

■ Digital risks in the banking sector

The advancing digitalisation of the world in which we live and work is putting German banks to the test. The resulting intensification of competition in financial services as well as customers' expectations have been putting them under significant pressure to adapt and evolve for a number of years now. New technologies such as artificial intelligence and the widespread use of scalable cloud services are accelerating the digital transformation. Information technology's current support of banking processes will become more pronounced as a result.

Over the course of the digital transformation, it is important not to lose sight of security, particularly in view of the fact that banks are increasingly becoming a target for professional hackers. Banks need to ensure that their customers' data are available at all times, secured against unwanted changes and protected against unauthorised access. Technology alone is not enough to stay ahead of digital risks. The human component as well as technical and organisational measures, together with well-structured, effective and interlinked processes, are the key factors for success.

To ensure that the scope needed to implement measures is always available, banking supervisors rely on an approach to regulation and oversight that is oriented around principles and processes. In this context, expectations are outlined in greater detail in a technology-neutral manner in the circulars Minimum Requirements for Risk Management (MaRisk) and the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT). These also make it possible to effectively supervise bank-internal processes based on current and future technological developments such as cloud computing and artificial intelligence.

Within the framework of the supervisory review and evaluation process (SREP), in particular by conducting inspections at banks, the Bundesbank assesses not only financial risks but also non-financial ones, such as digital risks. Although steady improvements can be seen in risk management processes, basic vulnerabilities and a need for improvement are identified time and again when it comes to addressing digital risk – particularly with respect to information risk management, information security management, and outsourcing management – and these are monitored closely by supervisors.

Digitalisation will continue to shape societal and economic developments, and the pace of technological change will remain high, especially in the banking sector. The Bundesbank has always taken a positive view of technological progress among banks, as digital innovation bolsters German banks by rendering them more competitive and profitable, and therefore more stable and resilient. Banks' long-term success nevertheless depends heavily on the consistent and proper use of innovative technologies. The Bundesbank will continue to promote the principles-based and technology-neutral regulation of digital risks at both the European and global levels. Technological progress needs to be facilitated, as does the proportionate and autonomous implementation of regulation at institutions. Only if institutions take the initiative and face up to the opportunities and risks presented by digitalisation in a confident and balanced manner will it be possible to safeguard the functioning of the financial system over the long term.

Digitalisation is changing banking

Information technology defines banking business

The way in which banks operate has always been highly influenced by the technology that is available. Nowadays, a functioning and modern information technology (IT) infrastructure is essential for an ever larger proportion of financial services and products.

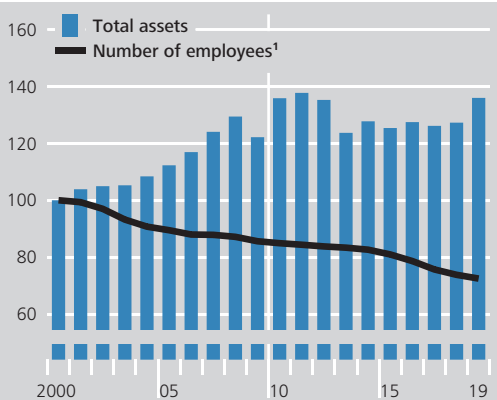
For example, the number of employees in the German banking industry has fallen continuously over the past two decades, while total assets have risen by approximately 50% over the same period. This productivity boost was made possible not least due to the increased use of IT. Today, running a bank without IT is unimaginable.

Digitalisation creates new opportunities ...

The sharp rise in the performance and interconnectivity of IT over the past few decades has made it possible to transfer and process huge volumes of data in very short spaces of time. Technologies such as artificial intelligence and machine learning use these volumes of data to carry out increasingly sophisticated processes, tasks and analyses in an autonomous and highly automated manner. Furthermore, new applications are continuously being developed through agile methods by drawing on their iterative and incremental approaches.

Total assets and employees in the German banking industry

2000 = 100



1 Source: Statista.
 Deutsche Bundesbank

These organisational and technological innovations are sustainably transforming not only the expectations of bank customers, but also the way in which financial services are offered and provided.

Digitalisation is also accompanied by a division of labour that was not possible in the past. Today, more than ever, banks can decide whether they provide services themselves or procure them from third parties. For example, specialist banking applications, including core banking systems, no longer need to be developed by banks themselves, but can instead be purchased from third parties and even run on their external IT infrastructure. Globally active providers thus offer quick, flexible and straightforward access to computer resources with almost unlimited options for customisation (see the box on pp. 51 ff.).

... accompanied by a sharper division of labour

At the same time, the intense competitive environment has, for a number of years now, been putting strong pressure on institutions to adapt both themselves and consequently their business models. Through the continued transformation and outsourcing of operating processes, banks are hoping particularly to achieve shorter provisioning times, better service quality and lower operating costs.

Institutions face rising pressure to adapt ...

The COVID-19 pandemic has considerably ramped up the trend towards digitalisation once again. For example, services have had to be provided to customers increasingly via digital channels for more than a year now. Simultaneously, an as yet unknown number of employees have been working from home. To make this possible, institutions were forced to invest more heavily in new hardware and software and to digitise previously analogue processes.

