BaFin’s Digitalisation Strategy
## Contents

### I. Introduction 3

### II. “Supervision and Regulation” area of activity 4

1. Baseline scenarios 4
2. Overarching goals 4
3. Status quo: What has BaFin already achieved? 4
4. Next steps 7

### III. “IT Supervision and security” area of activity 9

1. Baseline scenarios 9
2. Overarching goals 10
3. Status quo: What has BaFin already achieved? 11
4. Next steps 12

### IV. “Transformation of BaFin” area of activity 13

1. Baseline scenarios 14
2. Overarching goals 14
3. Status quo: What has BaFin already achieved? 14
4. **Next steps** 16
   4.1 Internal digitalisation 17
   4.1.1 Digitalisation of supervisory and support processes 19
   4.1.2 Evolution of supporting infrastructures 21
   4.2 Workplace resources 22
   4.3 Staff recruitment and continuing professional development 22

### V. Implementation and refinement of the digitalisation strategy 23
I. Introduction

Digitalisation is one of the pervasive topics of our time, and one that will change people’s lives like no other. Originally, the term “digitalisation” referred to the conversion of information from an analogue into a digital storage format and to delegating tasks previously performed by people to computers. This traditional technical interpretation still holds true, but when we talk of digitalisation today, we mainly mean “digital transformation”, in other words the far-reaching, progressive digital change that is manifesting itself in all areas of human life and that is also increasingly changing the face of the financial sector.

Whereas in the 20th century, digitalisation was mainly used for automating and optimising, for modernising private households and workplaces, and for networking computers, the focus since the early 2000s has been on technologies that are sometimes labelled “disruptive”, and sometimes “creatively destructive”. They have the potential to break open value chains and to give rise to new business models. And they make companies vulnerable in the true sense of the word.

This development is being fuelled by a phenomenon called “Big Data and Artificial Intelligence” (BDAI). Huge amounts of data are available that can be analysed, combined and used in a range of ways using artificial intelligence methodologies. These changes are also impacting the traditionally highly regulated financial market, which lives, to a greater extent than other markets, from the fact that its functionality, stability and integrity can be relied on.

BaFin’s job is to create a sound basis for this trust. Its primary objective is to safeguard and promote the proper functioning, stability and integrity of Germany as a financial centre within the framework of European integration and international cooperation, and to protect the collective interests of consumers. It also has to achieve all of this successfully in times of progressive digitalisation. BaFin must therefore ask itself three fundamental questions:

Three fundamental questions

- “Supervision and regulation” area of activity I What is the most appropriate supervisory and regulatory approach for addressing the market changes triggered by digitalisation?
- “IT supervision and security” area of activity I How can BaFin ensure that the innovative technologies, IT systems and data used by the supervised entities are secure?
- “Transformation of BaFin” area of activity I How will BaFin have to evolve further in light of progressive digitalisation – internally and at the interfaces to the market?

BaFin’s digitalisation strategy is designed to illustrate how it plans to respond in these three areas of activity. It is not starting from scratch in any of them: BaFin is already working and thinking digitally to a significant extent in many areas. However, BaFin is being guided by an ambitious benchmark: by the year 2025, it aims to be one of the leading supervisory authorities worldwide in terms of managing progressive digitalisation.

It can only achieve this in stages, which is why the digitalisation strategy starts by defining overarching goals for each area of activity. As well as the baseline scenario and the status quo, a selection of the next steps currently planned to achieve these goals is also described. In light of the constant digital transformation, a presentation like this cannot cover the full range of all the necessary measures. In addition, neither the overarching goals nor the routes to achieving them are static. They are evolving dynamically and must be continuously reviewed and realigned if necessary.
II. “Supervision and Regulation” area of activity

Basic question: What is the most appropriate supervisory and regulatory approach for addressing the market changes triggered by digitalisation?

1. Baseline scenarios

- **Technological innovations** Financial technology innovations that are significantly influencing the digitalisation of the financial services sector and that BaFin is focussing on include distributed ledger technology (DLT), which is also an umbrella term for example for blockchain technology and cryptotokens (“cryptocurrencies”), applications in the area of “Big Data and Artificial Intelligence” (BDAI), the interconnection of financial market participants (e.g. through application programming interfaces (API)) and cloud computing. Of course this list is not exhaustive; as the markets for new technologies such as quantum computing and innovative biometric processes become increasingly mature, a growing number of additional financial technology innovations will emerge.

- **New financial instruments and business models** The new technologies are reflected in new financial instruments and business models such as cryptotokens, initial coin offerings (ICOs) and token generating events (TGEs), the growing platformification in the financial market that takes such forms as open banking, white label banking, regulatory technology (RegTech), crowdfunding and robo-advice, and automated personal and collective portfolio management. The impact this is all having on the financial services sector and consumer behaviour is partly evolutionary, and partly revolutionary (disruptive).

2. Overarching goals

BaFin is following five overarching goals in the “Supervision and regulation” area of activity in light of the developments described above:

- **Also as a response to the dynamic pace of technology-driven market trends, it must ensure a comprehensive basic understanding in the long run.**

- **It can accurately categorise and assess the impact of digitalisation on the financial markets.**

- **Based on this, it can derive appropriate implications for supervision and regulation.**

- **It can anticipate future developments and track them from a supervisory perspective.**

- **It is permanently on an equal footing with the companies and institutions.**

3. Status quo: What has BaFin already achieved?

Among other things, BaFin has already taken the following steps in the “Supervision and regulation” area of activity, each of which serves at least one of the five overarching goals of this area of activity:
- **Hub-and-spoke concept implemented** BaFin has implemented a hub-and-spoke concept to enable it to keep pace with digitalisation-driven market developments and to capture and assess financial technology innovations on a cross-sector basis. The hub is formed by the Innovations in Financial Technology division (SR 3) that has been established in the President’s Office. It is connected to the relevant divisions and works closely with them. The hub-and-spoke architecture is used to identify financial technology innovations at an early stage, to formulate realistic scenarios for the near future and to elaborate implications for supervisors and regulators on that basis. In other words, on the one hand it means deriving supervisory consequences and potential courses of action, and extending the scope for supervisory action and reaction. On the other, the objective is to establish any need for regulatory change.

