Introduction

There is nothing new about the use of technology in the financial industry. It is part of everyday life for financial service providers. The pace of technological development is extremely rapid. This offers opportunities, not just for fintechs but also for banks. One way forward is for banks to work together with fintechs. These guidelines look at specific ways in which this cooperation can be improved while ensuring that banking supervisory requirements are met.

Background

These guidelines are a follow-up to our 2018 position paper "Banks and Fintechs: The Case for Outsourcing", in which we described the importance and the challenges of cooperation between banks and fintechs. The term “fintech” as used here covers all young companies that work together with banks to bring innovative, technology-based products and services to the market.

The position paper argued that productive cooperation between banks and fintechs would be furthered by guidelines on non-service-specific banking supervisory requirements. Banking supervisory requirements in these guidelines mean BaFin’s Minimum Requirements for Risk Management (MaRisk), which are referred to for reasons of practicability.

The guidelines are intended to make cooperation between banks and fintechs more efficient and robust. A particular objective is to speed up the time to market for products and services jointly developed by banks and fintechs. Our aim is to make it easy for our members to apply the guidelines in practice.

The content of the guidelines was developed in collaboration with selected member banks and fintechs of our association. It was then tested out by further members. There was also input from the Auditing Association of German Banks. Finally, we held discussions with the Federal Financial Supervisory Authority (BaFin) and Deutsche Bundesbank. BaFin considers the methodological approach of grading requirements for fintechs.

17 December 2019

Tobias Tenner
Digital Banking
+49 30 1663-2323
tobias.tenner@bdb.de

Frank Mehlhorn
Banking Supervision, Accounting
+49 30 1663-2140
frank.mehlhorn@bdb.de
according to the risk content of the business activities involved to be an appropriate one.

In parallel with our project, the European Banking Authority (EBA) published its own revised guidelines on outsourcing [3]. Initial analyses and discussions with BaFin indicate that there will also be adjustments to MaRisk. Since the scale of these changes is not yet clear, this document does not take account of the EBA requirements. We plan to assess the possible need for adjustments at a later date.

Challenges

If banks want to be competitive, they need to serve a very broad ecosystem. They must be able to react swiftly and flexibly: implementation of their onboarding processes, in particular, needs to be quick and systematic. Fintechs are important partners in the digital transformation of banks and can accelerate the transformation process with concrete products and solutions.

One of the biggest challenges when it comes to cooperation between banks and fintechs is that, from the outset, fintechs must often meet requirements that are disproportionately high in relation to the actual risk to the bank. Synergies from cooperation, on the other hand, are often only generated quite late in the process and are not proportionate to the initial time and effort involved in meeting these requirements (see figure 1, left-hand side).

Fintechs face the additional challenge that banks’ risk assessments of cooperation are insufficiently transparent and that the requirements set by different banks for the same service or the same product can differ greatly as a result. Even with simple yes or no questions it is not always clear why the bank is asking them and what exactly is expected of the fintech. When a fintech is seeking to cooperate with more than one bank, moreover, the risk classification, maturity level and also the requirements set for the fintech can vary widely in connection
with the same service. This makes matters significantly more costly and complex for the fintech.

The upshot of this lack of clarity is that the regulatory/administrative onboarding of fintechs at banks usually takes 12 to 18 months, while “technical” onboarding could be completed within a matter of weeks.

**Overarching objective and methodology**

Our objective is to facilitate and at the same time accelerate cooperation between banks and fintechs. The guidelines aim to achieve this with the help of the two steps below (see figure 1, right-hand side).

1. The risk arising from the bank-fintech cooperation is determined and converted into a corresponding risk maturity level (RML). There are four RMLs.
2. The RML determines the level of requirements that must be met. In the catalogue of requirements, four levels of specific requirements (one per RML) are defined for each requirement type.

We are convinced that the steps outlined above (and explained in more detail in the following sections) will result in uniform expectations and thus better preparation for cooperation between banks and fintechs. The efficiency gains for banks and for fintechs will make both partners more competitive and thus strengthen Germany’s (and Europe’s) position as a financial centre.

**Desired outcome**

The outsourcing guidelines of the Association of German Banks are designed to

1. give our members more certainty in interpreting and applying the principle of proportionality in the context of bank-fintech outsourcing;
2. support our members in designing internal processes and procedures; and
3. provide a basis for fintechs to better understand the requirements set for them, thus enabling them to prepare more efficiently for cooperation with banks.

The more frequently the guidelines are applied in practice, the easier it will be to achieve the associated objectives – namely to make cooperation between banks and fintechs more efficient and robust and to speed up the time to market. We would therefore encourage not only our banks and fintechs, but also their auditors, to take a close look at the guidelines.

We would also like to continue to refine the guidelines. After they are tested in practice, therefore, they will be subject to ongoing review and, where necessary, adjustment.
Overview of the guidelines

The guidelines were developed on the basis of existing regulatory requirements and best practices. They comprise two segments: (i) the RML model and (ii) the catalogue of requirements. These are to be applied one after the other.