... not least owing to COVID-19 pandemic

The Bundesbank has always taken a positive view of technological progress among banks. This also holds true for digitalisation because digital innovation bolsters German banks, making them more competitive and profitable, and

Bundesbank promotes digital innovation through various initiatives ...

Cloud computing

The trend towards outsourcing information technology (IT) processes has been picking up pace for a number of years now and is having a positive impact on digital transformation in the financial sector. As a result, the market has seen the emergence of new specialised service providers and technologies. The new tasks facing banks, supervisors and service providers stemming from digital transformation and how these can be managed can be illustrated using cloud computing as an example.

The use of third-party IT services is generally classed as outsourcing in cases where third parties are appointed to carry out bank transactions as well as financial or other institution-specific services.

The legal provisions pertaining to institutions' risk management of outsourcing and other external procurement of IT services are set out in Sections 25a and 25b of the German Banking Act (*Kreditwesengesetz*) and are outlined in greater detail in the BaFin Circular on the Minimum Requirements for Risk Management (MaRisk), and the Supervisory Requirements for IT in Financial Institutions (BAIT).

Outsourcing to cloud service providers

Shorter technology cycles, mounting cost pressure and specialisation are all reasons for institutions to outsource IT activities and processes, especially to providers of cloud services. Moreover, cloud services also provide smaller institutions with an efficient means to access modern technology, such as artificial intelligence and machine learning.

The US standards agency NIST (National Institute of Standards and Technology)

defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computer resources (e.g. networks, servers, storage systems, applications and services) that can be provisioned rapidly and released with minimal management effort or service provider interaction."¹

Cloud computing provides standardised IT services thus enabling such services to be provisioned with the highest degree of automation possible. Given customers' flexibility to use and scale these IT resources as required, institutions also hope that their cost structures will become more efficient as a result. In addition to increased flexibility, institutions are aiming for greater freedom in procuring services as well as improved availability and performance compared with their own IT infrastructures, which have usually evolved over a longer period of time.

Compared with 2018, when 91% of institutions still chose to operate their IT infrastructure themselves, according to a study conducted by PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft ("PwC") more and more institutions are now turning to third-party IT services.² Here a small number of large enterprises dominate the market; they share almost 60%³ of the global supply of cloud computing services.

Outsourcing to cloud service providers is, in general, subject to the same requirements regarding the management of outsourcing

¹ See Federal Office for Information Security (2021).

² See PwC (2021).

³ See Statista (2021).

and services as outsourcing to other (IT) service providers. The Federal Financial Supervisory Authority (BaFin) and the Bundesbank have formulated a joint assessment on outsourcing to cloud service providers and published this in a Guidance.⁴

Risks, challenges and current developments

Institutions that outsource to cloud service providers also have to set up processes to manage the risk arising from inadequate or failed internal processes, people and systems or from external events, including legal risk (operational risk).

If an institution wants to use cloud services, the impact of cloud computing has to be considered from the outset, starting as early as in the strategy process. Before migrating to cloud services, the IT landscape usually has to be standardised and internal processes adapted.

From the Bundesbank's perspective, but also from the perspective of the institutions' risk management and internal control functions, outsourcing to cloud service providers also presents particular challenges with regard to monitoring and managing outsourced services and the service provider itself. This results, in particular, from the size and complexity of the organisation, and the technology used by the large cloud service providers.

When using cloud computing, there is a risk that an institution – for legal, organisational or technical reasons – may become tied to one provider and can only switch to another provider with great difficulty (a state known as "vendor lock-in"). Supervisors expect institutions to consider these risks and analyse potential alternatives before concluding a contract.

Institutions are further hampered by their limited negotiating power with cloud service providers operating on an international or inter-sectoral scale. At the same time, cloud service providers are confronted with a large number of – essentially – similar requirements from the financial and banking sector.

The internal audit function of an institution has to examine and assess in a risk-oriented and process-independent manner the effectiveness and appropriateness of the risk management system and of the internal control system as well as the appropriateness of all activities and processes in general, even if they have been outsourced. Due to the size and complexity of cloud service providers, this is virtually impossible for individual institutions to achieve by themselves, which can obstruct audit activities.

Institutions are therefore increasingly turning to pooled audits, an approach already established under the Minimum Requirements for Risk Management (MaRisk). Auditors from several institutions come together to conduct on-site audits of cloud service providers in order to pool know-how and secure an efficient use of resources where audit areas overlap.

An institution must nevertheless still ensure that its contract monitoring, risk management and internal audit can keep pace with developments in IT and outsourcing. This also requires looking at the cloud service provider's structures, processes and tools in place to ensure transparency, for instance in the case of security incidents, at the extent to which risk-mitigating measures have been implemented and at test and audit results.

⁴ See Federal Financial Supervisory Authority (2018).