- **Benefits of integrated supervision** Within its hub-and-spoke architecture, BaFin consciously leverages the benefits of integrated supervision to ensure a holistic, balanced assessment of the many aspects and interactions of digitalisation for regulated and unregulated market participants and consumers.

- **Exchange with internal and external experts** The SR 3 division regularly exchanges information on innovative financial technologies actively with internal and external technology experts and other authorities in Germany and abroad. The findings obtained by SR 3 are processed by the division for internal purposes and made available to BaFin’s divisions.

- **Communication with specific target groups** On its website www.bafin.de, BaFin provides information tailored to specific target groups in the “Company start-ups and fintech companies” section. For example, it describes typical business models for the industry and their regulatory treatment in a form that is understandable even for addressees who have little experience in dealing with supervisory and regulatory issues. In addition to this initial information, BaFin also offers a “Contact form for start-ups and fintechs” that interested parties can use for enquiries to BaFin, for example on authorisation requirements. The forms are then forwarded to the competent teams to enable an initial response as quickly as possible.

- **Events organised** BaFin cultivates the direct exchange of information with new target groups from the fintech environment – for example at its BaFin Tech event, which was held for the second time in 2018 and aroused considerable interest. BaFin Tech addresses the implications of innovative financial technologies. It is aimed at new and established companies in the financial sector, especially fintechs, credit institutions, insurance undertakings, asset managers, software and hardware developers, as well as associations and researchers.

- **Report on Big Data and Artificial Intelligence (BDAI) published** In its report “Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services” report (BDAI report), which was developed in cooperation with Partnerschaft Deutschland, Fraunhofer IAIS and the Boston Consulting Group, BaFin comprehensively addresses the (supervisory and regulatory) implications of using BDAI in the financial services industry. The report was published on 15 June 2018 and is expected to be made publicly available for consultation on www.bafin.de.

- **Administrative practice aligned** The existing regulatory framework is competition- and technology-neutral, principle-based and designed in such a way that it is proportionate to the relevant risks. This offers two advantages: first, there is no risk that the existing regulatory arrangements will suddenly become totally outdated. Second, BaFin can react flexibly to changes in practice and adapt its administrative activities. It has already done this on several occasions, as shown by the following examples:
  - **Video identification procedures** BaFin issued Circular 3/2017 on video identification procedures, modifying its know-your-customer requirements. All obliged entities under the

---

1 See III 3 regarding changes in the “IT supervision and security” area of activity.
Money Laundering Act that are supervised by BaFin can therefore use the video identification procedure.

- **IT competency among management board members** For BaFin, ensuring that banks and insurance undertakings can confidently tackle the challenges posed by digitalisation is a matter of pivotal importance. At the end of 2017, BaFin therefore modified its administrative practice in relation to the practical experience required by management board members on a cross-sectoral basis. The new administrative practice was described in an article in BaFinJournal (December 2017 issue), which can be downloaded from www.bafin.de. By adapting its administrative practice, BaFin is providing greater scope for the appointment of IT specialists when it comes to weighing the increasing need for specialist knowledge against the requirements for essential professional qualifications that the management board needs in order to fulfil its collective responsibilities.

- **Classification** Bitcoin and other cryptocotkens are units of account and hence financial instruments under the German Banking Act (Kreditwesengesetz). BaFin already classified them as such in 2011, a global innovation at the time.

- **Classification of tokens** In an advisory letter\(^2\) published in February 2018, BaFin clarified that initial coin offerings (ICOs) do not exist in a regulatory vacuum, but – depending on the structure of the tokens – are subject to the applicable prudential requirements. In other words, the provider requires, for example, authorisation under the German Banking Act the German Investment Code (Kapitalanlagegesetzbuch), the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz) or the German Insurance Supervision Act (Versicherungsaufsichtsgesetz), or has to comply with the requirements governing prospectuses.

- **Competition-neutral supervision of fintechs and new market participants** Based on the existing technology-neutral, principle-based, proportionate, reasonable regulatory framework, BaFin ensures the risk-based, competition-neutral supervision of both established and new market participants. In its supervisory practice, BaFin expressly does not follow any sandbox approach, but is guided by the proven principle of “the same business, the same risk, the same regulation”. As a consequence, fintechs are – depending on their business model – supervised just like other banks, insurance undertakings, portfolio managers etc. The same applies to providers of automated advisory offerings (robo-advice). The only differences that BaFin makes relate to the intensity of supervision – depending on the risk involved – where it applies the principle of proportionality.

- **Macro-prudential supervision**

  - **Financial Stability Committee** The progressive digitalisation is also a topic at the Financial Stability Committee (FSC), in which the German Federal Ministry of Finance (Bundesfinanzministerium) and the Bundesbank are represented in addition to BaFin. The FSC addresses various aspects of digitalisation and their potential impact on financial stability. For example, BaFin initiated a discussion by the FSC on the outsourcing of IT services by credit institutions and the national implementation of the G7’s fundamental elements of cyber security. In addition, BaFin works closely with the Bundesbank, which also monitors digitalisation and its consequences in the macro-prudential supervision of the financial markets.

  - **Strategy and Risk Committee** BaFin’s Strategy and Risk Committee (SRC) also repeatedly addresses various aspects of digitalisation and connects the macro and micro perspectives on a cross-sectoral basis. The Bundesbank’s attendance at SRC meetings additionally promotes this connection.

- **Consumer protection** In times of progressive digitalisation, BaFin also does all it can to accomplish its mission of protecting the collective interests of consumers, as shown by the following examples:

\(^2\) “Supervisory classification of tokens or cryptocurrencies underlying “initial coin offerings” (ICOs) as financial instruments in the field of securities supervision”.

---
• **Consumer warning on risks of ICOs** I In November 2017, BaFin warned consumers about the risk of losses if they invest in ICOs.

• **Consumer information on BaFin’s website** I BaFin regularly informs consumers about issues relating to digitalisation under the heading “Digitalisation and fintechs” at www.bafin.de.

• **Events** I Additionally, BaFin regularly informs consumers about innovative financial technologies at trade fairs, stock exchange events and its own events.