The RML model is used to assign the risk associated with bank-fintech cooperation to one of four individual RMLs. To determine the RML, a list of 18 questions must be answered. The questions are divided into risk and impact questions. Each question has various answer options. The option selected results in a score, which is then weighted. The total risk score and the total impact score are multiplied together to produce a total score. This total score corresponds to one of the four RMLs, which each have a “from ... to ...” range.

The catalogue of requirements consists of a list of specific, risk-proportionate requirements which a fintech should fulfil in the context of a particular form of bank-fintech cooperation. The requirements are also divided into four levels, with each level corresponding to an RML, i.e. at RML 1 level 1 requirements must be met; at RML 2 level 2 requirements must be met, and so on. The requirements progressively become more stringent and extensive.

The procedure and the segments were tested for their practicability with the help of use cases (UCs). The UCs establish a direct, practical link to existing cases of cooperation between banks and fintechs.

The guidelines in more detail: risk maturity level model

Explanation of the logic of the risk maturity level model

Summary

The RML model is designed to carry out a differentiated and service-specific assessment of the risk associated with a service to be provided by a fintech. The aim is to determine an RML with the help of a questionnaire.

Since cooperation between banks and fintechs is often much more dynamic than that between banks and traditional service providers, it is envisaged that – depending on the extent to which the provision of the service or the cooperation intensifies – the RML assessment using the RML model will be carried out
on a regular basis. This means that the corresponding requirements may also change.

Catalogue of questions

The centrepiece of the RML model is a catalogue of 18 questions. The questionnaire was designed to meet the following criteria:

- questions and answer options should be clear to the user;
- all questions should be relevant since they are based on recent UCs of bank-fintech cooperation;
- it should be possible to swiftly assign new UCs to an RML;
- there should be transparency and certainty for fintechs and banks regarding the assignment to an RML;
- the model should be universally applicable in that it can accommodate all individual cases of different (participating) banks.

A structured approach was taken to developing the questions. (The methodology is explained in more detail in the annex 2 “Validation process for the risk maturity level model”.)

Questions and answer options were compiled on the basis of the following universally applicable risk categories of a service:

- business continuity,
- regulatory requirements,
- service provision by the fintech,
- service provision by the bank,
- information security.

These five risk categories allow the questions to be clearly structured and ensure a high degree of coverage by the RML model. To ensure high-quality results, it is essential to answer all 18 questions.

Each question is assigned to one of the coordinates of the model: “risk” or “impact” \[4\] The range of questions is particularly clear in the area of information security: the five questions cover the type of server hosting, the region where the servers are located, data classification, the level of data accuracy, and the impact of a data breach.
In addition, the questions and replies are tailored to obtaining services from fintechs (as opposed to traditional service providers).

- The answer options for comparable service providers are adapted to the small size of the fintech market, i.e. reduced compared to traditional service providers in the market.[5]
- The question about the fintech's financial stability focuses on the duration of funding in connection with the ownership structure, unlike in conventional analysis models of banks.

Each question has various answer options and – where necessary – is accompanied by explanatory notes to ensure the greatest possible transparency. If, for example, the options "low", "medium" and "high" are offered without further explanation, no quantitative grading is intended since each bank will assess this individually. In practice, however, the bank should explain to the fintech why it has decided on the selected option. This will ensure transparency and mutual understanding.

The answers to the questions correspond to individual scores, which are then weighted according to their importance to banks in the context of the project and thus adjusted to reflect actual practice (standard = 1, minimum = 0.5, maximum = 4). The weighted individual scores add up to a total risk score and a total impact score, with a maximum score of 50 possible in each of the two coordinates.

Question 18 is especially important because it lies, so to speak, outside the scope of the RML model. Its purpose is to potentially adjust the RML determined from the previous 17 questions upwards in line with the bank’s risk appetite. It is a yes/no question, with the “yes” option having the effect of increasing the risk score (if the “no” option is selected, the answers to the other questions can still produce the maximum total risk score of 50). This approach makes sense because it was established during the test phase that UCs could lead to an RML that did not reflect the importance in practice: the RML calculated was lower than the bank’s own assessment of the business relationship. This is plausible given the different business models of banks (in this case a white label bank) and is also reflected in the principles-based approach of banking regulatory requirements.

**Specifics of the risk maturity level model**

The two coordinates on which the RML model is based, namely “risk” and “impact”, make it possible not only to assess the risk of a specific fintech service for the bank but also to include the anticipated impact of the service and service provider risks on the bank.

This means, for example, that (assuming the total scores are identical) a fintech service with a high risk score and a low
impact score will be assigned to the same or a similar RML as a fintech service with a low risk score and a high impact score.

After answering the questionnaire, the total risk and total impact scores are recorded separately on the x-axis (risk) and the y-axis (impact). This generates the RML of the fintech service for the bank.

A total of four RMLs have been defined to cover the scores; these are plotted graphically as curves in the coordinate system and range from dark green (RML 1 = minimum) to red (RML 4 = maximum).