For supervisors, it will become increasingly important to analyse institutions' dependency on IT services. Concentration risk could lead to systemic risk. The European Banking Authority's Guidelines on outsourcing arrangements, which have currently been implemented in the German Banking Act and the corresponding statutory orders as well as in MaRisk, address this inter alia with new requirements to set up an outsourcing register for institutions and to report outsourcing information to supervisors.

therefore more stable and resilient. The Bundesbank itself is taking numerous initiatives in order to better fulfil its stability mandate through the use of digital technologies, including in the field of banking supervision.

... networks internally and in the central banking community ...

Digital innovation is not primarily concerned with technology per se, but rather with how to use it in a meaningful way. As a result, the Bundesbank has set up a common platform within the Eurosystem for cooperation across business units on projects and topics surrounding the digital transformation at the Bank. In cooperation with the Banque de France, the Bundesbank runs the Eurosystem's BIS Innovation Hub in Frankfurt, which focuses on modern technologies aiming to support financial supervision (SupTech and RegTech) as well as cybersecurity and sustainability issues (green finance).

... and beyond

The Bundesbank also has networks outside of the central banking community, such as in the

start-up scene, where it is an institutional partner of the TechQuartier innovation platform in Frankfurt, which brings together enterprises, innovators, academic institutions, as well as the financial and public sectors. This may provide the Bundesbank with additional impetus when coming up with ideas for its own digitalisation projects and also allows the Bank to pass on its own experiences.

However, new technologies and types of procurement must not endanger the institutions' security. Dependence on functional and secure IT has risen, as failures in key IT systems, such as core banking, payment or trading systems, can have a severe impact on the ability of an institution to provide its services. Customers become particularly aware of this when online banking or cash machines do not function as normal, or when payments or security orders are executed incorrectly or not executed at all. The threat of cyberattacks is another growing challenge for institutions and the wider finan-

Use of technology must not jeopardise security

cial system. Hackers are benefiting from the growing level of technical complexity and are themselves becoming more professional in terms of how they operate. Hackers are particularly interested in payment systems, which can be targeted in order to fraudulently transfer funds, for example, and in core banking systems, which are a prime target for extortion due to the damage that could be caused by taking them down. If hackers gain access to business-critical data, they encrypt these data using ransomware, for instance, so that they can then demand a ransom for their decryption. Furthermore, attacks can take down or otherwise interfere with a bank's key IT systems for communicating with customers, such as its website or email system.

Protection against digital risks required

The broad application and intensive use of IT therefore call for a greater focus on compliance with the necessary security requirements. Banks need to manage the digital risks associated with digitalisation in a reliable way, which means that their and their customers' data are available at all times, secured against unwanted changes and protected against unauthorised access.

Outlook of banking and financial supervision on digital risks

Supervisory approach to digital risks

The financial system is intended to ensure the efficient and cost-effective provision of financial resources and services to economic agents and individuals. Banking supervisors are tasked with monitoring the business activity of credit institutions by guaranteeing the efficiency and stability of the banking system.

Secure use of IT requires the successful combination of human components with organisational and technical measures – it is therefore not enough to focus solely on technology. In

addition, well-structured and effectively implemented processes are a key factor for success in managing digital risks. Supervisors are thus taking an approach that is targeted towards analysing systems, not only with regard to the functioning of individual elements of risk management, but with respect to how these elements interact with each other within the risk management system and how they are embedded in the bank's integrated performance and risk management strategy.

As with other material risks, an approach towards regulation and monitoring that is based on principles and processes has proven to be effective. For instance, the organisational duties under Section 25a and Section 25b of the German Banking Act (*Kreditwesengesetz*) are intended to ensure that credit institutions have adequate risk management, and this also covers outsourced processes.

The circulars issued by the Federal Financial Supervisory Authority (BaFin) on the Minimum Requirements for Risk Management (MaRisk) and Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT – BAIT*) outline in greater detail the expectations of the Banking Act in a technology-neutral manner. They reflect European requirements and the supervisory experience gleaned from IT inspections.

The Bundesbank and BaFin collaborate closely in drafting the circulars. Amongst other things, the Bundesbank relies on its practical experience gained from conducting on-site inspections. This, alongside discussions in expert panels and public consultations, has made it possible to structure the regulatory framework in line with practice. The specific information in the circulars is not exhaustive, as institutions also need to be aligned with the current standards and best practices on how to deal with digital risks.

These supervisory requirements are formulated on the basis of principles and leave it to the in-

Supervisors pursue holistic approach and require appropriate risk management processes












Institutions need to limit digital risks

BAIT requirements flesh out expectations regarding governance of digital risks ...

... reflect international requirements and many years of experience from inspections ...

What are the prudential requirements for IT in banks?

