As the BAIT builds on the BaFin's Circular on Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – MaRisk), which itself further details (amongst others) IT requirements of the KWG, the BAIT and the MaRisk must be read together. For further information on the 2017 updates to the MaRisk please see our Client Alert which forms parts of this briefing series.[8]

1 The BaFin has also established a separate organizational unit for IT supervision in the financial services sector within the BaFin (Group IT Supervision / Payment Transactions / Cyber Security). This unit is directly attached to the BaFin's Banking Supervision Division.

2 See BaFin Journal, January 2018, p. 17.

3 The original German text of the BAIT is binding. However, the BaFin has also provided an English version of the BAIT for information purposes on its website. The BAIT was prepared with the help of the BaFin IT Expert Panel (Fachgremium IT). Further, the final version of the BAIT takes into account a lot of comments from market participants during the consultation phase of the (draft) BAIT.

4 See BaFin's letter to the associations from 6 November 2017.

5 See BaFin's letter to the associations from 6 November 2017.

6 See BaFin Journal, January 2018, p. 21.

7 See sec. 25a para. 1 sent. 3 no. 4 and 5 and sec. 25b KWG.

8 Client Alert „The German BaFin's changes to MaRisk and the impact on market participants", downloadable at dentons.com/en/EurozoneHub.

The close link between the MaRisk and the BAIT is also apparent in that both Circulars have the same intended recipients: In-scope firms include (inter alia) credit and financial institutions within the meaning of the KWG[9] as well as German branches of third country firms providing banking business or financial services in Germany (third country branches).[10] The scope further e.g. extends to branches of German credit or financial institutions carrying out business internationally. Explicitly excluded from the MaRisk's and the BAIT's application are German branches of EEA firms which make use of the European "passport" for providing banking business or financial services in Germany.[11] For those firms relocating operations to Germany as a result of Brexit or otherwise, the BAIT will apply to them regardless of whether such a firm sets up a third country branch"[12] in Germany or, as is more likely, a fully standalone subsidiary.

Subject areas – an overview

The BAIT further details requirements on the following subject areas:

IT strategy

The management board must define an IT strategy that is consistent with the institution's business strategy and contains (at least) the minimum requirements specified in the BAIT. Amongst others, these requirements include the strategic development of the institution's organizational and operational structure of IT and of the outsourcing of IT services, the responsibilities and integration of information security into the organization and the strategic development of the IT architecture.

IT governance

In scope-firms must provide for a structure to manage and monitor the operation and further development of IT systems including related IT processes on the basis of the IT strategy (IT governance). As part of this, the institution must ensure e.g. that appropriate staff are available for information risk management, information security management, IT operations and application development (in particular) and that conflicts of interest and activities that are not compatible with each other are avoided within the structure of IT.

Information risk management

As part of information risk management, institutions must set up a catalogue of target measures which specifies and suitably documents the institution's requirements for implementing the protection objectives ("integrity", "availability", "confidentiality" and "authenticity") in the various categories of protection requirements.

The BAIT further specifies the requirements on the risk analysis and the reporting to the management board on information risks.

Information security management

It is the management board's responsibility to agree an information security policy and to communicate this within the institution. The information security policy should serve as the basis for more specific information security guidelines and processes in the institution.

Further, an independent "information security officer function" must be established within the in-scope firm's organization. The information security officer is responsible for all information security issues within the institution and with regard to third parties and must report to the management body on the status of information security regularly, at least once a quarter, and on an ad hoc basis. Under certain conditions regionally active institutions and small institutions can appoint a joint information security officer.[13]

User access management

Under the BAIT, user access management should be based on user access rights concepts. By way of technical and organizational measures institutions must ensure that circumvention of the requirements contained in the user access rights concepts is excluded. The processing of access rights (setting up, changing etc. of access rights) must be documented "in a way that facilitates comprehension and analysis".

IT projects and application development

Institutions must establish an organizational framework for IT projects and manage IT projects (including the IT project portfolio in its entirety) appropriately. Major IT projects and IT project risks are subject to reporting to the management body (regularly and on an ad hoc basis).

Further, institutions must base their application development on defined and appropriate processes. Appropriate arrangements must ensure that after the application goes live the confidentiality, integrity, availability and authenticity of the data to be processed are comprehensively assured. Applications must be tested on the basis of a defined testing methodology.

IT operations

The BAIT further contains specific requirements for IT operations. Institutions must e.g. manage the portfolio of IT systems appropriately and set up processes for changing IT systems taking account of their nature, scale, complexity and riskiness. Further, the BAIT specifies inter alia the processing of change requests for IT systems and the setting up of a data backup strategy.