![Risk Maturity Level Model](image)

Figure 3: Risk maturity level model

The thresholds between individual RMLs are determined as follows:

- **Maturity level 1 (risk x impact 8-199)**
- **Maturity level 2 (risk x impact 200-799)**
- **Maturity level 3 (risk x impact 800-1499)**
- **Maturity level 4 (risk x impact 1500-2500)**

Figure 4: Risk maturity levels and thresholds
The RML of the example shown in figure 3 is therefore calculated as follows:

\[ \text{risk (21)} \times \text{impact (35)} = 735, \] which corresponds to RML 2.

Once the RML has been determined, the requirements the fintech must meet can be taken from the relevant column in the catalogue of requirements. Adjusted for risk, the requirements gradually increase from RML 1 to RML 4. The requirements are generally based directly on the maximum regulatory requirements for outsourcing.

Description of risk maturity levels

The following descriptions of the RMLs are for illustrative purposes to show how the RMLs progress from one to the other.

Risk maturity level 1

RML 1 is the least risky level of cooperation between a fintech and bank. At this RML, the fintech service will normally relate to only a limited product range or limited user group. Services covered by this RML may not be classified as outsourcing within the meaning of section 25b of the German Banking Act/MaRisk AT9 unless real customer data are used productively.

Risk maturity level 2

At RML 2, the cooperation between fintech and bank is already at an advanced stage. Although the scope or the reach of the service in the bank’s customer base or internal processes is limited, it is broader than at RML 1 even if the risk remains manageable. The fintech’s service will be provided largely independently and will not be closely integrated into the bank’s own systems and processes. The service can be classified as outsourcing within the meaning of section 25b of the German Banking Act/MaRisk AT9. As a rule, this will be non-material outsourcing [6].

Risk maturity level 3

RML 3 describes cooperation between a fintech and bank which has become far advanced. The form or environment of the service poses an increased risk to the bank owing, for example to strict legal requirements that the service must meet, to greater dependency on the fintech or to the extended scope of the service. As a rule, integration into the bank’s own systems and processes will be (far) advanced and the service will be available to varying degrees to a large number of the bank’s customers or will have a significant impact on the bank’s internal processes. It is highly likely that the service will be classified as outsourcing within the meaning of section 25b of the German Banking Act/MaRisk AT9 and there will be a greater
need for risk assessment in this respect. For some banks, this may already represent material outsourcing.

Risk maturity level 4

The bank-fintech cooperation has reached its highest level. The risk arising from the service provided by the fintech has a high degree of relevance to the bank because it is used by the majority of the bank’s customers, for example, and customers are dependent on the service and unable to fall back on an alternative. In addition, the fintech’s service may be essential to carrying out or supporting core banking processes such as payments or securities transactions processing. At RML 4, the service will normally be deemed material outsourcing within the meaning of section 25b of the German Banking Act/MaRisk AT9.

The guidelines in more detail: catalogue of requirements

Distinction between non-service-specific and service-specific banking supervisory requirements

It was pointed out in the introduction that these guidelines cover “non-service-specific banking supervisory requirements”. In the interests of simplicity, reference is generally made only to “requirements” and a “catalogue of requirements”. Non-service-specific banking supervisory requirements are nevertheless always meant. It therefore makes good sense to explain this term further.

Non-service-specific banking supervisory requirements distinguish themselves from service-specific supervisory requirements in that they are general requirements banks expect fintechs to meet irrespective of the precise product or service concerned. Most are requirements concerning proper business organisation (based on section 25a of the German Banking Act) and regulatory requirements directly related to outsourcing (e.g. in accordance with MaRisk).

The advantage of our approach is that it enables standardised requirements to be set for fintechs regardless of the type of individual cooperation between a fintech and bank, since for requirement types like business continuity management, certain conditions must always be fulfilled.

By dividing the requirements into four levels (RML 1 = level 1 to RML 4 = level 4), standard guidance is created on implementing these requirements at the fintech.

By contrast, requirements concerning matters such as drafting contracts or service level agreements are to be considered service-specific banking supervisory requirements. EU data protection and anti-money laundering requirements are also
examples of service-specific banking supervisory requirements because they depend on very specific aspects of the cooperation in question. It is not possible to grade requirements of this kind into various RMLs. They are consequently outside the scope of these guidelines.

Determining and grading the requirements

The catalogue of requirements contains the following requirement types, which cover a large proportion of supervisory requirements relevant to outsourcing.

1) Business continuity management (BCM)
2) Internal controls
3) Information security, subdivided into
   a. governance
   b. authorisation system
   c. physical security
4) Organisational guidelines and documentation
5) Auditing activities
6) Vendor management

The following section describes the basic methodology for determining and grading the requirement types. It names the standards from which the requirements are derived and describes the dimensions needed to subdivide and grade them. A detailed description of the requirement types addressed in this document and a list of the individual requirements per level can be found in annex 1, sheet 3.