• **Supervision of violations of statutory provisions** I Although data protection authorities are responsible for monitoring the implementation of data protection requirements, if there is evidence that an institution or company frequently violates data protection standards, this may constitute an irregularity that also concerns BaFin. In cases like this, BaFin will take appropriate measures as part of its supervisory activities.

### 4. Next steps

In the “Supervision and regulation” area of activity, BaFin is planning the following steps, among others. Each of them serves at least one of the five overarching goals of this area of activity:

• **Continue monitoring the markets** I The momentum and speed of progressive digitalisation require BaFin to continue closely monitoring developments in the markets. Going forward, BaFin will continue to use the hub-and-spoke architecture described above to enable it to identify financial technology innovations in the various financial market sectors at an early stage and assess their consequences, including for consumers. Further in-depth studies and reports – which will also involve external experts – will supplement these observations and analyses. **Continuous implementation**

• **Identify the need for change in supervision and regulation** I Based on the monitoring described above, the SR 3 division is developing future scenarios in coordination with the other divisions. Using these scenarios, BaFin reviews whether its administrative practice still adequately captures the digitalisation-driven trends on the financial markets (see below). It also derives from this the need for any regulatory changes (see below). **Continuous implementation**

• **Adapt administrative practice if necessary** I If BaFin establishes that its administrative practice will no longer do justice to digital transformation in the foreseeable future, it will adapt it quickly.\(^3\) In doing so, it continues to be guided by technology- and competition-neutrality, proportionality and risk orientation. BaFin also advocates appropriate, up-to-date supervisory practice at the European level, for instance at the European supervisory authorities and within the framework of the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM). **Continuous implementation**

  • **Digital declarations (screening standards)** I Wherever possible, BaFin wants to offer administrative services electronically and hence adapt its administrative practice to the digital age. To do this, it plans to systematically scrutinise standards that run counter to this sort of administrative practice. Background: Federal administrative law currently stipulates several thousand requirements for written form. The acceptance of digital declarations – for example by email – is being impeded by existing legal requirements governing form. BaFin is striving to contribute its expertise at federal level in the form of recommended amendments to the relevant statutory provisions.

• **Address the need to adapt the regulatory framework** I Current supervisory law is technology-neutral and principle-based, but BaFin presumes that digital transformation will make it necessary to adapt it. BaFin is addressing this need for regulatory change, which is likely to arise repeatedly, with the

\(^3\) See III.4 regarding future changes in the "IT supervision and security" area of activity.
BaFin believes that a need for regulatory change is emerging in the following areas, and this should be examined in greater detail:

- **New business models** There may be a need to adapt regulatory requirements in particular where disruptive technological innovations produce new business models that are as yet unregulated. BaFin monitors the market closely for such innovations.

- **Risk transfer** There may also be a need for adaptation if risks associated with existing business models are transferred, for example if core banking processes are outsourced and unregulated market participants occupy the customer interface. BaFin will continue to keep track of this issue. It will also examine how supervised entities or their management can discharge their responsibilities if they no longer themselves occupy the customer interface and (now merely) function as an (infrastructure) provider in a distributed value network.

- **Potential efficiency gains and cutting red tape** In light of digitalisation, supervisory law may offer opportunities for efficiency gains and cutting red tape. It is important to analyse this continuously. One option, for instance, would be to simplify or reduce reporting obligations.

- **Big Data and Artificial Intelligence** In its “Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services” report (which BaFin has now made available for public consultation), among other things BaFin addresses the possible supervisory and regulatory implications of BDAI technology. Examples of the questions raised by the report include:

  - **New risks at interfaces** Because of the stronger interconnectedness and the increasing complexity of market activities, new risks can arise at the interfaces between market participants – both indirectly, for example because they use the same models, data and platforms, and directly through new contractual and trading relationships that will only emerge from the use of BDAI. The structure of this dynamic market and the resulting risks must be analysed.

  - **Redefine systemic importance** BDAI could create new types of systemically important entities (for example data, platform and algorithm providers). However, systemic importance could also result from the interaction of various market participants. As a result, traditional supervisory indicators would then be unsuitable for identification. In addition, familiar risk mitigation measures such as capital add-ons may not have the intended effect. The question therefore arises as to whether and how the concept of systemic importance, which is dominated by banking and insurance considerations, must be further refined in order to do justice to new business models and market structures.

  - **Responsibility cannot be transferred** BDAI will create further opportunities for automating standard market processes. However, responsibility for the results of BDAI-driven processes cannot be delegated to machines. It is therefore important to establish the right regulatory and supervisory framework when designing (partially) automated systems.

---

4 See also the “IT supervision and security” area of activity.
processes and to ensure they are embedded in an effective, appropriate and proper business organisation.

- **New governance concepts** I It might be necessary to extend existing governance concepts to automated processes as automation continues to grow.
- **BDAI in internal models** I The question arises of whether all BDAI methodologies are suitable for use in internal models that have to be authorised by the supervisor. An additional analysis is needed to determine whether the existing statutory (minimum) requirements applicable to the data used and the model transparency are adequate or should be extended. In the case of dynamic BDAI models, it must also be discussed which adaptations constitute a model change in the supervisory sense. The regulated entities would have to notify such a change and have it approved if necessary.
- **Consumer protection** I The BDAI phenomenon also raises several regulatory issues of relevance to consumers that BaFin will focus on: for example, unlawful discrimination must be avoided. If the objective is still to provide access to financial services to as many people as possible, it is also important to consider adapting the regulatory regime in such a way that sufficiently data-minimising or conventional financial services are offered as alternatives. Doing this would counteract the effective obligation to disclose personal data. The question of how data minimisation or conventionality should be defined and which financial services should be included needs further discussion. BaFin is more than willing to participate in this debate.

### Consultation and publication series

To answer these and further regulatory questions about digitalisation and issues surrounding BDAI, BaFin is consciously seeking an exchange of views with the public. For example, it made available the “Big data meets artificial intelligence - Challenges and implications for the supervision and regulation of financial services” report available for public consultation in the summer of 2018 and will report on the results in the second issue of its new “BaFin Perspectives” series. This series of publications is published in German and English on BaFin’s website. The first issue of “BaFin Perspectives” is also devoted to the topic of digitalisation. In addition to the President and other BaFin authors, external experts also have their say. BaFinJournal also reports regularly on how BaFin deals with the consequences of digitalisation.

