# The German BaFin's changes to MaRisk and the impact on market participants

大成 DENTONS

## How does the 'new' MaRisk shift the tone of regulatory and supervisory engagement?

In the EU, conduct of business rules and organisational rules, including principles of how risk and compliance functions should operate are contained in various pieces of sectoral legislation[1]. These in turn are often supplemented by European Supervisory Authorities' (**ESA**s) rulemaking as well as in a number of jurisdictions, including Germany, rules set out by national competent authorities (**NCA**s) which supplement or expand on EU-level rules.

In Germany, the conduct of business and the organisational rules applicable to financial services are set out in statutory legislative instruments (in particular in the German Banking Act (*Kreditwesengesetz* – **KWG**) and the German Securities Trading Act (*Gesetz über den Wertpapierhandel* – **WpHG**)) and are further detailed in supervisory guidance such as the Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* – **MaRisk**) and the Minimum Requirements for the Compliance Function (*Mindestanforderungen an die Compliance-Funktion*[2] – **MaComp**). The German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*, the **BaFin**), as the conduct of business regulator in Germany is the regulatory gatekeeper for MaRisk and supplemental guidance. The MaRisk was updated by publication of an administrative 'Circular' that took effect from 27 October 2017[3] and introduces some important changes. The new version of MaRisk allows a one year transition period for those rules which are substantial and thus go beyond mere clarifications[4].

In summary, even if the EU is in charge of finalising its "Single Rulebook for financial services" and even though the NCAs cooperate with the ESAs to form the European System of Financial Supervision (**ESFS**), MaRisk still sets a distinct tone and one that complements obligations set in the EU's MiFID II/MiFIR Framework. What happens in the German NCA mandate may also have wide-reaching impacts on a range of "run the business" and "change the business" workstreams for a breadth of market participants already active in or looking to establish themselves in Germany. Some of the practical impacts of those changes at the German level and how they interoperate with those at the EU-level are discussed herein.

MaRisk was last updated in 2012. At the time of writing, only the German language version of the 27 October 2017 Circular[5], the 2017 MaRisk[5] as well as the Annexes thereto[7] are the binding versions. An (informal) English language version has yet to be published. Some of MaRisk's concepts and/or the prescriptive detail of contents and/or the supervisory guidance may go beyond principles embedded in other EU or national rules. As a result, MaRisk may - although it largely derives from common principles - be rather unfamiliar for a range of firms and thus may mark a change in supervisory culture.

1 Such as the MiFID II/MiFIR Framework as well as the CRD IV/CRR Framework.

2 Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzanforderungen – MaComp

3 See: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_anschreiben_pdf_ba.pdf;jsessionid=000DF83270261DDB9422C06E5D99C00A.2_cid363?__blob=publicationFile&v=4

4 A three year transition period applies for the application of module 4.3.4 (requirements on data management, data quality and the aggregation of risk data); however, the BaFin clarified in its accompanying letter to the associations of the credit sector *(Anschreiben an die Verbände der Kreditwirtschaft)* that globally systemically important financial institutions do not benefit from this transition period as they already have to abide by these requirements since January 2016.

5 See: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_anschreiben_pdf_ba.pdf?__blob=publicationFile&v=4

## MaRisk's structure, its place in Germany and its interoperability with EU-level requirements.

MaRisk was developed by the BaFin with the aim to communicate BaFin's supervisory expectations applicable to in-scope financial institutions (in particular, credit institutions and other financial institutions) regarding their risk management arrangements and compliance with the German Banking Act. BaFin considers that MaRisk provides a "...principles-based framework that gives institutions the flexibility to implement solutions individually. Moreover, the MaRisk contains numerous opening clauses which ensure that smaller institutions can also comply with the requirements in a flexible way." That approach exists in other jurisdictions, as well.