The starting point for the description of the requirements to be met by the fintech and monitored by the bank is always the regulatory regime governing the bank in question.

Under section 25a (1) of the German Banking Act, banks licensed in Germany must fulfil “particular organisational duties”, which are fleshed out further by administrative requirements – such as the BaFin circular on the Minimum Requirements for Risk Management (MaRisk) – and by international or national security standards. Examples of security standards are the IT basic protection catalogue of the German Federal Office for Information Security (BSI) and the international ISO/IEC 2700X security standard of the International Organization for Standardization. The box below shows examples of the requirement types considered in this document and the standards on which the requirements are based.
<table>
<thead>
<tr>
<th>Requirement type</th>
<th>Minimum standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity management</td>
<td>MaRisk AT 7.3: Contingency plan; BSI standard 100-4</td>
</tr>
<tr>
<td>Internal control system</td>
<td>MaRisk AT 4: Internal control system; COSO Framework[7]</td>
</tr>
<tr>
<td>Information security</td>
<td>MaRisk AT 7.2 (1) and (2): Technical and organisational resources; BSI’s IT basic protection catalogue, especially BSI-ISO 27001; BaFin’s Supervisory Requirements for IT in Financial Institutions (BAIT), especially sections 2 to 5Where required further international standards such as NIST, PCI, DSS</td>
</tr>
</tbody>
</table>

The standards listed always set the maximum requirements for the corresponding requirement type and thus provide the framework for RML 4. This is not, however, to imply that the standards are final or exhaustive. The feedback review cycle (see “Outlook” section of the guidelines) will allow the standards to be adapted.

At level 4, the degree of cooperation between fintech and bank will always be very high (see “Description of risk maturity levels” section) and processes and data flows will therefore be closely interlinked. If a process or system at one party does not function correctly or even fails, a direct impact on the other party can be expected (contagion). In consequence, level 4 requires the highest due diligence standards, which can be derived from the “particular organisational duties” applicable to banks.

*Take, for example, the information security/governance requirement type: as described in detail in annex 1, governance would need to be designed to satisfy, among other things, the principles and requirements of the BSI’s IT basic protection catalogue, especially BSI-ISO 27001. This would involve setting up an independent organisational unit and assigning it qualified personnel, who would deal with information security issues and ensure information security in day-to-day business. The unit would have to define, document, implement and establish appropriate risk management, incident management and training processes.*

*For the business continuity management requirement type, banks would have to follow the German BSI 100-4 standard on emergency management. At level 4, the basic BCM control cycle would have to be implemented for the purposes of emergency management, so that BCM plans for buildings, IT and persons would have to be described and the BCM plans of the fintech and bank would have to be coordinated with each other.*
In addition, crisis manuals, guidelines, organizational charts and contact details would have to be drawn up for use in the event of a crisis.

Level 4 is the starting point for the other levels. The minimum requirements of level 4 are scaled back step by step to level 1 with due regard to the risk involved and to the dimensions “degree of organisational importance” and “degree of structural implementation”. The introduction of these two dimensions is needed to ensure that third parties – above all banks, supervisors and auditors – can understand the rationale and to provide an objective framework for the partly subjective expert assessment of the progression from RML 1 to 4.

The degree of organisational importance implicitly breaks down the individual minimum requirements from level 4 into the elements essential to a (risk) management cycle, namely (A) governance (including knowledge transfer/training), (B) identification, management and monitoring, and (C) validation and adjustment. These categories are then ranked relative to one another. (A) and (B) are of major while (C) is of lesser importance. Elements of high relative importance must also be included in the lower RML requirements, whereas this is not necessary for elements of minor importance (cf. figure 5).

<table>
<thead>
<tr>
<th></th>
<th>(A)</th>
<th>(B)</th>
<th>(C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 4</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Level 3</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Level 2</td>
<td>X</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td>Level 1</td>
<td>(X)</td>
<td>(X)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: Requirements per risk maturity level

While the degree of organisational importance aims at a fundamental definition of requirements, the degree of structural implementation adds a qualitative dimension in terms of qualitatively comprehensive or simplified implementation. A high degree of structural implementation along the lines of level 4 requires structured, comprehensive or standardised implementation, while for a low degree, as at level 1, a case-by-case or simplified implementation would suffice. Nevertheless, a thorough expert assessment is indispensable when it comes to grading the requirements between the two extremes (4 and 1) since this dimension ultimately determines only the range of the descending steps (cf. figure 6). The bank must, in any event, substantiate its decision.
Going back to the two previous examples, namely information security/governance and BCM, requirements would be graded as follows.

For the information security/governance requirement type, the minimum requirements of high organisational importance need to be met across all RMLs. This means, for instance, that under (A), governance, an information security officer always has to be appointed who, depending on the RML, will be progressively downgraded from full-time to part-time employee in the structural implementation. In addition, appropriate policies or guidelines will be needed and these will also be differentiated qualitatively. Level 3 continues to require an updating and approval process for all documents, while at level 2 it is enough to have corresponding documents in place and at level 1 even general guidelines would suffice.