### III. “IT Supervision and security” area of activity

**Basic question:** How can BaFin ensure that the innovative technologies, IT systems and data used by the supervised entities are secure?

1. **Baseline scenarios**

   Progressive digitalisation means that IT risks and hence also cyber risks are becoming increasingly important.
- **IT risks of individual institutions and companies** Today, information technology already constitutes the underlying infrastructure for all processes at financial services providers. The availability of the IT infrastructures and the integrity, authenticity and confidentiality of the data to be processed are of central importance for the proper functioning of the individual institutions and companies – and for their customers.

- **Systemic importance** Because of the high degree of interconnectedness in the financial sector, there is a risk, for example, that failures in the IT infrastructure might spread to other market participants and have a greater, and possibly even systemically important, range of impacts. The growing outsourcing of IT services, and above all the use of cloud computing, can also lead to the danger of concentration risks at individual IT service providers.

- **Cyberattacks** Moreover, companies and institutions in the financial sector are a prime target for cyberattacks because they move and process money, financial instruments and sensitive data. As a general observation, cyber attackers are mainly organised and increasingly professional.

- **Regulatory impact** Regulatory regimes such as the Second Payment Services Directive (PSD2) directly impact the interaction between technology, companies and consumers – and thus also IT security. PSD2 provides regulatory support for developing an API ecosystem in payment transactions by requiring institutions to provide access to the payment accounts and a small amount of selected customer data they hold to third-party payment service providers supervised by BaFin – with the consent of their customers and observing strict security requirements. The resulting increasing interconnectedness of organisations, people and data (disaggregated value chains) could see forms of new risk emerging. For example, additional interfaces also provide potential attack opportunities for cybercriminals and increase the complexity of the overall system.

2. **Overarching goals**

In light of the developments described above in the “IT supervision and security” area of activity, BaFin – as the competent authority for IT and cyber security in the German financial services sector – is guided by the following two overarching goals with regard to the entities it supervises:

- **BaFin helps safeguard information security, meaning protecting information integrity, availability, authenticity and confidentiality.**

- **BaFin establishes state-of-the-art supervisory standards for IT management.**

---

**Information and IT security and cybersecurity**

- **Information security** Its goal is to comprehensively protect information. This information can be stored in IT systems, but also for example on paper.

- **IT security** This primarily concerns protecting and processing information stored electronically.³

- **Cybersecurity** This extends the area of activity of classic IT security to the whole cyberspace. It comprises any and all information technology connected to the internet and comparable networks and includes communication, applications, processes and processed information based on it.⁷
3. Status quo: What has BaFin already achieved?

Among other things, BaFin has already taken the following steps in the “IT supervision and security” area of activity, each of which serves at least one of the two overarching goals of this area of activity:

- **Holistic approach** I BaFin takes a holistic approach to IT and cyber risks for its supervisory activities, i.e. from IT strategy and IT governance through information risk and security management, down to IT operations and the outsourcing of IT services. Whereas the focus is on technical and organisational aspects in the case of classic IT risks, cyber risks extend the perspective to the whole cyberspace.

- **Central unit established** I BaFin has established the IT Supervision/Payment Transactions/Cyber Security (GIT) group to address these issues on a BaFin-wide basis. GIT pools competencies on fundamental IT supervision issues across BaFin’s sectors as part of an integrated approach and possesses its own audit powers in the field of IT security. In addition to the fields of IT and cyber security in the financial services sector, this unit is also responsible for the supervisory implications of PSD2 and the German implementing act (Payment Services Supervision Act – ZAG).

- **Ongoing monitoring of IT security ensured** I Based on the applicable legal norms and statutory requirements, IT Supervision ensures that the entities it supervises install, use and refine IT systems and processes that ensure the permanent integrity, availability, authenticity and confidentiality of the data. BaFin performs IT audits to do this – through its banking supervision units and, in the case of certain financial market infrastructures, together with the Deutsche Bundesbank. A comprehensive supervisory concept for IT supervision was developed and approved for insurance supervision.

- **BaFin has gained an overview of the situation at insurance undertakings and credit institutions** I BaFin conducted an industry-wide survey to learn more about how German insurance undertakings and pension funds address their IT and cyber risks. This surveyed the status quo of all core IT supervisory areas – from IT governance down to the ability to defend against a cyberattack. The goal was also to identify typical strengths and weaknesses at the companies and to gain insights for supervisory practices. At the same time, the survey also sent a strong signal to the insurance and the banking industry.

- **BaFin has gained an overview of concentration risks** I BaFin has gained an overview of potential concentration risks in the financial sector that could arise because of the growing outsourcing of IT services to individual service providers. As part of this, it surveyed the less significant German institutions, the financial market infrastructures, insurance undertakings and pension funds regarding information on the outsourcing of IT services. For the significant German institutions that are supervised directly by the European Central Bank, BaFin relied on the results of a corresponding survey conducted by the SSM.

- **Supervisory requirements established for IT security** I BaFin already published its Supervisory Requirements for IT in Financial Institutions (BAIT) in November 2017. The BAIT expand on the statutory requirements of section 25a (1) of the German Banking Act with regard to secure arrangements for IT systems and governance. BaFin developed the BAIT to establish supervisory requirements for IT security at banks that allow scope for entity-specific technical/organisational implementation, reflect the principle of proportionality and take a holistic approach to IT and cyber risks. In line with its integrated supervisory approach, BaFin additionally developed Supervisory Requirements for IT in the Insurance Sector (VAIT), whose content is harmonised with the BAIT, and issued them for consultation. The VAIT were published on 2 July 2018. In the BAIT and VAIT, BaFin also expands on the statutory requirements governing cloud computing, meaning the outsourcing of IT resources to an internet-based IT system that can be used dynamically. In doing so, BaFin also takes
into account the relevant standards issued by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI).

- **Helping shape European and global regulation** The momentum of the progressive digitalisation is reflected in a large number of European and global regulatory initiatives surrounding the topics of IT and cyber security. BaFin is participating in these projects in the various European and global bodies and is actively championing the consistent alignment of the various projects. As an integrated supervisory authority, BaFin is very well positioned to do this. From BaFin's perspective, it is important to ensure that no diverging requirements are imposed on market participants that would result in an objectively unjustifiable implementation effort.

