CORE®

BAFIN'S FINAL VERSION OF THE AMENDMENT TO MINIMUM REQUIREMENTS FOR RISK MANAGEMENT HAS BEEN PUBLISHED

Christian Everts
Dr. Waldemar Grudzien

October 2017
COREtechmonitor | Blogpost

Key Facts

- Details of requirements concerning risk reporting for all credit institutions and integration of the requirements stemming from BCBS 239 for system-relevant institutions regarding Minimum Requirements for Risk Management (MaRisk) finalized
- Requirements honed for a risk culture specific to credit institutions
- Refining current requirements for risk management, especially regarding IT risk management
- Finalizing organizational and management requirements for outsourcing
- Amendment to Minimum Requirements for Risk Management (MaRisk-Novelle) come into force following publication

Report

I. Finalizing requirements for risk management

Following the implementation of the Basel Standard 239 (BCBS 239) in AT 4.3.4, the requirements concerning data aggregation and risk reporting for system-relevant credit institutions have now also been included in the Minimum Requirements for Risk Management (MaRisk).

Furthermore, the German Financial Supervisory Authority (BaFin) is also reviewing the requirements of risk reporting for all credit institutions by consolidating the requirements of risk reporting in the revised BT3 MaRisk.

According to the principle of proportionality, smaller credit institutions do not have to abide by the extensive requirements of AT 4.3.4. They can direct risk reporting to their commercial needs.

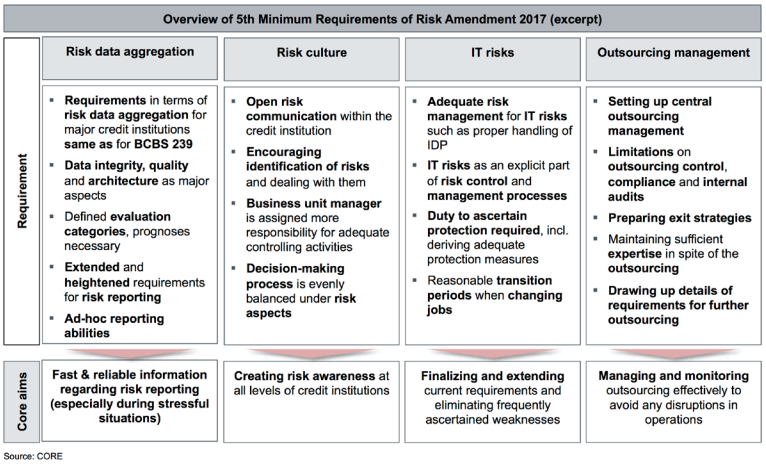
II. Establishing an appropriate risk culture

BaFin is implementing the requirements for an adequate risk culture in MaRisk proposed by the Financial Stability Board (FSB) in 2014 as part of its “Guidance on Supervisory Interaction with Financial Institutions on Risk Culture” by revising the AT 3 and AT 5.

A significant aspect here was that BaFin considers management, executives and the established decision-making processes to represent the key parameters of risk culture, meaning that management and executives have to set an example as far as the requirements for an effective risk culture are concerned.

It should be noted here that BaFin is very much aware of the problem of quantitative measurability of a risk culture that is predominantly based on purely qualitative aspects. However, it considers risk culture as a key tool in risk management and, accordingly, will get an idea of how this tool is implemented during regulatory practice.

Changes to Minimum Requirements for Risk (MaRisk) following the recently approved 5th MaRisk Amendment focusing on four aspects



Source: CORE

III. New: Key focus on managing IT risks and data

Furthermore, BaFin is heightening and finalizing the requirements concerning IT risk and data management by including specific additions.

As a result of AT 4.3.1. MaRisk, BaFin is not only finalizing the requirements of adequate cooling-off periods for persons taking up new positions within the organization, it is also setting out the details of requirements regarding IT authentications as well as putting them under regular scrutiny.