MaRisk applies to financial institutions, such as those engaged in the banking or asset management sector, as well as MiFID investment firms. Its scope extends to entities within Germany as well as to institutions headquartered in Germany carrying out business internationally. By way of example, it applies to a German headquartered firm conducting business in the United Kingdom or the United States. By contrast, MaRisk does not apply to German branches of EU headquartered institutions i.e., it does not apply to a French firm's Frankfurt branch, whereas it does apply to a German subsidiary of an EU headquartered institution.

MaRisk, whilst a core component of BaFin's supervisory approach and rules, is not the only "Circular" that communicates compliance expectations and which sets relevant minimum standards (*Mindestanforderungen*). In short, other "Ma's" matter as well, in particular MaComp. The latter details for investment firms[8] conduct of business, organisational and transparency requirements and sets minimum expectations on the design of the compliance function. The MaComp has undergone a number of amendments. The latest version was published on 19 April 2018 as part of the implementation of MiFID II into German law[9]. As a result, market participants subject to both the MaRisk and the MaComp (e.g. CRR credit institutions, which provide both banking business and investment services to customers in Germany) need to comply with the requirements under the MaRisk as well the MaComp (the applicable rules depend on the specific business model) and then also Banking Union specific rules.

Moreover, the insurance sector has its own BaFin Circular referred to as "MaGo"[10]. In addition to sector-specific Ma's, the MaRisk should also be read in the context of cross-sectoral Ma's such as the BaFin Circular (*Rundschreiben 10/2017 - Bankaufsichtliche Anforderungen an die IT*) Regulatory Requirements for Bank IT systems (**BAIT**)[11] as well as ESA publications covering the same supervisory principles.

The 2017 MaRisk changes have left the core modular structure of how rules are presented unchanged. It is comprised of a:

- General Section (*Allgemeiner Teil* - the AT Modules) which contains basic requirements for internal risk management including outsourcing standards; and
- Special Section (*Besonderer Teil* - the BT Modules) which specifies qualitative criteria on the organisation of internal control systems (including compliance and risk functions) for particular types of business and types of risk as well as the organisation of the internal audit function. The BT Modules are further split between (i) rules that relate to the organisational and operational structure of the credit business i.e., lending as well as trading (BTO) and (ii) rules that relate to relevant risk types (BTR). The BT Modules should also be read in conjunction with MaComp and BAIT.

With the "Europeanisation" of banking sector supervision in the Eurozone and the creation of the Banking Union, a number of firms that fall within the scope of BaFin's rules are also subject to competing requirements set by other authorities, including the ESAs and/or the European Central Bank in its capacity as supervisory authority within the Banking Union (the **ECB-SSM**). Firms will want to consider how MaRisk interoperates with Banking Union specific rules.

Irrespective of how and to whom MaRisk applies, all financial services providers will want to consider how the domestic rules and the domestic supervisory engagement interoperates with the BaFin and/or will be shaped by EU-level regulation and supervision along with the rulemaking and guidance issued by the relevant ESAs and/or other components of the ESFS. There are a number of instances where supervisory expectations and requirements may conceptually diverge, even where they cover the same thematic area or where there are different compliance standards altogether.

---

6 See: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html

7 Comprised of:

- Annex 1: which provides comments and guidance to the terms of MaRisk : https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5 ; and
- Annex 2: which provides a deltaview showing changes made in the MaRisk October 2017 version compared to the 14 December 2012 version as well as changes made to the comments and guidance to MaRisk that are set out in Annex 1.

8 See module AT 3.1 for all entities subject to the MaComp.

9 See our dedicated coverage on this development.

10 See: Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen. MaGo which entered into force on 1 February 2017 and complements the German Insurance Supervisory Act as well as EU legislative requirements and ESA Guidelines.

11 See our dedicated coverage on this development.

## What is new about MaRisk 2017 and why does it matter?

BaFin has redrafted large parts of both wthe AT Modules as well as the BT Modules. It has introduced a major overhaul to AT Modules 4.3.1 (Organisational and operational structure) and AT 4.3.2 (Risk management and risk control processes). Part of those changes are aimed at aligning these provisions with EU level legislative requirements but also with the supervisory principles and expectations of the ESAs already communicated to market participants.