- **Advocating appropriate consideration of German specificities** In the various European and global bodies, BaFin successfully advocates for appropriate consideration to be given to the special features of Germany as a financial centre in regulatory initiatives addressing IT and cyber security.

- **Exchange of information with BSI established** BaFin works closely with the BSI on the basis of an administrative agreement, combining the BSI’s technical know-how with BaFin’s supervisory expertise. A mutual exchange of incoming reporting information has been established. Additionally, BaFin has started integrating specific BSI requirements for critical infrastructures into the BAIT and VAIT.

- **Transparency through information events** BaFin has already organised a large number of conferences, workshops and other formats for exchanging information with industry representatives with the aim of informing companies at an early stage about the PSD2 requirements, for example.

4. **Next steps**

In the “IT supervision and security” area of activity, BaFin is planning the following steps, among others. Each of them serves at least one of the two overarching goals of this area of activity:

- **Ensure ongoing monitoring of IT security** Based on the relevant legal requirements, IT Supervision will continue to monitor that the entities it supervises install, use and refine IT systems and processes that ensure the continuous integrity, availability, authenticity and confidentiality of the data. It will continue to apply the holistic approach described under 3. Continuous implementation

- **Continue to develop supervisory practice** BaFin will continue to review whether it needs to adapt its supervisory requirements and practice. Continuous implementation

Some current examples are described in the following:

- **BAIT and VAIT** BaFin will continue to develop and expand the BAIT, for example by adding an optional module for operators of critical infrastructures. BaFin plans to successively expand BAIT into a set of central IT requirements for the institutions. The same applies to the VAIT. Implementation expected by end-2019

- **Asset management** For securities supervision, BaFin is examining which requirements need to be defined, for example for the area of asset management. Implementation expected by mid-2019

- **Cloud services** BaFin plans to publish separate guidance on the supervisory requirements applying to the use of cloud services. Implementation expected by October 2018

- **Continue to shape national, European and global regulation** BaFin will continue to play an active role in national, European and global regulatory initiatives surrounding the topics of IT and cyber security and leverage its strengths as an integrated supervisor. BaFin advocates harmonised,

---

8 See II 4 regarding changes in the “Supervision and regulation” area of activity.
appropriate, proportionate and consistent European and global regulation that adequately considers national specificities. **Continuous implementation**

- **Address and combat elevated IT risks with the help of BDAI** The Big Data and Artificial Intelligence phenomenon poses new challenges to managing IT risks, as described in BaFin’s BDAI report referred to above. First, the potential attack surface is growing larger, making control more difficult. Second, new forms of attack are emerging. Conversely, BDAI could also be used to defend against information security risks, for instance in risk analysis and detection. For example, BDAI could be used to identify irregularities in consumer behaviour in online banking and reveal possible abuse. These questions must be addressed. **Continuous implementation**

- **Multi-client service providers subject to supervision?** BaFin will examine whether multi-client service providers that provide more or less standardised IT services for a large number of institutions and companies should be subject to supervision by BaFin. So far, this has not normally been the case. However, these service providers play an essential role in the proper functioning and security of the IT used by the entities and institutions supervised by BaFin. IT security incidents at these service providers can also have significant effects on financial stability due to risk concentrations. **Implementation expected by end-2019**

- **Design and implement emergency simulations and crisis exercises** In Germany and internationally, BaFin is involved in the design and implementation of emergency simulations (generally more technical) and cyber crisis exercises (organisational/process-related). These aim to test and refine the ability of the actors involved to communicate and respond in the event of significant cyber incidents with material adverse effects on the financial system. From BaFin’s perspective, emergency simulations and crisis exercises are therefore key tools that can be used to strengthen the resilience of companies and institutions. **Implementation expected in 2018 and then ongoing**

- **Review introduction of framework for controlled hacking** BaFin is examining whether to introduce and update a framework for controlled cyber-hacking attacks based on threat intelligence (Threat Intelligence-based Ethical Red Teaming - TIBER). This is continuously aligned with international best practices and TIBER-EU, a framework for controlled and individually tuned cyber hacking attacks published by the ECB in March 2018. Controlled hacking attacks are designed to test the resilience of financial market actors. **Initial implementation expected by mid-2019**

- **Improve the cross-sector and international exchange of information** A high level of IT and cyber security can only be ensured in times of cross-sector and international interconnectedness if there is a structured flow of information, at both national and international level, between supervisory authorities and companies and between the companies themselves. BaFin is involved nationally and internationally in the design and implementation of corresponding concepts. **Continuous implementation**

- **Develop objectifiable criteria for API solutions used to access payment accounts** In the course of the further implementation of PSD2, BaFin is developing precise, objectifiable criteria for assessing the PSD2-compliant implementation of API solutions for accessing payment accounts, based on the European framework conditions. In particular, it is supporting the development of standardised API specifications to offer market participants legal certainty. **Implementation expected by mid-2019**

**IV. “Transformation of BaFin” area of activity**

**Basic question:** How will BaFin have to evolve further in light of progressive digitalisation - internally and at the interfaces to the market?
1. Baseline scenarios

BaFin operates in an increasingly digital environment. Among other things, digital transformation has implications for

- BaFin’s supervisory processes,
- its support processes,
- workplace resources and
- the selection and qualification of staff.

In all of these areas, BaFin must meet the requirements of the German e-Government Act.

2. Overarching goals

BaFin is leveraging the opportunities offered by digitalisation in the “Transformation of BaFin” area of activity

- to make its supervisory and support processes largely paperless and more efficient across its sectors;
- to develop appropriate new supervisory tools and solutions;
- to perform the functions assigned to it efficiently and with a high level of quality.

**Return on digitalisation**

The return on the growing digitalisation of supervisory and administrative work is to deploy resources in a targeted and efficient manner and to further improve the quality of supervision. Both of these have benefits for financial market stability.