Under (B), identification, management and monitoring, both the joiner/mover/leaver process (access rights) and incident management remain core elements and a basic requirement to be met by fintechs across all RMLs. But here, too, requirements are graded in the dimension of structural implementation in terms of the quality and number of measures. At level 3, for example, an additional separation of functions is required, as well as security risk management with respect to identification and prevention of risks. At level 1, by contrast, incident management only has to be carried out on a case-by-case basis and does not need to be structured as at the other RMLs.

For (C), validation and adjustment, the extensive level 4 requirements are gradually reduced in line with their organisational importance to measures to be implemented in a simplified manner. At RML 3
only frameworks and guidelines need to be reviewed and updated while at the following levels (RML 1 and 2) these activities are no longer even considered hard minimum requirements. The reason for this is the non-systematic and looser cooperation between fintech and bank with the resulting low or marginal risk to the processes or operations of the bank.

A similar picture emerges when it comes to the BCM requirement type. Requirements for (A), governance, and (B), identification, management and monitoring (of BCM processes or plans, for instance), remain unchanged over levels 2 and 3. But as with information security/governance, the requirements differ according to degree of structural implementation. In line with the risk assessment, BCM processes must be implemented in full at level 3, for example, and in simplified form at level 2 (“risks known and limited”).

Unlike with the information security/governance example, there are no minimum requirements for level 1. The assumption is that there will be no systematic exchange of (test) data at this RML and that the cooperation and initial integration of processes between the fintech and bank is only in the process of being set up. In consequence, there will be no risk to the bank or its business processes in the event of an incident at the fintech.

Possible testing of BCM plans under category (C), validation and adjustment, would need to be carried out at levels 3 and 2 but measures would also be graded according to the degree of structural implementation. At level 3, tests would have to be carried out regularly in consultation with the bank, while at level 2 they would no longer have to be carried out systematically but only if it proved necessary.

Application in practice
We would now like to make some concrete recommendations for the practical application of the guidelines.

Application in borderline cases
In cases where an RML result lies on a boundary between two RMLs, the requirements of the higher level are generally applied for risk reasons. This may mean the fintech has to spend more time and effort on implementation. This approach is nevertheless always advisable if the cooperation between the bank and fintech is likely to develop further in the future,
since the risk and impact and thus also the requirements to be met will increase as the fintech service becomes increasingly integrated into the bank’s systems.

It should also be noted that an individual assessment of a bank-fintech cooperation may sometimes make it necessary to set a requirement type at a higher level than that corresponding to the actual RML classification (conservative approach). One business continuity requirement, for example, may exceed the level for other requirement types; this particular requirement will then deviate from the general RML classification (e.g. the fintech service may be at RML 2 overall but need to meet level 3 requirements for BCM). This approach takes account of the complex possible forms of bank-fintech cooperation and the complex regulatory requirements needing to be met. It should be stressed, however, that such an arrangement should be the exception rather than the rule.

Recommendations to banks

1. **Application of the guidelines to a bank’s outsourcing management and monitoring practices**
   Before integrating the guidelines into the bank’s own outsourcing management, it is advisable to test the guidelines on the procedures and methods in use with existing outsourcing arrangements. When evaluating a bank-fintech cooperation, it may also make good sense to apply both the existing procedures and the guidelines in parallel. We would also recommend the involvement at an early stage of senior management and all the relevant functions (risk controlling, compliance, internal audit, information security, data protection officer) since they are responsible for the bank’s risk strategy and risk-bearing capacity and will have to defend the use of the guidelines.

2. **Application of the guidelines to individual bank-fintech outsourcing arrangements**
   - Individual analysis remains indispensable
   It is true that the guidelines are intended to establish a basis for more consistent treatment of certain types of requirements across banks and that a clear and simple methodology is used in the form of the RMLs. It should nevertheless be borne in mind that a bank’s individual analysis of a specific outsourcing arrangement may show a need for certain adjustments to the requirements to be met by the fintech. The RML (and corresponding scale of requirements) should therefore be understood as a point of orientation based on extensive practical experience and tested on concrete UCs. This does not, however, mean that requirements across different requirement types can only be taken from the same RML. If the specific design of bank-fintech...
cooperation and the associated risk assessment necessitate it, it may make good sense to take requirements from a lower or higher level for individual requirement types.

3. **Ongoing monitoring of fintech outsourcing and regular re-evaluation of the RML**

Business relationships between banks and fintechs and the associated outsourcing arrangements may develop more dynamically than is the case in traditional outsourcing. Regular re-evaluation of the RML may be necessary, especially when a low RML is initially determined at the outset of the cooperation and where the fintech consequently has to meet a comparatively low level of requirements. This is important in order to ensure that the implementation of the requirements by the fintech is proportional to the risk to the bank. There may also be certain occasions when it is necessary to use other models and processes to assess and manage the outsourcing arrangement. Reasons for changes might include:

a) the provision of an additional service outside the EU
b) a change in the cloud service environment
c) a change in the bank’s risk appetite due, for example, to an increase in the market or revenue share as a result of the fintech service
d) the fintech is taken over or there is a change in its ownership structure

**Recommendations to fintechs**

Fintechs could apply the guidelines in three specific ways extending over various phases of the company’s development.