Outsourcing and other external procurement of IT services

Under the BAIT, risk assessments must be conducted prior to each instance of "other external procurement of IT services". According to the MaRisk Interpretative Guide (Auslegungshilfe) "other external procurement of IT service" does not qualify as "outsourcing" within the meaning of the MaRisk. It covers e.g. the one-off or occasional external procurement of goods

9 See sec. 1b KWG.
10 See sec. 53 para. 1 KWG.
11 See MaRisk, module AT 2.1 and BAIT, I. Preliminary remarks point 4.
12 See sec. 53 para. 1 KWG.
13 See BAIT, Interpretative Guide, p. 10.

and services, the procurement of services which is typically arranged by the institution (typischerweise bezogen) and which cannot be provided by the institution itself (neither at the time of external procurement nor in future) due to factual circumstances or legal requirements.[14] Further, institutions' risk assessments are subject to the requirement of review and amendment (on a regular and ad hoc-basis) by the institutions.[15] As regards contractual arrangements with external IT service providers institutions must further take "appropriate account of the measures derived from the risk assessment relating to other external procurement of IT services".

In light of the BAIT, institutions should prudently review and, where necessary, amend their IT arrangements and processes. Apart from the purely technical side, the BAIT's impact on institutions' general organizational set-up and governance arrangements must be analyzed and necessary amendments made. In this regard, particular focus should be on the establishment of the information security officer function. With the requirement of at least quarterly reporting to the management board the BAIT underlines the significance of this function within institutions' internal control framework.[16]

Further, the BAIT emphasizes once more the necessity that the management board displays the required IT competency and assumes the ultimate responsibility for financial institutions' compliance with the supervisory requirements on IT.

Outlook and next steps for in-scope firms

The BAIT provides practical guidance on the BaFin's expectations for compliance with IT requirements in financial institutions. For smaller firms, however, it might be difficult to identify which provisions allow for a flexible or simplified implementation.[17] This is even more challenging as the Circular does not provide for a transitional period.[18]

Further, institutions must take into account that the BAIT and the MaRisk do not compile the supervisory expectations for compliance with the requirements for IT in financial institutions in an exhaustive way. In this regard, the BAIT explicitly states that "the depth and scope of the topics addressed in this Circular is not exhaustive" and that "institution(s) shall continue to be required to apply generally established standards to the arrangement of the IT systems and the related IT processes in particular over and above the specifications in this Circular".[19] Further, specific IT requirements are set forth in various other pieces of financial regulation (e.g. the Markets in Financial Instruments Directive II and the Payment Services Directive II as well as local and EU implementing law). Besides this, EU and national regulators provide guidance on the application of IT requirements in different fields.[20] In addition to the on-going supervisory dialogue, the European Central Bank is currently in the process of issuing uniform requirements and guidance on the management of IT risks for major banks.[21]

In scope-firms should also take into account that the BaFin plans to supplement the BAIT by further modules specifying requirements on IT emergency management including testing and recovery procedures (IT-Notfallmanagement inklusive Test- und Wiederherstellungsverfahren). The German regulator further considers adding a new module to the BAIT for the providers of critical infrastructures (Betreiber Kritischer Infrastrukturen).[22]

As a result, firms that are within the scope of the BAIT will need to carefully identify and compile the IT requirements applicable to them as a result of the BAIT and multiple other requirements stipulated in EU and local regulation as well as supervisory guidance. Moreover, in-scope firms may want to review and update their IT arrangements, project governance policies and procedures to ensure that justifications for certain actions and compliance measures can be evidenced and explained to supervisors.

Author:

Dr. Katja Michel
Senior Associate
Frankfurt
D+49 69 45 00 12 272
katja.michel@dentons.com

Should you wish to continue the conversation on the subjects raised herein, please do get in touch with any of our Eurozone Hub key contacts on the next page.

[14] See MaRisk Interpretative Guide, p. 33.
[15] Together with the contractual details, where appropriate.
[16] By way of comparison, under the MaRisk the compliance function must report to the management board at least annually (see MaRisk, module AT 4.4.2 point 7).
[17] The BAIT enables the application of the principle of dual proportionality.
[18] According to the BaFin, a transitional period is not set forth as the BAIT only clarifies pre-existing requirements.
[19] See BAIT, I. Preliminary remarks point 2; as regards these standards, the BAIT explicitly mentions the IT Baseline Protection Manuals (Grundschutz) issued by the Federal Office for Information Security (BSI).
[20] See e.g. the European Banking Authority's „Recommendations on outsourcing to cloud service providers" from 20 December 2017 and Consultation Paper on "Draft Guidelines on Outsourcing Arrangements" from 22 June 2018.
[21] See Börsen-Zeitung from 7 June 2018, issue 106, p. 3.
[22] See BaFin Journal, January 2018, p. 21.

Our Eurozone Hub Contacts:

Michael Huertas
Partner
Frankfurt
D +49 69 45 00 12 330
michael.huertas@dentons.com

Dr. Markus Schrader
Counsel
Frankfurt
D +49 69 45 00 12 362
markus.schrader@dentons.com

Dr. Katja Michel
Senior Associate
Frankfurt
D+49 69 45 00 12 272
katja.michel@dentons.com

CSBrand-9774-Client Alert Bait_04 — 25/06/2018