3. Status quo: What has BaFin already achieved?

Among other things, BaFin has already taken the following steps in the “Transformation of BaFin” area of activity, each of which serves at least one of the three overarching goals of this area of activity:

- **Internal digitalisation** Since it was established in May 2002, BaFin has digitalised a significant proportion of the supervisory and support processes in all of its directorates. Among other things, it has created specialist applications for file and document management and data analysis. Additionally, BaFin has written an application for the electronic receipt of reports, for example. BaFin’s reporting and publishing platform (MVP) already offers more than 80 options for submitting reports (see Figure 1, page 16).
Figure 1: “Detail of the data flows between parties subject to reporting requirements, BaFin and other institutions and authorities”
In 2017, BaFin established an e-tendering platform and is now increasingly using it to manage tendering procedures. Using this platform, BaFin can electronically manage all Europe-wide procurement procedures well before the legally stipulated implementation date.

- **Modern work environment** Digitalisation also enables flexible working outside the office. BaFin therefore already offers its staff teleworking and home office work options under certain conditions, including the use of mobile devices. BaFin strives to further expand these options and to further improve the provision of mobile devices to its staff.

- **Staff recruitment and continuing professional development (CPD)** The progressive digitalisation outside and inside BaFin is changing working patterns and placing new demands on staff and managers. That’s why BaFin launched the “Fit for the Future” initiative in 2017. It represents BaFin’s plan to strengthen and – if necessary – to realign its human resources development tools so as to expand especially important qualifications such as IT skills. The following elements have already been implemented:
  - **Develop specific recruitment requirements** When recruiting new staff, BaFin’s sectors set continuously adaptable specific requirements for skills and qualifications that are especially critical in a progressively digitalised working environment. BaFin also continuously reviews the recruitment channels it can use to approach suitably qualified applicants.
  - **Promoting an exchange of information** BaFin has implemented a broad range of ways in which specialist information can be exchanged, including on issues relating to digitalisation. A large number of expert panels, working groups and regular meetings have been established internally, for example. BaFin staff also participate in expert meetings (exchanges of experience, conferences, congresses, etc.), including as speakers, in Germany and abroad. In turn, BaFin also offers various platforms for exchanging information at information events for representatives of supervised entities or other authorities. The project-based approach to work practised in many areas is also an important instrument for bringing together experts from different fields of work and for networking knowledge from different disciplines.

- **Targeted continuing professional development** BaFin continuously realigns its CPD offering for staff and managers with new qualification requirements resulting from the digitalisation of the market. This relates to hard skills such as IT security in banks as well as soft skills. For example, BaFin offers managers training on the topics of “Networked thinking”, “Thinking out of the box – Solving problems systematically and creatively”, “Leading at a distance” and “Leadership in digital transformation”.

- **Rewarding performance** The performance of staff members who make a particular contribution to making BaFin fit for the future thanks to the knowledge they have acquired in digitalisation issues can be recognised, for example, by positive assessments and performance bonuses.

4. **Next steps**

Despite the large number of subprocesses that have already been digitalised, BaFin is in the midst of transforming itself into an entirely digitalised supervisory authority. In the “Transformation of BaFin” area of activity, BaFin has therefore identified a number of additional projects that are expected to add considerable value for one or more of BaFin’s sectors and that each serve at least one of the three overarching goals of this area of activity.

---

10 See also III 4.3 for information on “Fit for the future”. 
4.1 Internal digitalisation

The internal digitalisation projects described in the following are selected lighthouse projects on which there is a particular focus in the digitalisation strategy. The Zeus project, the introduction of the e-file, plays a pivotal role.\footnote{See page 22.}

The IT sector and the relevant division have closely coordinated each of these lighthouse projects.

Projects have already been launched for a number of these plans. Some of them are already close to completion, while others are in the project initialisation phase. The other lighthouse projects will continue to run as plans until they have achieved corresponding technical maturity.

The lighthouse projects are expected to be implemented over the next three to five years. Some of these projects are interdependent, so all of the projects are regularly reassessed. If new projects emerge from the overriding goals, these are taken into account when the list is updated.

To allow the lighthouse projects described below to be prioritised in light of limited human and financial resources, BaFin has ranked them using the criteria of benefit and feasibility (see Tables 1 and 2, pages 18–19).

<table>
<thead>
<tr>
<th>Subcriterion</th>
<th>Description</th>
<th>Influence on overall ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reach</td>
<td>Describes how comprehensively the project can be used (only by a few scattered staff members or by all staff members across sectors).</td>
<td>30%</td>
</tr>
<tr>
<td>Efficiency and quality gains</td>
<td>Describes the extent to which the project contributes to a faster, simpler, less resource-intensive and better way of working.</td>
<td>20%</td>
</tr>
<tr>
<td>Standardisation</td>
<td>Describes the extent to which common international, national or internal standards can be used.</td>
<td>20%</td>
</tr>
<tr>
<td>Reusability</td>
<td>Describes the extent to which existing knowledge, processes and resources can be leveraged.</td>
<td>20%</td>
</tr>
<tr>
<td>Scalability</td>
<td>Describes the ability of the project or process to alter its size; in the current context, this refers to the ability to expand.</td>
<td>10%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subcriterion</th>
<th>Description</th>
<th>Influence on overall ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation effort required from competent divisions</td>
<td>Describes the use of resources, the time required, the coordination effort (with other divisions, IT, etc.) as well as the effort required from competent divisions for project work, testing and acceptance.</td>
<td>30%</td>
</tr>
<tr>
<td>Evaluation Criteria</td>
<td>Description</td>
<td>Weight</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>IT implementation effort</td>
<td>Describes the coordination effort, the time required and resource-related effort for project work, IT design, going live, tests, commissioning, maintenance and updating incurred by IT. The cost of hardware and external resources is also taken into account.</td>
<td>30%</td>
</tr>
<tr>
<td>Independence from external resources</td>
<td>Describes the extent to which there are interfaces or coordination effort with other institutions, companies or national/international authorities.</td>
<td>20%</td>
</tr>
<tr>
<td>Use of existing resources</td>
<td>Describes the extent to which existing systems, processes or experience can be leveraged.</td>
<td>20%</td>
</tr>
</tbody>
</table>

The following evaluation matrix shows how BaFin has prioritised the lighthouse projects on which there is a particular focus by the two criteria of “feasibility” and “benefit”. The projects are explained in sections 4.1.1 and 4.1.2. The assessment of benefit in particular reflects the relevance for supervisory and administrative activities.
As mentioned above, the portfolio presented here and described in greater detail in the following is not static. It is regularly reviewed and adapted or extended if necessary.