1. **From the start-up phase through to market maturity - knowledge transfer and integration of requirements into company planning at an early stage**

   Particularly in their start-up phase, fintechs often have little knowledge and experience of banking supervisory requirements and of how they relate to outsourcing. The guidelines can therefore be used as a practical collection of information and hands-on manual from a user’s perspective. They can enable requirement types to be identified at an early stage and a road map for compliance with supervisory requirements to be planned out. This allows supervisory requirements to be continuously taken into account in a timely manner when planning and allocating resources both in product development and in the organisational structure of the fintech.
2. **Preparation for concrete cooperation with banks and constant support in a business relationship**

The guidelines can enable fintechs to carry out a self-assessment to the best of their knowledge and consider the bank’s perspective so that they can deduce what regulatory requirements they will be expected to meet when cooperating with the bank. This, in turn, can be used to carry out a target/actual comparison between expected requirements and existing implementation when first initiating the business relationship, enabling any need for action and adjustment to be identified and prepared for at an early stage. The guidelines take account of the risk proportionality of regulatory requirements, so they can also be used on an ongoing basis to infer upcoming requirements in the context of an existing and dynamically developing business relationship. As a rule, the more substantial and important the business relationship becomes for a bank, the higher the RML will be and, as a result, the greater the regulatory requirements that the fintech will need to meet.

3. **Preparation to obtain a licence**

Fintechs whose business models require a banking licence, often begin by working together with another, already licensed firm (“licence/banking as a service”). The longer a fintech of this kind exists on the market and the more established its business becomes, the more advantageous it may be to apply for a licence of its own. Here, too, the guidelines can be seen as a road map plotting progress across the various RMLs towards fulfilling at least some, if not all, prerequisites for obtaining a licence of the fintech’s own (e.g. with regard to business management processes, internal control mechanisms, risk management, organisational structure and operational procedures).

**Outlook**

The Association of German Banks would like the guidelines to be used by as many of its members as possible. We would also like to continuously refine the guidelines. If the guidelines meet with broad acceptance among our members and are applied in practice, we intend to establish a systematic feedback loop. This should ideally function electronically, comprise standardised documents and offer various evaluation options. At the same time we want to offer our members support in applying the guidelines by setting up a telephone helpline, for example.

Those involved in drawing up the guidelines can envisage developing a certificate based on the guidelines. The certificate would confirm a fintech’s compliance with a given level of requirements. It could, for example, be used to reduce the
need for repetitive audits on the part of banks and fintechs. The Association of German Banks intends to develop corresponding proposals in collaboration with its members.

**Definitions**

**Bank**

Within the meaning of section 1 of the German Banking Act Covers all members of the Association of German Banks (BdB)

**Cooperation**

The bank and fintech deploy products and services together. Operational cooperation of varying format and duration and with varying objectives between a bank and fintech as legally independent companies. Levels of intensity might range from an exchange of information, joint projects with/without outsourcing of one (or more) company function(s) to a joint venture. Covers various models, such as fintech-as-a-service, white labelling and joint new developments As well as products and services offered on the market, it also includes products and services used internally by the bank.

**Coordinates**

The x and y axes of our RML model (risk and impact)

**Degree of organisational importance**

A dimension considered when grading requirements Implicitly assigns individual minimum requirements from level 4 to the main elements of a (risk) management cycle: (A) governance (including knowledge transfer/training), (B) identification, management and monitoring, and (C) validation and adjustment

**Degree of structural implementation**

A dimension considered when grading requirements Intended to provide a qualitative dimension in the sense of qualitatively comprehensive or simplified implementation
Dimension

Describes the main aspects considered in the process of grading requirements

Fintech

For the purposes of these guidelines, fintech means a young company that cooperates with banks to deploy innovative, technology-based products and services. Covers most extraordinary members of the Association of German Banks

Impact

Coordinate of RML model
The effect when a risk materialises
One question in the questionnaire asks, for example: “How much time is needed to switch to an alternative service provider?”, the impact is the effect on the bank in terms of time.

Level

Refers to the list of requirements
Each requirement type is divided into four levels of requirements corresponding to the relevant RML.

Non-service-specific banking supervisory requirements

General requirements which banks expect fintechs to meet and which are not related to concrete products/services. Mostly requirements concerning proper business organisation (based on section 25a of the German Banking Act) and regulatory requirements directly related to outsourcing (under MaRisk, for example). In these guidelines, a catalogue fleshes out these requirements in more detail and grades them on the basis of the degree of risk involved.