Moreover, the BaFin introduces a wholly new AT Module 4.3.4 (Data management, data quality and aggregation of risk data) as well as BT Module 3 (Risk Reporting). It is worth noting that these thematic areas of governance and control as well as data management and quality are also on the ECB-SSM's supervisory priorities for 2018 as well as the Supervisory Review and Evaluation Process (**SREP**)[12]. Overlaps are flagged below. Annex 2 to MaRisk and the deltaview of changes provide an exhaustive overview of the relevant changes. Some of those changes are highlighted in the Annex hereto. The key changes introduce new or updated rules in respect of:

- New rules on data aggregation - these rules apply only to systemically important institutions, designated in accordance with the KWG;
- New rules on risk reporting;
- Significantly updated rules on qualitative requirements and justifications on risk culture; and
- Tying in of MaRisk standards to EU and ESA level standards and expectations applicable to regulated outsourcing and delegation arrangements (notably the requirements to introduce a central outsourcing management process as well as limitations in respect of the outsourcing and delegation of the risk control, compliance and internal audit function(s) which must - subject to limited exemptions - remain within MaRisk relevant firms to the extent possible).

In summary, it might be advisable for certain financial services providers to consider conducting a supervisory "stocktake" and, as part thereof, conduct a self-assessment on their degree of compliance and/or potential need to take remedial action.

## How is MaRisk supervised in practice?

BaFin is the lead NCA in relation to conducting business supervision for most market participants in the financial services sector that are active in Germany. In relation to financial services providers operating under a German licence, the Deutsche Bundesbank shares certain supervisory responsibilities and may also express its own supervisory preferences. For those firms with a banking licence, and which fall within the supervisory mandate of the Banking Union, the ECB-SSM will lead on prudential supervisory matters.

In practical terms, this means that a financial services provider, irrespective of who in the ESFS leads its supervision, will be subject to multiple points of engagement on a periodic, ad hoc, thematic and at the very least annual basis to verify compliance with rules, principles and supervisory expectations are being adhered to. It is important to note that the BaFin has the power to issue administrative fines and impose supervisory sanctions for rule breaches and/or issue remedial action plans separate or in addition to those of its peers in the ESFS.

## Outlook in Germany and what's next from the EU level?

The regulation and supervision of financial services, including within the individual Member States of the EU, is increasingly moving towards a more harmonised application of the Single Rulebook built on a more uniform and "Europeanised" supervisory culture. The BaFin's actions, including in respect of the 2017 MaRisk changes, as one of the more active and larger NCAs in the ESFS is [de facto] helping shape that transition. Market participants and internal stakeholders as well as their professional advisers will need to remain cognisant of how best to navigate opportunities as they arise at all the relevant levels of supervisory engagement, where there are common trends and approaches but also divergences.

The ESFS' desired end-state of how financial services ought to be regulated is becoming increasingly clear and whilst the BaFin's supervisory expectations of compliance standards and remedial action are equally clearly communicated in MaRisk as well as the other Ma's, regulators' and supervisors' resourcing of supervisory staff is still an issue.

12 For a further discussion on this development please see our coverage from our Eurozone Hub here.

Viewed through the lens of firms and their supervisory engagement this may sharpen the tone as supervisory authorities are concerned with non-compliance happening "on their watch" but also having to do substantially more with less support with equally having to work with other ESFS members on supervisory convergence and increased cooperation. Irrespective of whether in-scope MaRisk firms are already on the ground or looking to move, the MaRisk 2017 changes and those of other Ma's as well as what may be on the horizon further ahead at the national and ESA driven level will matter to a wide range of stakeholders in supervised institutions.

