www.pwclegal.de

Germany's BaFin updates its supervisory expectations on ICT use by financial services firms

pwc

Table of content

Quick Take

The breadth of information and communications technology (ICT) services on offer to financial services firms continues to develop rapidly. In many ways COVID-19 has acted as a catalyst prompting fundamental change as firms move to embed hybrid and location-independent working arrangements and transition to more digitalised operating models, including when dealing with clients and customers.

Financial markets regulatory policymakers and supervisory authorities have begun to assess how to best supervise how financial services firms use ICT and how they engage with ICT service providers, in monitoring concentration and over-reliance risks. This is challenging and as a result, EU and national-level financial services regulatory and supervisory authorities have published various rulemaking instruments along with supervisory guidance. In Germany, the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin) has introduced several supervisory measures in terms of specific rulemaking instruments focusing on ICT.[1]

According to BaFin, the "core component" of these measures in ICT supervision are set out in their “circular” (Rundschreiben) on “Supervisory Requirements for IT in Banks and Financial Services Institutions in Germany” (Bankaufsichtliche Anforderungen an die IT in Kreditinstitute und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland - BAIT). BAIT clarifies BaFin’s supervisory expectations for in-scope firms and their compliance with the requirements on secure ICT systems and associated ICT processes (as regard the integrity, availability, authenticity and confidentiality of data) as well as on ICT governance.

BAIT was first published in November 2017 and has been updated successively since then. The most recent amendments were published in a draft form during October 2020[2], which ultimately entered into force in its final form in August 2021.[3] These August 2021 amendments also serve to implement those ICT-specific supervisory outcomes as set at the EU-level, notably by the European Banking Authority (EBA) in its own “Guidelines on ICT and Security Risk Management”, which entered into force on 30 June 2020.

The EBA's ICT Guidelines set out standardised requirements concerning the management of internal and external ICT security and risks for credit institutions i.e., banks, investment firms and payment service providers. The EBA guidelines are binding on the supervisory authorities in the individual EU Member States and thus, in Germany, on the BaFin. Most of the measures in the EBA’s ICT Guidelines are ultimately directed at market participants who are subject to a "comply or explain" approach. An amendment to BAIT was therefore necessary to ensure these reflect the outcomes set in the EBA’s ICT Guidelines notably on operational ICT security measures as well as ICT-specific contingency management procedures.

---

[1] The BaFin has also established a separate organisational unit for IT supervision in the financial services sector within the BaFin (Group IT Supervision / Payment Transactions / Cyber Security). This unit is directly attached to the BaFin’s Banking Supervision Division.

[2] Compared to the draft circular of October 2020, language adjustments have been made on the one hand. For example, the term "IT security" has been consistently replaced by the more comprehensive term "information security". In other places, deletions have been made to clarify that protective measures are to be applied comprehensively. In Chapter 6 on identity access management, for example, the addition that access must be assignable "even for non-personalised activities" has been deleted. The following is now shorter, but more unambiguous: “Accesses and accounts must at all times be unequivocally assignable to an acting or responsible person (preferably in an automated manner)”.

[3] The original German text of BAIT is binding. However, the BaFin has also provided an English version of BAIT for information purposes on its website. Non-binding English version available here. Binding German version available here. See also BaFin’s article available here (from October 2021) as to the context for amendments.

While there were no fundamental changes to concepts contained in BAIT, some parts were expanded and adapted. Three new chapters were added to the existing nine setting out requirements. Moreover, the scope and tone of what is covered has also shifted and broadened both in granularity and prescriptiveness. Specifically, BAIT's focus has moved from "IT security" which the BaFin concluded was limited to ICT security specific risks, to "information security" which aims to, as the BaFin has stated "aims to protect relevant information regardless of the form it takes. The area of information security therefore encompasses everything related to information processing. In the context of information security and information risk management (ISM/IRM), it is now spelled out more clearly that the business processes concerned must take effect across the entire organisation, and that it is not enough to provide adequate resources to IT operations and application development alone. The BAIT requirements now clarify, for example, that the institutions must develop a comprehensive training and awareness programme for their staff on the topic of information security."

The requirements set out in the 2021 version of BAIT will also likely need to be updated in the future to accommodate further reforms introduced by the EU's cross-sectoral Regulation for a digital operational resilience act (DORA), which is (at the time of writing) largely expected (at the earliest) to become operational reality from 2024 onwards. This idea is supported by the fact that DORA aims for further full harmonisation – including across all regulated sectors in financial services. DORA driven reforms will however likely cause more fundamental changes to BAIT. Thus, for the immediate future financial services firms will have to meet the expectations in BAIT and MaRisk (more on that below) along with preparing for DORA's debut.[4]

This Background Briefing assesses the changes introduced in the August 2021 updates to BAIT and highlights changes to previous versions as well as some key considerations firms will want to take note of.