Onboarding

Standardised procedure from first contact to realisation of the cooperation and/or outsourcing. Enables risk-appropriate and neutral, qualitatively consistent decisions on entering into cooperation and outsourcing arrangements
Option

A possible answer in the RML model questionnaire

Outsourcing

Within the meaning of BaFin’s Minimum Requirements for Risk Management (MaRisk)

Requirement type

Category of “non-service-specific banking supervisory requirement”, e.g. business continuity management, internal controls, information security

Risk

A coordinate of the RML model
Refers to a possible danger which would adversely affect the bank
One question in the questionnaire asks, for example: “Are there alternative service providers/fintechs on the market?”. The danger here is of the bank being unable to obtain the service or product elsewhere.
Probabilities are normally also taken into account when determining risks. Our RML model does not do so – among other things, because we want to provide a model that is easy and straightforward to apply in practice. In addition, our focus is on consequences and on the corresponding requirements a fintech should have to meet.

Risk appetite

Referred to in Q18 of the questionnaire
Means the extent to which the bank is willing to take on risks that may result from cooperation with a fintech

Risk assessment

Result of the RML
Bank’s evaluation of the risk associated with cooperating with a fintech

Risk categories

Categories of questions in the RML model questionnaire
RML

Stands for risk maturity level
Assessment of the level of risk associated with a specific bank-fintech cooperation

RML model

Model used to determine the RML of a bank-fintech cooperation
Consists of a questionnaire with questions about risks and impacts and a graphical model showing total risk and impact scores from the questionnaire on the x-axis (risk) and y-axis (impact)

Score

Each option in the RML model questionnaire corresponds to a score.
Each score is weighted in such a way that the total risk and total impact score each amount to a maximum of 50.
The total score is the product of the total risk score and the total impact score.

Service-specific banking supervisory requirements

Requirements relating to very specific aspects of cooperation and which cannot be graded, e.g. data protection and anti-money laundering requirements
Service-specific banking supervisory requirements are outside the scope of these guidelines

Threshold

Boundary between the four individual RMLs as a total score

Time to market

Period of time before a product or service idea jointly developed by the bank and fintech is ready for, and can be placed on, the market

UC

Short for use case
A direct, practical reference to an actual example of cooperation between a bank and fintech
**White labelling**

Provision of a bank’s infrastructure (including the associated banking licence) to a third party, which operates as a bank for its customers. The white-label bank does not offer its banking services to the actual end customer (in a B2C context) but only to third parties or partners (in a B2B context).

**ANNEX 1: Guideline model (Excel document)**

The Association of German Banks will make the Excel document available to its members on request. Enquiries should be emailed to bab_buero@bdb.de quoting “BdB POL – request for Excel document” in the subject line.

**ANNEX 2: Validation process for the risk maturity level model**

The RML model was validated iteratively with the help of real UCs involving cooperation between banks and fintechs. The goal was a methodical, systematic approach producing results that could be objectively understood and reproduced by everyone.

The iterative approach was stringently applied, with each individual step of the model developed jointly and critically scrutinised in project group discussions to see if the objectives were being met. Based on the five risk categories (business continuity, regulatory requirements, service provision by the fintech, service provision by the bank and information security), relevant questions were initially collected from all participating banks. These questions were then discussed a number of times by the entire project group, redundancies were eliminated and questions were consolidated in order to keep the model manageable. A broad range of questions remained the aim of the approach.

A further element of the work was dividing the questions into the coordinates “risk” and “impact”. In two separate working groups, the questions and reply options of the two coordinates were first further developed, then discussed again in a plenary session and tested for the first time on UCs. During testing, the terms used were defined more precisely and wording was improved so that the questions would be as clear and unambiguous as possible for users of the model.

Once the questions, response options and scores had been defined, the model was validated using UCs from members.
banks and the corresponding RMLs were determined. The RMLs were then compared with the banks’ own internal evaluations.

Cases where there was a discrepancy between the bank’s evaluation of the outsourcing and the evaluation using the RML model were analysed by the project group and the reasons for the discrepancy were identified. Differences were frequently due to a lack of precision in the questions or excessive scope for interpretation in the responses. All questions and response options were then individually examined in iterative loops. Subsequently,

- some questions were reformulated or formulated more precisely,
- or merged with another question,
- responses were validated,
- response options were analysed and honed, and
- the weighting of the questions was discussed.

The aim was to ensure that the questions and their answers were totally clear. In addition, the response options and scoring were adapted to the special needs and characteristics of fintechs.

A total of 17 UCs were used to validate the RML model. The UCs were tested intensively and repeatedly by individuals and the project group. In one case, a fintech and bank separately and independently assessed an existing outsourcing arrangement with the help of the RML model, and the results were compared and discussed. Where differences were found, the cause was investigated and critically reflected in the context of the RML model. Discrepancies resulted exclusively from different understandings of the service components involved and could be eliminated once a common understanding had been reached. Experience with this example, in particular, demonstrated that the RML model is clear and easy to apply. When evaluations were discussed, views could be swiftly exchanged and explained, which made the evaluation highly transparent.