Selected topics from the 2021 BAIT amendment

MaRisk ¹	BAIT ²
Strategies	 IT strategy <ul style="list-style-type: none"> – Management is responsible for the IT and information security strategies – Orientation of IT and information security in line with established standards
Internal control system	 IT governance <ul style="list-style-type: none"> – Effective IT organisational and operational structure – Risk control processes and adequate allocation of resources
Organisational guidelines	 Information risk management <ul style="list-style-type: none"> – Up-to-date overview of IT systems and their dependencies – Regular review of the implementation of security measures
Documentation	 Information security management <ul style="list-style-type: none"> – ISO³ is responsible for defining and monitoring security measures – Regular review, awareness-raising and training on information security
Staff	 Operational information security <ul style="list-style-type: none"> – State-of-the-art security measures and processes – Permanent monitoring and independent review of IT system security
Reports	 Identity and access management <ul style="list-style-type: none"> – Access to IT systems and premises are restricted and monitored – Regular review of access rights granted
Technical and organisational resources	 IT projects and application development <ul style="list-style-type: none"> – Management and monitoring of IT projects/project portfolio – Secure development of application incl. comprehensive tests and documentation
Segregation of duties	 IT operations <ul style="list-style-type: none"> – Monitoring of IT systems, regulated implementation of changes and troubleshooting – Reliable data backup and management of capacity needs
Adjustment processes	 Outsourcing and other external procurement of IT services <ul style="list-style-type: none"> – Management of risks arising from other external procurement of IT services – Regular review of risk assessments and contracts with service providers
Outsourcing	 IT service continuity management <ul style="list-style-type: none"> – Identification of time-critical IT processes and precautionary measures for their failure – Annual review of the efficacy of these precautionary measures
Business continuity management	 Management of relationships with payment service users <ul style="list-style-type: none"> – Duty to provide information on security-related aspects to payment service users – Payment service users must receive technical and organisational support
ZAIT ⁴	

¹ Minimum Requirements for Risk Management. ² Supervisory Requirements for IT in Financial Institutions. ³ Information security officer. ⁴ Payment services regulatory requirements for the IT of payment and e-money institutions.

... and permit new technologies and methods

stitutions themselves to decide which technologies or methods they wish to employ. This means that current developments such as cloud computing are also regulated in principle. The principles-based requirements even allow effective supervision of artificial intelligence and machine learning. In this context, it is essential to identify new methods and risks early on and to direct supervisors' focus towards them (see the box on pp. 57 ff.).

The Bundesbank's role in addressing digital risks in the banking sector

Operational banking supervision in Germany conducted by Bundesbank

Working in conjunction with BaFin, the Bundesbank supervises around 1,650 credit institutions in Germany. Cooperation in the off-site supervision of institutions is governed by Section 7(1) of the Banking Act and the Prudential Supervisory Guideline (*Aufsichtsrichtlinie*). The bulk of the Bundesbank's work is carried out in its nine regional offices, in geographical proximity to the institutions. Since 2014, the Bank has also been part of the Single Supervisory Mechanism (SSM) for the supervision of significant institutions (SIs) in Europe, in which it also plays an important operational role through its participation in joint supervisory teams.

Information on digital risks assessed through off-site supervision

The cornerstone of supervisory activity is the supervisory review and evaluation process (SREP). In addition to financial risks, non-financial risks, including those of the digital variety, are also assessed within this framework. Starting this year, the information required for this purpose has been collected not only from SIs¹ but also directly from less significant institutions (LSIs) using a structured questionnaire. This is used as a basis for performing a supervisory assessment of the potential digital threat facing an institution and how this is handled in the institution's internal risk management system.

On-site inspections provide the Bundesbank with a deep insight into institutions' business

operations and, in particular, their risk management. The Bundesbank's inspections are commissioned by BaFin in the case of LSIs and by the European Central Bank in the case of SIs. For IT inspections, the scope of the inspections relates to the organisational and technical requirements set out in Sections 25a and 25b of the Banking Act and the further details on these provided in the MaRisk and BAIT circulars. These system inspections are designed to assess the adequacy of risk management in light of the specific circumstances of each institution. The resulting ability to gain an overall picture of an institution's digital risks as well as the process-oriented approach to IT inspections has proved to be a very effective way of working for the Bundesbank.

Over the last decade, the Bundesbank's inspections of institutions and their IT service providers have increasingly focused on IT-related aspects and identified or brought about steady improvements in risk management processes. However, they frequently also detect fundamental vulnerabilities, problem areas and points for improvement with respect to addressing digital risks. Since 2010, the Bundesbank has carried out more than 2,000 on-site inspections and found material risk management deficiencies in almost half of all inspections. Around 15% of these findings related to IT issues, primarily in the areas of information risk management, outsourcing management and information security management.

In addition to raising awareness of these issues through its inspections, the Bundesbank works towards the permanent elimination of deficits by continually monitoring them and conducting follow-up inspections. Supervisors thus continue to attach a great deal of importance to the topic of digital risks, particularly since the inspections routinely highlight the tasks

On-site inspections provide comprehensive overview of digital risks and reveal potential for optimisation

¹ See <https://www.bankingsupervision.europa.eu/ecb/pub/html/ssm.aroutcomesrepitriskquestionnaire202007-9ed9a aa17d.en.html>

Artificial intelligence and machine learning

The increased performance of IT infrastructure and advances in the application of machine learning processes open up the possibility of the banking industry, too, using such innovative processes in both front and back office areas, for example in rating systems. From a supervisory perspective, the use of such processes in risk measurement and risk management systems is of particular interest. Manual processes and conventional risk models are replaced with artificial intelligence (AI) or machine learning (ML) processes, collectively referred to as ML methods for short. In this context, the term “AI” refers to the aim of using computer systems to perform complex tasks that traditionally have required human intelligence.¹ ML is focused less on replicating human intelligence and more on applying learning processes such as neural networks – which are capable of mapping complex, non-linear relationships – and ensuring they can be deployed efficiently in decision-making processes. However, ML methods also give rise to new risks that need to be assessed by banking supervisors and ultimately contained.