4.1.1 Digitalisation of supervisory and support processes

BaFin plans to refine and network existing electronic procedures and integrate them into a service-driven, portal-based target architecture. It also wants to digitalise additional suitable supervisory and support processes in the coming years. BaFin’s intention is to enable work to be carried out as seamlessly as possible – from the receipt of a message or information to the completion of the supervisory procedure. The focus is not only on information security and standardisation, but also on enhancing efficiency.

By successively networking data and information, including from different sectors, BaFin plans to create new options for evaluations and analyses. This will allow the benefits of integrated supervision to be leveraged more effectively and the quality of supervision to be further improved.

Projects to improve information gathering and interfaces
Growing volumes of data are already being transmitted today between supervisory authorities, supervised entities and parties subject to reporting requirements. BaFin will improve data quality and reduce the transmission effort by establishing electronic interfaces and automating data transmission.

- **Demeter - Notification procedure I** This procedure is designed to enable electronic support for processing all notifications under the European passport. It digitalises a process that has a high frequency in European and international cooperation and is of significance across sectors at BaFin.

- **Hephaistos - Banking supervision reports to BaFin I** This implements the EU reporting requirements under PSD2. In the first step, BaFin created a new reporting procedure for receiving reports on incidents under Article 96 of PSD2.
- **Persephone - Automated account information access procedure** | BaFin’s Prevention of money laundering directorate electronically accesses certain account data from credit institutions. Agencies that send inquiries to BaFin (e.g. police authorities) will also be technically integrated so that the inquiries no longer have to be processed manually at BaFin, in contrast to the current situation. Preventing money laundering is one of BaFin’s core functions.

- **Nike - Recovery plans** | A new notification procedure will be created for digitally filing recovery plans and – if possible – a technical procedure to evaluate them automatically. This procedure is an important support mechanism for banking supervision.

- **Charon - Resolution plans** | This project will involve enhancing the existing reporting procedure on the MVP in the direction of an XBRL-based reporting procedure, and the transfer and evaluation of the resolution data in a data warehouse. This is the central reporting procedure in the Resolution sector.

**Projects to improve information analysis**

Examining and evaluating information in accordance with the relevant legal norms and standards lies at the heart of supervisory activities. A challenge for the future will be to recognise patterns on the basis of existing information and to ask further questions. Methods such as data mining can support this in some of the projects mentioned here.

- **Hera - Narrative reports in insurance supervision** | This enables the preliminary evaluation of all narrative reports (e.g. audit reports) supported by suitable text mining tools. This project is designed to establish a basis evaluating further narrative documents using text mining tools. All sectors will be able to benefit from these functions in the long term.

- **Gaia - Appointments of individuals** | Appointments of individuals at the entities (such as members of the management and supervisory boards) supervised by all of BaFin’s sectors will be notified and reviewed electronically. This is a process implemented BaFin-wide that is a fundamental element of its supervisory work and comprises a large number of notifications every year (approximately 10,000).

- **Nemesis - Data analysis in market supervision** | This project aims to deliver electronic support for analysing securities sales reports, for example, to make it easier to detect market manipulation and insider trading. This is a core function of securities supervision.

- **Apollon - Crisis early warning system** | System-driven monitoring and reporting when threshold values for crisis early warning indicators are reached. From a technical perspective, the crisis early warning system will be implemented in such a way that the indicators can largely be evaluated automatically. This is designed to enable banking supervision in particular to identify and assess emerging crises at an earlier stage.

- **Artemis - SREP/RAS** | Implementation of the Supervisory Review and Evaluation Process (SREP), including the Risk Assessment System (RAS) that forms part of the SREP. The goal of Artemis is to create a uniform toolkit for assessing the risks of the individual institutions. A uniform Europe-wide assessment methodology is a requirement imposed by the ECB. The resulting database will enable valuable insights to be gained in the Banking Supervision and Resolution sectors.

**Projects to improve support for supervisory activities**

Financial supervision tasks range from routine procedures with a high number of cases down to complex individual measures in which large amounts of data and documents have to be processed. In both cases, digitalisation can help to keep the focus on the essentials.

- **Zeus - E-file/document management system** | The new e-file is designed to completely replace the combination of DOM EA (BaFin’s existing document management system) and paper files currently in
use. This will do more than merely optimise file management. Above all, the e-file will serve as a cornerstone for digitalising processes in other projects. This includes issues relating to e-government (see below), as well as many of the digitalisation projects presented in this strategy that are relevant to files and document-based. The e-file serves as a common tool and is linked directly to specialist processes in many cases. Special consideration is given to the requirement for written form. However, the e-file will make paper-based documents usable electronically independently of this. As a core tool, the e-file supports almost all supervisory and administrative processes and hence plays a key role in digitalisation projects, as mentioned above.

- **Kronos - Qualifying holdings I** The process steps of the qualifying holding procedure will be optimised by means of electronic support – for example by introducing electronic workflows. The qualifying holding procedure is a comprehensive procedure that is conducted in the Banking, Insurance and Securities Supervision sectors. It is based in part on the appointment of individuals (see Gaia).

- **Aither - Notifications of intention to commence marketing I** BaFin will use this project to ensure the electronic editing, enhancement and further processing of reported notifications of the intention to commence marketing. In particular in the field of European cooperation, preparing and processing notifications of the intention to commence marketing are important tasks that can be made even more efficient by means of automation.

- **Ares - Authorisation procedure/extension for financial services institutions (project) I** This project aims to ensure the seamless modelling of authorisation processes from the application to the granting of authorisations. This is one of the core functions of securities, insurance and banking supervision.

- **Dike - Completing standardised certificates and model forms with data available in IDIS (Investment Database and Information System) I** This project relates to the automated generation of various reports and certificates (land register certificates, tax certificates, European passporting sub-projects under the UCITS Directive, etc.). This will help cut manual activities and thus enable securities supervision to work more efficiently.