Once all the validations had been completed, the UCs and their RMLs were explicable, readily understandable and largely consistent with the banks’ internal assessments.

**ANNEX 3: Validation process for the catalogue of requirements**

The following section deals with the validation of the grading of individual requirement types per RML.

The RML (from 1 to 4) is a risk assessment of a specific case of cooperation between a bank and fintech. It results from the responses to a number of questions (see “Explanation of the
logic of the risk maturity level model” section). The RML shows the level (1-4) of the requirements that a fintech must meet.

To check the plausibility of our model, we selected three representative UCs and tested the appropriateness of the level of requirements for three requirement types, namely business continuity management, internal controls and information security.

The following three UCs were selected:

1) RML 2 ==> additional cash payment service
2) RML 3 ==> account switching service
3) RML 4 ==> full IT service with substantial dependency and extensive (= all) customer services for retail clients

![Figure 8: Chart showing UC examples used in the validation process for the catalogue of requirements](image)

1. Risk maturity level 2, use case: additional cash payment service

The evaluation by the RML model puts the use case at RML 2, meaning that the impact and risk are moderate for the outsourcing bank. This is a plausible result since the bank’s customers also have other deposit and withdrawal options available to them.

The specific requirements which the fintech has to meet at level 2 can be found in annex 1.
2. Risk maturity level 3, use case: account switching service[^8]

The account switching service UC was judged by the RML model to have increased risk and impact for the bank and was consequently assigned to RML 3. A second account switching service UC for another bank, by contrast, was assessed have lower risk and impact which would put it at RML 2. This may seem surprising, but it is plausible and logical since the criteria influencing the risk and impact, such as the cost of changing the service or the type of hosting, may translate into higher requirements for information security or business continuity management and thus a higher level of requirement types.

The specific requirements which the fintech has to meet at level 3 can be found in annex 1.

3. Risk maturity level 4, use case: full IT service with substantial dependency and extensive (= all) customer services for retail clients

This IT service is classified as RML 4, which means that the impact and risk associated with the service offered to the outsourcing bank are comparatively high and that the fintech has to meet correspondingly stringent requirements. This is also plausible since the fintech involved in this UC is not a "true" fintech as such but an established outsourcing company with extensive processes and structures tailored to banks. The outsourcing company has to fulfil the requirements of level 4.

The reason for selecting this UC is that very few fintechs have yet achieved such an advanced RML with their services. The specific requirements set at level 4 can be found in annex 1.

[^1]: The term “non-service-specific banking supervisory require-ment” is defined in more detail in the section “Distinction between non-service-specific and service-specific banking supervisory requirements”. The term “requirement” is herein-after to be understood as a non-service-specific banking supervisory requirement.

[^2]: Based on section 25a of the German Banking Act, which specifies banks’ organisational obligations with respect to internal risk management, MaRisk set out a framework for managing all material risks. Among other things, they are intended to standardise the administrative activity of supervi-sors. For banks, the principles-based approach of MaRisk provides scope for individual implementation. Every bank must therefore analyse itself which part of a requirement needs to be implemented in what form. Depending on the bank, these may or must be more or fewer requirements in terms of scale. The practicability of the bank’s own requirements should be subject to continuous review.

[^3]: On 25 February 2019 the EBA published the final version of
its Guidelines on Outsourcing (EBA/GL/2019/02). These guidelines are intended to create a harmonised regulatory framework for all institutions supervised by the EBA. This means that, unlike the old CEBS guidelines on outsourcing, the EBA’s guidelines also apply to payment institutions and electronic money institutions. The EBA guidelines came into force on 30 September 2019 but contain transitional arrangements to give institutions time to implement certain requirements and adapt to the significant changes in the requirements for outsourcing.

Some questions include a reference to “customer(s)”. This usually means external customers. But depending on the service or product, employees of the bank (users) may also be considered customers.

One question, for example, asks “How may service providers in the market at present can provide a comparable service for the bank?”. One reply option is “more than 5”. This means the risk is low because there are enough other providers in the market. For a traditional service such as cash-in-transit, by contrast, the German Association of Cash/Valuables-in-transit Companies lists over 30 members.

The bank must use risk analysis to determine what risks are associated with the planned measure and whether these risks are material or non-material overall. A wide variety of aspects can play a role here (concrete subject of the outsourcing, effects of the measure on the bank, place of performance, complexity of the planned measure, suitability of potential service providers, etc.). Finally, a risk analysis will also determine – or conclude – whether an outsourcing is to be regarded as material or non-material. The risk analysis will help the bank to become aware of the risks associated with the outsourcing.

In June 2017, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an updated version of its framework entitled “Enterprise Risk Management – Integrating with Strategy and Performance”, which highlights the importance of the interplay between strategy, risk management and a company’s performance.

We carried out a validation for this use case based on two bank-fintech UCs. Two different banks and fintechs were involved.

**Kontakt**

Association of German Banks
Burgstraße 28
10178 Berlin
Germany