Relevant ML methods

There are many different approaches to defining ML.² In order to delineate the areas that are relevant to banking supervision, it is therefore necessary to formulate a pragmatic approach to identifying innovative models and their associated risks. The Bundesbank has thus chosen to base its considerations on a three-dimensional ML scenario.³

– The first dimension, which comprises the dataset and methodology, describes the complexity of an ML method. For example, if banks make use of deep neural networks, this leads to a high degree of

complexity. On the other side of the spectrum are traditional statistical methods, as have been used in the financial sector for decades (such as logistic regressions or expert systems).

- The second dimension is based on the ML method itself and describes how the output is used. It thus represents the significance of the method within the risk management process. Here, account should be taken of how much weight the ML method has within the overall model as well as of how, and with what impact, its output is used in areas relevant for supervision. If these first two dimensions are particularly strongly pronounced, the inspection techniques and inspection intensity of supervisory practices must be adapted.
- The third dimension relates to outsourcing and IT infrastructure. Supervisors have proposed a technology-neutral approach that, in particular, makes no distinction between in-house development and outsourcing or between underlying IT infrastructures. As central service providers and fintech companies are expected to be the driving force behind the development of ML methods, there are plans to carry out prudential on-site inspections – within the scope of the existing regulatory framework for outsour-

¹ See Financial Stability Board (2017).

² Definition by the Financial Stability Board (2017): “Machine learning may be defined as a method of designing a sequence of actions to solve a problem, known as algorithms, which optimise automatically through experience and with limited or no human intervention.” Mitchell (1997): “A computer program is said to learn from experience E with respect to some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E.”

³ See Deutsche Bundesbank (2020a).

cing – at external service providers as well.

The role of current supervisory law

ML methods constitute neither their own supervisory area nor are they prudentially relevant solely due to the new technologies involved. Instead, these new methods can be largely assessed and evaluated for risk on the basis of existing process-oriented inspection frameworks. This applies, for example, to rating systems, which are in any case subject to approval, and to early warning systems, which have been operated in the past without the use of ML. The supervisory approach can be applied in a technology-neutral way, even if ML methods give rise to their own specific issues. Primarily, it is a matter of identifying the differences that exist compared to traditional models and processes, and determining how supervisors can deal with these. Above all, there are differences with regard to explainability, model development and validation, and training cycles. In order for banks to have certainty of planning when investing in ML methods, supervisors should tighten their focus and communicate any new requirements in a transparent way.⁴

Explainability

Banks must be able to understand their own decision-making processes and justify the measures that they implement. Decisions should be based on causalities and functional relationships. By contrast, ML methods are successful mainly because they are able to independently recognise patterns within data without being provided with fixed causalities, and thus enable measures to be derived from these patterns. An inherent property of many ML methods is that, as a result of forgoing prior knowledge of causalities, they have a lack of explainability. This deficiency can be a

hindrance to applying these methods – specifically if causal explanations are required when using the output. Banks must therefore weigh up the benefits offered by ML methods against the disadvantages presented by this “black box” characteristic. To this extent, increased model performance and/or predictive ability, or a lack of other suitable methods, may justify the use of ML. However, it must be ensured that clear accountability is taken for decisions that are prepared chiefly, or even made entirely, by a black box method, and that these decisions are well integrated into comprehensive control processes. A number of approaches have been developed to make ML retroactively explainable (“explainable AI”, or XAI). These approaches are highly promising, as they provide selective and often intuitive insight into how ML methods function. However, caution is still needed, as no XAI approach is able to offer complete explainability. The degree to which this black box characteristic can be tolerated therefore depends on the ML scenario in each individual case.

Model development and validation

In comparison with traditional statistical procedures, ML methods exhibit particular features in their development and maintenance. As the volume, frequency and significance of data – including unstructured data – increases, so too does the importance of data quality and data preparation. There is a danger that inadequate data will be used to satisfy the high data requirements of ML methods, while the resulting consequences remain obscured due to their black box characteristic. However, insufficient data quality not only has an impact on

⁴ The Bundesbank and BaFin have put their perspective on ML methods up for joint consultation (<https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/maschinelle-lernverfahren>).

model development, but also makes validation more difficult, which is especially important in the case of black box methods.

Like all models, ML methods must therefore be integrated into a suitable control environment, too. This must ensure that model developers, validators and users are all equally convinced of the good quality of the model output, that accountability for errors is clearly regulated, and that both internal and external control units can gain adequate insight into the ML methods.