## Annex - MaRisk 2017's changes in detail and the compliance impact

MaRisk 2017 will likely have a number of impacts for a wide range of in scope firms. These will differ in depth, breadth and severity across "change the business", "run the business" and/or "change the compliance" workstreams. They will evolve over time as the way MaRisk 2017 operates itself becomes subject to change as new or known rules in the pipeline come online, whether as a result of EU, ESA, Eurozone or German-specific rule changes. Some of the immediate issues from MaRisk 2017 are changes such as:

- new cross-references tying in rules in MaRisk that apply to systemically important credit institutions to those that are recognised, in accordance with Section 10f KWG as globally systemically important financial institutions and other systemically important institutions as defined in Section 10g KWG (together, for purposes herein, SIFIs). It is important to note that SIFIs at the global or EU level are likely to be SIFIs for purposes of the KWG, but that SIFIs determined solely in applying the KWG may not qualify as SIFIs for EU and global purposes. For those affected, to the extent they are not already taking preparatory action, this may mean rolling out institution and group-wide level changes to data collection, aggregation and use policy and much of this may require senior and/or board approval as well as specialists put in place in relation to running as well as checking those obligations;

- an amendment to ensure that the BAIT also applies to those firms to whom MaRisk applies to, which may thus, for a number of firms, translate into a range of IT policy and/or systems changes including in relation to outsourcing and delegation;

- an amendment inter alia to AT Module 3 (Joint responsibility of the management board members) and in particular the guidance notes to describe what the BaFin considers to be a "risk culture" (Risikokultur). In summary, firms are required to, and may need to conduct a self-assessment on their compliance and/or take remedial action to swiftly ensure they:

  - develop, promote and embed an appropriate risk culture within the relevant firm and its group. The BaFin expects that a "good" risk culture set standards and methods of how persons (ought to) act in identification and management of risk as well as the fact that decision processes lead to actions;

  - have senior and executive functions evidence a tangible commitment to risk sensitive approaches and transparent and open dialogue on risk as well as conformity of all employees with the firm's communicated level of risk appetite;

  - introduce ownership on control and monitoring processes through individual accountability for senior management for their respective areas of business;

  - reinforce the importance of a three lines of defence model as a basis for effective compliance as well as, depending on the risk exposure and complexity of a firm, maintain a formal code of conduct (*Verhaltenskodex* as per AT Module 5);

- an amendment to AT Module 4.1 (Internal capital adequacy) which emphasises that internal capital adequacy levels must concretely reflect both the continuity of the business and the impact of economic losses that might be borne by creditors of the firm. Internal capital adequacy remains an area that is very much in-scope of the ECB-SSM's 2018 supervisory priorities and SREP;

- a minor amendment to AT Module 4.2 (Strategies) that introduces the requirement on SIFIs to self-assess how to improve risk data aggregation and how existing or future arrangements may be affected by regulated delegation and/or outsourcing arrangements;