As regards IT risks, BaFin is also analyzing the finite details in AT 7.2.; IT risks are considered to be an explicit part of risk control and the management process, individual data processing shall be put extensively on par with standard applications, and thus equipped with adequate IT risk management and the task of making sure protection needs are ascertained.

IV. Details of requirements for outsourcing

The regulations most frequently discussed during the consultation phase are how to handle outsourcing.

By revising AT 9 MaRisk, BaFin is reacting to shortcomings which were specified during checks made as part of their regulatory activities.

Whilst very few would be surprised to hear that major credit institutions are not allowed to outsource risk functions completely according to the principle of proportionality, the requirement to set up a central outsourcing management represents a major reform. In future, outsourcing will therefore no longer be solely made based on the regulations and checks undertaken by the outsourcing department. Instead, outsourcing will also have to satisfy harmonized corporate standards.

In the future, it is likely that particular emphasis will be put on differentiating between miscellaneous external procurement and outsourcing in respect of banking software.

BaFin generally defines every purchase of software as a miscellaneous external procurement, but basically excludes software which is used to carry out essential banking tasks or which identifies, assesses, controls, monitors and communicates risks from this definition.

According to its own statement, BaFin has, in this respect, pragmatically solved the controversies associated with these topics. Furthermore, BaFin requires either external support services or the software to be operated by an external service provider for the purposes of outsourcing.

This definition chosen by BaFin should indeed lead to a further need for finalizing the details, especially as regards the trend to operate standard software using Software as a Service (SaaS) solutions and the increased requirements associated with outsourcing.

Consequently, classifying as outsourcing does not only result in the obligation to ensure sufficient expertise is available for the outsourced process (which is required in order to ensure that the process can be continued seamlessly in the case of the circumstances surrounding the outsourcing being terminated).

By making the requirements of further outsourcing more precise, not only will the areas to be outsourced and, possibly, central access management be faced with new challenges, the entire outsourcing chain must be incorporated into the verification and control process in the future.

V. Amendment comes into force

Following the lengthy consultation phase, and as many regulations and detailed information are based on regulations and standards which have already been established at a European legislative or international level, the Amendment to Minimum Requirements for Risk Management is now in force. Nevertheless, BaFin has granted an implementation period for new requirements until October 31, 2018, insofar as credit institutions are not otherwise already required to abide by regulations (which form an integral part of this Amendment).

Conclusion

The consultation phase of the Amendment of Minimum Requirements for Risk Management has lasted for one-and-a-half years. As far as the authors are concerned, this is too long a time period from the ever-present digitalization needs such as Brexit activities, during which items subject to regulatory supervision have to adapt their IT expertise “in view“ across the non-stable supervisory guidelines. As such, the Amendment now in force can be welcomed with open arms as being reliable supervisory practice.

Finalizing the details of requirements for information technology are now keenly awaited by means of the “Requirements of Banking Regulatory Authorities for IT” (BAIT). Furthermore, the tandem supervision of the credit institutions BAIT/MaRisk is likely to release immense charisma for the supervisory practice of insurance companies. Here, BaFin intends to transfer the supervisory system to insurance companies.

The first steps in this direction were taken at the beginning of the year with the “minimum supervisory requirements for the business organization of insurance companies“(MaGo). Preparations for a VAIT, which stands for supervisory requirements in the insurance industry on IT, are expected to start in November with an expert committee especially set up for the task. BaFin had already sent out a questionnaire to all insurance companies containing “Questions related to dealing with cyber risks” in order to assess the status of information security. This was due to be returned by November 3rd.

The widespread and in-depth work carried out by BaFin concerning IT supervision underpins the threshold of information-technology for all sectors of the finance industry (which has since been attained). The credit institutions were first on the agenda, and work is now centered around the insurance industry. Other sectors and objects of supervision under BaFin are likely to be next on the list soon.

Source

MaRisk-Novelle der BaFin

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

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