Training cycle

ML methods often allow for ongoing adjustment to take account of new data. This process, known as retraining, can either change the structure of the method and what are known as its hyperparameters,⁵ or be limited to optimising the method within

its existing framework. This way, a model can be brought closer to a changing reality (for example in the case of structural changes and breaks). Nevertheless, banks should be aware of the disadvantages of retraining – specifically, reduced continuity and comparability. It is crucial that banks justify the need for the selected training cycle. In particular, model validation that typically takes place in predefined cycles must also be able to sufficiently cover and comprehensively evaluate a model with ongoing retraining.

⁵ ML method parameters that are determined before optimisation.

that institutions were faced with and, in some cases, still are.

into sufficient depth or are carried out too infrequently.

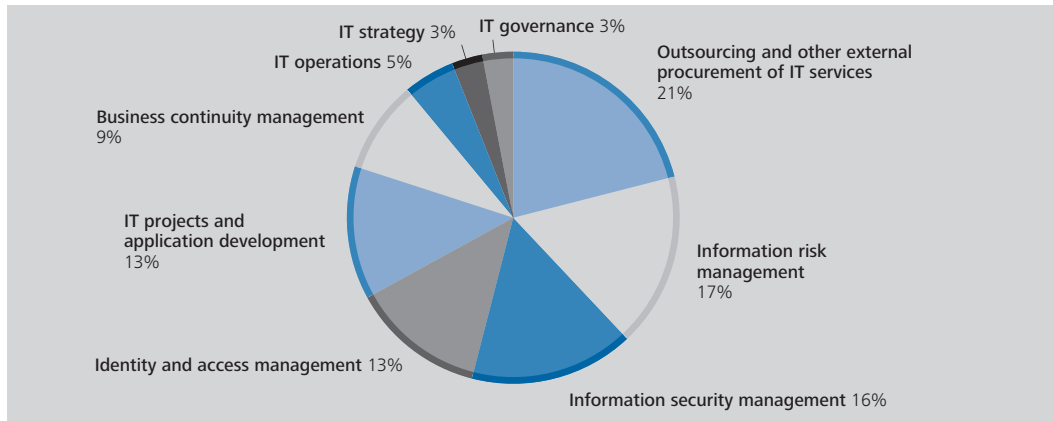
Institutions need to be more transparent about their digital risks ...

Information risk management is of particular importance in the management of digital risks. It represents a control loop in which safeguards are assigned to all IT components and risks, in particular from the incomplete implementation of these safeguards, are identified and monitored on an ongoing basis. Process deficiencies in information risk management can lead to the institution lacking transparency regarding digital risks and consequently not managing these appropriately. It is often observed that institutions lack a complete overview of their key IT components and therefore not all necessary elements can be factored into risk analyses. In addition, many institutions still need to set out complete and consistent requirements for the safeguards needed and implement the maintenance processes necessary for these. Where there are requirements to be met, reviews of actual compliance with these often do not go

Outsourcing management is the practice of managing and monitoring outsourced processes and the risks associated with these. This is mainly a decentralised process performed by the institution's outsourcing units, which should be supported by central units such as an outsourcing function or central outsourcing management. The core principle of outsourcing management is that, whilst an institution can outsource the processes themselves, it can never outsource responsibility for them. As such, each institution must have a sufficient level of expertise on hand to be able to fully oversee its outsourcing arrangements and outsourcing risks. Shortcomings in the outsourcing management process can result in digital risks, especially those relating to IT services, going undetected or being subject to no more than rudimentary assessment. Inspections have repeatedly found that services are not classified

... manage and monitor risks arising from outsourced processes and activities, ...

Material deficiencies identified by IT inspections conducted at German banks over the past ten years



Deutsche Bundesbank

as outsourcing and that risk analyses for determining the materiality of an outsourcing arrangement exhibit basic failings. Moreover, there are shortcomings related to the stipulation of information and audit rights in outsourcing contracts and to requirements regarding sub-outsourcing. Monitoring long or complex chains of outsourcing is a challenging task for outsourcing management.

security measures do not always go into sufficient depth or are carried out too infrequently.

In particular, attacks that exploit inadequate security measures have become one of the most significant digital risks and, due to the complex IT links between institutions, now pose a challenge to the financial system as a whole. The Bundesbank is making a vital contribution to enhancing the cyber resilience of Germany's financial sector on a lasting basis by conducting TIBER²-DE tests, as these tests determine how effectively an enterprise's defence mechanisms avert cyberattacks using attack scenarios that are as realistic as possible (see the box on pp. 61 f.).

Bundesbank supports voluntary review of financial sector resilience to digital risks

... and consistently employ effective, state-of-the-art security measures

Information security management involves defining and monitoring compliance with measures intended to safeguard IT under the direction of an information security officer. However, protection against hackers is only ever as good as the weakest link in the chain. Process deficiencies in information security management can prevent institutions from reaching an appropriate and consistent level of security. With that in mind, safeguards implemented to protect IT should always comply with the requirements set out in the prevailing standards, be in keeping with the state of the art and be tested regularly. However, if information security officers are too close to the operational units they are monitoring, there is a risk that they will not be able to carry out their work without conflicts of interest. Inspection practice shows that there is often catching-up to do in both of these areas. In addition, internal tests to assess the effectiveness of implemented

■ Outlook

The Bundesbank addresses digital risks in both SREP assessments and on-site inspections. As a voluntary instrument, TIBER-DE tests also help the financial sector to evaluate its resilience to digital risks. However, as the division of labour among market participants and their level of interconnectedness increase and technical and organisational innovations emerge, adjust-

Bundesbank plays a role in effective supervision of digital risks and adapts practices to new conditions

² Threat Intelligence-based Ethical Red Teaming.