- major amendments in AT 4.3.1 (Organisational and operational structure) and AT 4.3.2 (Risk management and risk control processes) that have the following practical impacts for firms:
    - an introduction of a time-limited ban[13] on employees moving from market and client-facing business areas (*Handels- und Marktbereiche*) to performing reviews on their own activities or those of others when such employees move into business support and processing units, risk controlling, compliance, or other control functions of the relevant firm;
    - processes and competencies are required to be clearly defined, subject to timely adjustments and operate on a need-to-know basis as well as clearly defined IT access rights and signing authorisations;
    - intra-group arrangements and how these fit into the risk and control processes are required to be reflected in the appropriate policies and procedures;
- the new addition in AT Module 4.3.4 (Data management, data quality and aggregation of risk data), which follows the international accepted principles set by the Basel Committee on Banking Supervision (**BCBS 239**)[14], which only apply to SIFIs. It should be noted that whilst **BCBS 239** may be favoured by the ECB-SSM it may not be embedded in other jurisdictions in the same way as MaRisk embeds relevant principles;
- clarifications inserted in AT Module 4.4.1 (Risk control function) that this must be a function that is independent of business units active or connected to the initiation and conclusion of transactions and not merely responsible for independent oversight. The new guidance note sets out the degree of this segregation both in terms of depth and breadth as well as how it should apply proportionally to entities;
- a new guidance note is introduced detailing what the BaFin considers in AT Module 4.4.1(4) to constitute sufficient independence of the head of the risk control function and a new rule in AT 4.4.1(5) as to how and when SIFIs should appoint a Chief Risk Officer. Similar clarifications are introduced in respect of the compliance function which is detailed in AT Module 4.4.2;
- clarifications that internal and external audit activities should facilitate the comparability of standards applied in the audit exercise;
- adjustments on document retention standards from two to five years for business, control and supervision documentation;
- a new introduction in AT Module 8.1 (New product process) which requires each in-scope institution, but drafted very much with credit institutions, i.e., banks, in mind to maintain an up-to-date "Catalogue of Products and Markets" it is commercially active in and to periodically check whether those products are still being used or to wind these down. This requirement may be quite different to what exists (as a rule as opposed to best practice) in other jurisdictions;
- substantial amendments to meet ESA and ECB-SSM guidance on outsourcing have been introduced in AT 9 (Outsourcing) including the relevant control processes (including a centralised outsourcing management and review process) and consent/review processes required in relation to additional outsourcing as well as requirements on how outsourced functions are to be reviewed, controlled and findings as well as remedial actions documented and checked. The changes in AT Module 9 are likely to require specialist advice tailored to the respective business engaging the outsourcing provider as well as consideration of the latter and relevant risks. A notable takeaway and which fits in with the supervisory expectations of the ESAs and the ECB-SSM is that in future the risk control, the compliance and the internal audit function must, unless in limited justifiable circumstances of a group/subsidiary relationship, remain with the relevant supervised firm;
- substantial amendments in BTO Module 1.2 that clearly emphasise a requirement to review the valuation, management, custody and provisioning of a security interest/collateral asset provided in connection with "credit business" (*Kreditgeschäft)* i.e., lending. This is reiterated in BTO 1.2.1 (granting of loans - although NB the German term is wider in application to credit other than just loans). Similar items are set out in the new guidance BTO 1.2.4 (intensified loan management) although this should be read in conjunction with the ECB-SSM's rules on NPLs as well as the EU's 2017 Action Plan . As a general note, a lot of the BT Modules' requirements may be of secondary importance given the supervisory expectations set in the ECB-SSM's NPL

13 Smaller and less complex institutions are permitted to introduce measures that are proportionate to the business and its risks, but these must still reflect the supervisory principles and objectives of this AT 4.3.1(1).

14 See: https://www.bis.org/publ/bcbs239.pdf

Guide which the EU's 2017 Action Plan aims to roll-out to all credit institutions in the EU regardless of how or who supervises them;

- additions made in BTR Module 3.1(12) introduce a requirement for firms to maintain an internal refinancing plan, which is separate and in addition to a Recovery Plan;
- changes introduced in BTR Module 4 (Operational risk) bring those requirements more closely aligned with international standards in respect of capturing and reporting operational risk as well as "near misses"; and
- finally, the new component of BT Module 3 (Risk reporting requirements), which runs to three pages, introduces risk reporting requirements that are quite prescriptive and places a central focus on sufficient:
  - frequency (on going and at least quarterly and for certain reports, at least daily) and depth of reporting including forward looking assessments;
  - greater consideration of stress-test results; and
  - prescriptively detailed measures on accountability to supervisory body within the firm with at least quarterly reports on risks to date, mitigants, impact on going and future operations as well as strategic implications etc. that are presented in writing (and thus subject to the document retention requirements).

If you would like to receive more about MaRisk 2017, its changes and differences to rules in other key global jurisdictions and what it means for your business in Germany or in relation to processes and considerations connected with a relocation to Germany, please do speak to any of our regulatory experts including any of our Eurozone Hub key contacts below.

# 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





BRAND-9680_BaFin_client_alert_regulatory_newsletter_no2_06–03/07/2018