- **Hermes - Written procedures I** Briefings on written procedures of the SSM Supervisory Board will be distributed electronically to those responsible within BaFin's internal specialist teams. BaFin is examining the extent to which the requirements of the divisions will be covered by the new document management system (Zeus project). Synergy effects with the Zeus project are possible. This process constitutes a core responsibility of the Banking Supervision sector in the SSM.

- **Momos - Audit planning/action tracking I** A standard application will be used to support the planning, implementation and follow-up of regulatory audits. Audit planning, on-site inspections and audit follow-up measures/tracking findings and measures (including the evaluation of documents) will be digitally modelled and linked. Audit planning, execution and follow-up are core supervisory functions.

### 4.1.2 Evolution of supporting infrastructures

**Projects to improve the systems environment and the implementation of IT requirements of specialist functions**

As the operator of the various IT systems, BaFin IT performs an interface role within the authority. This applies all the more when more processes are digitalised. To be able to still function effectively, IT relies on standardisation wherever different requirements of specialist functions can be implemented using similar processes and systems.

---

12 See II.4.
- **Hestia - Development of a configuration management database (CMDB) and an integrated process platform** | The first part of this project models the entire IT infrastructure in a configuration management database (CMDB), while the second part involves the standardisation of the configuration management process over BaFin's locations. The CMDB is the basis for modelling the IT infrastructure.

- **Uranos - Introduction of identity management** | Identity management (IdM) is designed to simplify and automate user and authorisation processes, primarily in the IT directorate. As a key data hub, the IdM can also securely communicate personal and organisational data to other systems. This avoids redundant data capture, which is of vital importance for administration.

- **Themis - Implementing standard processes under the ITIL standard in the IT directorate** | This project aims to optimise IT service management processes under ITIL V3 (Information Technology Infrastructure Library, Version 3). The IT processes will be coordinated, made more transparent and standardised. Defined, documented descriptions will be created and used to implement IT processes. Aligning the way the IT directorate works with the ITIL processes is one of the key standardisation measures for delivering efficient IT operations.

- **Styx - Introducing a business process modelling notation suite** | A BPMN suite for developing information systems for process support will be evaluated and introduced. BPMN suites offer very good facilities for the efficient, standardised implementation of operations management workflows. In addition, modelling specialist processes using BPMN supports a common understanding by the specialist functions and IT when evaluating specialist requirements.

- **Dionysos - Target architecture for BaFin specialist applications** | BaFin plans to establish a portal-based, service-driven target architecture for the specialised procedures developed by BaFin itself. This will allow shared-use functions to be reused and enable the even more efficient delivery of IT solutions.

### 4.2 Workplace resources

- **Modern work environment** | BaFin remains committed to offering its staff teleworking and home office work options under certain conditions. It intends building on its existing approach and creating an appropriate organisational framework that takes account of the specific requirements of the modern work environment – including in light of protecting its employees and ensuring IT security. *Implementation expected by mid-2019*

- **Modern work infrastructure** | As far as possible and to the extent necessary, BaFin will continue to exploit the possibilities offered by technology to create modern work infrastructures for its staff that can be used while they are travelling – meaning on business trips, at the European Central Bank as part of the SSM and at the Single Resolution Board as part of the SRM – but at the same time ensure the necessary working capacity and quality. *Continuous implementation*

- **Encouraging cooperation** | BaFin is also increasingly using collaboration systems to improve cooperation across directorates and automate communication within BaFin as a whole. *Continuous implementation*

### 4.3 Staff recruitment and continuing professional development

- **Recruitment** | As part of its “Fit for the future” concept, BaFin will scrutinise its requirements profiles and recruitment processes in light of the progressive digitalisation and refine them if necessary. *Implementation expected by end-2019*
Continuing professional development I Also under the heading of “Fit for the Future”, this project will further strengthen the skills and capabilities of staff members and managers who are particularly important in light of digitalisation and will constitute the supervisors of the future. Implementation expected by end-2019

“Fit for the Future” is designed to strengthen the skills of staff members in the following areas:

- **IT competence for supervisory activities I** Staff members are expected to further deepen their understanding of the importance of digitalisation. They will also gain a basic understanding of the technical IT workflows and infrastructures at the companies. Additionally, they will develop their understanding of new risks from the use of current technologies (e.g. cybercrime).
- **Analytical competence I** The scale and complexity of data will continue to increase, among other things because of the progressive digitalisation/automation. As well as other skills, staff members will develop a basic understanding of the data to be analysed and its significance for supervisory activities.
- **Planning and performing audits I** Digital transformation is changing the qualitative and, where applicable, the quantitative requirements for audit procedures. Staff members are therefore expected to develop their skills in areas where audits are already routinely performed and in areas where no audits have yet been performed.
- **Financial mathematics and product expertise I** Knowledge of financial mathematics is becoming increasingly important in certain supervisory areas - for example when the use of models and algorithms is involved. This knowledge will therefore be deepened and broadened. The same applies to the use of innovative financial products.
- **Developing leadership skills I** Managers will be empowered to support change processes associated with digitalisation and to promote the personal development of staff. The programme also includes leadership in the digitalised working world and modern work organisation. In addition, networked thinking and overarching specialist knowledge will be further developed.
- **Leveraging internal knowledge I** BaFin already possesses comprehensive expertise in the above-mentioned areas. This specialist knowledge will be made available to the entire organisation. The Programme for Strengthening Integrated Supervision (PSIA), which consists of training events by staff members, for staff members, will therefore be promoted.
- **Learning at the workplace I** The bulk of the expertise at BaFin is acquired informally, i.e. at the workplace and not in further education or continuing professional development measures. For this reason, BaFin plans in particular to further encourage cooperation within and between the divisions and the exchange of specialist information within BaFin.

V. Implementation and refinement of the digitalisation strategy

Responsibility for implementing the digitalisation strategy and its refinement and updating is allocated as follows in the individual areas of activity:

- **“Supervision and regulation” area of activity:** The SR 3 (Innovations in Financial Technology) division is responsible.

- **“IT supervision and security” area of activity:** The GiT Group (IT Supervision/Payment Transactions/Cyber Security) is responsible.
“Transformation of BaFin” area of activity: Going forward, a Chief Digital Officer (CDO), who will also coordinate the refinement of the overall strategy, will be responsible. The functions of the CDO and his or her office are described in a separate concept document.