TIBER-DE

As the pace of digital transformation picks up in the financial sector, so does vulnerability to cyberattacks. Against this backdrop, central banks are increasingly focusing on how to improve resilience to both internal and external attacks.

In summer 2019, the Bundesbank and the Federal Ministry of Finance implemented the European System of Central Banks' framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) in Germany as TIBER-DE.¹ The TIBER-DE implementation document was published in July 2020.² The aim behind TIBER-DE is to strengthen the cyber resilience of entities in Germany's financial sector and thus make a major contribution to keeping the financial system stable and up and running.

During a TIBER-DE test, ethical hackers carry out simulated attacks on an entity. The tests take place under controlled conditions and are subject to strict risk management. The objective is to determine how effectively the entity's defence mechanisms avert cyberattacks using attack scenarios that are as realistic as possible. To this end, information collected about the entity-specific threat situation is exploited during the TIBER-DE test using techniques applied by real hackers. Such attacks explicitly target the entity's critical functions and the corresponding live systems. For banks, this could be cash or cashless payment systems, lending systems or online banking. Unlike classic penetration testing, which focuses solely on technical vulnerabilities in systems, TIBER-DE tests also cover organisational shortcomings as well as the human factor in their attack scenarios.

Ideal candidates for TIBER-DE are large banks, insurers, financial market infrastructures and their critical service providers. Participation in TIBER-DE tests is voluntary and encourages entities to act on their own initiative and take a critical look at their own cyber resilience. To raise awareness of the growing threat posed by cyberattacks, the executive board of the entity being tested is involved in the process from the outset. A TIBER-DE test should not be seen as a pass-fail test; instead it is successful if it has been conducted in accordance with the framework.

The national competence centre for TIBER-DE – the TIBER Cyber Team (TCT) – is based at the Bundesbank and is separate from financial supervision in both organisational and procedural terms. However, financial supervisors are informed that a test is to be carried out and involved at set points in the proceedings. The TCT is overseen by a steering committee comprising representatives from the Bundesbank and the Federal Financial Supervisory Authority (BaFin). This steering committee defines the strategic objectives for TIBER-DE.

The TCT supports entities throughout the TIBER-DE test, providing them with the necessary expertise and checking compliance with the TIBER-DE framework. Once the test has been completed – a process which can take up to one year – the TCT provides attestation confirming that the entity's test was conducted in accordance with the framework.

¹ See Deutsche Bundesbank and Federal Ministry of Finance (2019).

² See Deutsche Bundesbank (2020b).

The TIBER-EU framework has been implemented in other EU Member States, too, for instance in the Netherlands, Denmark and Belgium. Those Member States that have already implemented TIBER-EU have agreed to mutual recognition of test completion. Close cooperation and a coordinated approach between the authorities involved and the entities should thus improve cyber resilience throughout the financial sector and appropriately counter the risks stemming from digital transformation.

There is high-level acceptance of and demand for TIBER-DE in the German financial sector. At the time of writing, the number of TIBER-DE tests that have begun already stood at nine.

TIBER-DE tests can make a major contribution towards strengthening cyber resilience. In particular, they enable participating entities to use a concrete attack scenario to test the interplay between various processes to thwart cyberattacks, the employees involved in these processes and the systems affected. TIBER-DE tests show that human error or a lack of security guidelines may render technologically sophisticated security measures ineffective. They also highlight shortcomings in existing processes and insufficient investment in safeguards, and convey these findings transparently to management. Raising management's awareness of specific cyber risks can help to pinpoint additional areas that require investment, tailor budget decisions more closely to security requirements and implement corrective measures in a more targeted manner.

TIBER-DE tests also show that attentive and informed employees are able to detect and ward off even sophisticated attacks early on if entities have well-defined internal security protocols and processes. Regular campaigns

to raise staff awareness of cyberattacks are one possible defence measure, and the effectiveness of such campaigns can be examined in TIBER-DE tests.

By implementing standardised TIBER tests in Germany, the Bundesbank is ensuring that entities' resilience does not just exist on paper but that this is also checked in practical terms and under real-world conditions. In view of the growing risk situation, TIBER-DE tests are therefore making a vital contribution to enhancing the cyber resilience of Germany's financial sector on a lasting basis.

ments also have to be made to the supervisory approach.

For example, in its updated principles for the management of operational risk³ and new principles for operational resilience,⁴ the Basel Committee on Banking Supervision recently gave the banking sector clear guidance on the design of the essential elements in dealing with digital risks and on how to address them. These principles are adopted by supervisory authorities in national frameworks and supervisory practice, amongst other things, and should be implemented proportionately by banks.

Furthermore, in drawing up the Digital Operational Resilience Act (DORA),⁵ the European Commission will create harmonised requirements for managing digital risks at institutions, increase transparency with regard to any possible concentration of digital risks, and strengthen financial supervisory authorities' ability to act with regard to banks and critical third-party IT providers. This outsourcing issue is also addressed in the Act to Strengthen Financial Market Integrity (*Gesetz zur Stärkung der Finanzmarktintegrität*),⁶ which was adopted by the Bundestag in May of this year.

Work is also being carried out to harmonise the supervisory approach to artificial intelligence and machine learning at the international level in the future in order to create a level playing field. In addition to the principles published by the Basel Committee on Banking Supervision, the European Commission is drafting a regulation on artificial intelligence that proposes harmonised rules to apply beyond the financial sector.⁷ However, taking machine learning as a case in point shows that the risks stemming from new technologies and methods can already be adequately addressed within the scope of existing regulatory requirements.

Digitalisation will continue to shape societal and economic developments, and the pace of technological change will remain high, especially in the banking sector. Institutions' long-

term success therefore also depends heavily on the consistent and proper use of innovative technologies. Institutions have to face up to this rapid transformation and play an active part in shaping it in order to be able to continue offering services relevant to their customers and thus remain structurally competitive.

The downside of digitalisation, however, is that the rising complexity and increasing division of labour in banking business is also causing the potential for risk to grow, especially where institutions continue to work with highly fragmented IT landscapes and technologies that have evolved over time. It is important to continue operating IT infrastructures and applications securely and enhance them as needed in order to protect sensitive customer data and ensure stable operation. To this end, banks need to have, first and foremost, a thorough understanding and must ensure that their digital risks are managed in an appropriate manner. The same applies to outsourced processes. This is the only way for institutions to keep their customers' trust and maintain the level of resilience needed as key factors for sustainable economic success.

The Bundesbank will continue to promote the principles-based and technology-neutral regulation of digital risks at all levels. Technological progress needs to be facilitated, as does the proportionate and autonomous implementation of regulation at institutions. In addition, the Bundesbank will continue to encourage institutions to be resolute in taking advantage of the opportunities offered by digitalisation. At the same time, however, it is necessary for banks to systematically strengthen the way in which they manage the risks that these entail in order to keep up with the growing digital

Banking business will continue to be shaped by digital transformation; ...

... it is thus essential to take a consistent approach to digital risks

Bundesbank will continue to promote principles-based, technology-neutral, real world-based and thus effective regulation of digital risks

³ See Bank for International Settlements (2021a).

⁴ See Bank for International Settlements (2021b).

⁵ See <https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:52020PC0595&from=EN>

⁶ See Federal Ministry of Finance (2021), *Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG)*.

⁷ See European Commission (2021).

risks. Only if institutions take the initiative and face up to the opportunities and risks presented by digitalisation in a confident and balanced manner will it be possible to safeguard the functioning of the financial system in the long term.

■ List of references

Bank for International Settlements (2021a), Revisions to the Principles for the Sound Management of Operational Risk, available at <https://www.bis.org/bcbs/publ/d515.pdf>

Bank for International Settlements (2021b), Principles for Operational Resilience, available at <https://www.bis.org/bcbs/publ/d516.pdf>

Deutsche Bundesbank (2020a), The Use of Artificial Intelligence and Machine Learning in the Financial Sector, available at <https://www.bundesbank.de/resource/blob/598256/d7d26167bceb18ee7c0c296902e42162/mL/2020-11-policy-dp-aiml-data.pdf>

Deutsche Bundesbank (2020b), Implementation of TIBER-DE, 8 July 2020, available at <https://www.bundesbank.de/resource/blob/848920/c38b564c6c5de80d9d6dbb0200ff895a/mL/tiber-implementation-data.pdf>

Deutsche Bundesbank and Federal Ministry of Finance (2019), TIBER-DE macht das deutsche Finanzsystem sicherer, 12 September 2019, available at <https://www.bundesbank.de/de/presse/presstexten/tiber-de-macht-das-deutsche-finanzsystem-sicherer-806020>

European Commission (2021), Artificial Intelligence Act, available at <https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>

Federal Financial Supervisory Authority (2018), Guidance on outsourcing to cloud service providers.

Federal Ministry of Finance (2021), Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG), available at https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-06-10-FISG/0-Gesetz.html

Federal Office for Information Security (2021), accessed on 25 May 2021 at https://www.bsi.bund.de/EN/Topics/CloudComputing/Basics/Basics_node.html

Financial Stability Board (2017), Artificial intelligence and machine learning in financial services.

Mitchell, T. (1997), Machine Learning.

PwC (2021), Cloud Computing im Bankensektor, accessed on 25 May 2021 at <https://www.pwc.de/de/finanzdienstleistungen/cloud-computing-im-bankensektor.html>

statista (2021), available at <https://de.statista.com/infografik/20802/weltweiter-marktanteil-von-cloud-infrastruktur-dienstleistern/>