[4] However, these changes not only impact regulated financial services firms, but may also require changes to the design and processes of ICT service providers, including software-as-a-service (SaaS) providers, cloud computing service providers, and/or other external service providers (including those that are not ICT service providers) on which these regulated financial services firms rely. It is therefore advisable for in-scope financial services firms to engage in early dialogue with their ICT service providers to advance any amendments or to confirm the resilience and compliance of existing arrangements as early as possible. Amendments to contractual as well as regulated outsourcing agreements, ranging from agreed service levels and/or key performance indicators (KPIs), may be required, and financial services firms may have to rethink or otherwise top-up previous outsourcing compliance assessments.

Scope of BAIT

ICT processes have become an integral part of financial service providers' operations, and reliance on third-party service providers is unavoidable. It is precisely this dependence on third-party ICT service providers and processes that makes it challenging to cope with the dynamic regulations. BAIT was intended to be one of the means to facilitate that and as such was first published by BaFin in November 2017.

BAIT further details statutory requirements of the German Banking Act (Gesetz über das Kreditwesen (Kreditwesengesetz– KWG)) on the proper business organisation (ordnungsgemäße Geschäftsorganisation) of institutions and the outsourcing of activities and processes from an IT point of view.[5] Additionally, BAIT builds on the BaFin's Circular on Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – MaRisk), which itself further details (amongst others) IT requirements of the KWG. As such, BAIT and MaRisk ought to be read together.

To illustrate, both MaRisk and BAIT refer to the same group of intended recipients: in-scope firms. These include (inter alia) credit and financial institutions within the meaning of the KWG[6] as well as German branches of third country firms providing banking business or financial services in Germany (third country branches).[7] The scope further extends to branches of German credit or financial institutions carrying out business internationally. Explicitly excluded from MaRisk's and BAIT's application are German branches of EEA firms which make use of the European "passport" for providing banking business or financial services in Germany.[8]

Firms must take into account that BAIT and MaRisk do not constitute and exhaustive list of the supervisory expectations for compliance with the requirements for IT in financial institutions. In this regard, BAIT explicitly states that "…the depth and scope of the topics addressed in this Circular is not exhaustive" and that "…institution(s) shall continue to be required to apply generally established standards to the arrangement of the IT systems and the related IT processes in particular over and above the specifications in this Circular".[9] Further, in addition to BAIT and MaRisk, further ICT-specific rules and compliance outcomes are set forth in various other pieces of financial regulation (e.g., the Markets in Financial Instruments Directive II (MiFID II) and the Payment Services Directive II (PSD II) as well as local and EU implementing law).

BAIT has been updated a total of two times since its original publication in 2017. The September 2018 BAIT update added the "critical infrastructure" (KRITIS) module to the requirements. This included measures to achieve the KRITIS protection goals for the financial sector, which, when fully implemented, serve as proof of implementation of the German IT Security Act (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – IT SiG)[10].

The 2021 update to BAIT implements a number of changes set at the EU-level in particular concerning EBA's ICT Guidelines. Targeted changes were also made that place a new focus in BAIT on operational information security and contingency management. These changes are also accompanied drafting changes to broaden the focus concerning customer relationships with those payment service providers that are supervised under Germany's transposition of the EU's Payment Services Directive 2 (PSD2) i.e., into its Payment Services Supervision Act (Gesetz über die Beaufsichtigung von Zahlungsdiensten - ZAG) and emergency management.

Accordingly, a holistic view is emerging with which BaFin will in future also concentrate on assessing relevant risks outside the institution's own ICT arrangements. Banks must therefore not only structure and secure their own ICT operations as well as upstream and downstream processes, but also adapt their interaction with external service providers and sub-service providers to the BAIT rules.

[5] See sec. 25a para. 1 sent. 3 no. 4 and 5 and sec. 25b KWG.
[6] See sec. 1b KWG.
[7] See sec. 53 para. 1 KWG.
[8] See MaRisk, module AT 2.1.
[9] See BAIT, I. Preliminary remarks point 3; as regards these standards, BAIT explicitly mentions the IT Baseline Protection Manuals (Grundschutz) issued by the Federal Office for Information Security (BSI).
[10] Available here.

BAIT's key principles – an overview

Although BAIT is not, from a strict hierarchy of norms perspective, legally binding, it does specify BaFin's supervisory expectations on financial institutions i.e., in-scope firms on their compliance with ICT risk management. As such, BAIT has a significant impact on the market: Firms that are in-scope will want to implement the requirements of BAIT in order to avoid the risk of attracting supervisory scrutiny if they do not comply with the requirements. BaFin itself even emphasises in its letter to the associations (Anschreiben an die Verbände)[11], that it considers BAIT to be just as relevant as firms' compliance with prudential regulatory rules on capital and liquidity requirements, which is a high bar. Key principles of BAIT are the following:

- setting a top-down approach, whereby responsibilities for compliance increase through levels of seniority of management;[12]
- adopting a holistic compliance requirement, meaning BaFin will assess the overall compliance with BAIT and related supervisory expectations in its entirety;
- requiring a tailored compliance approach that is reflective of individual needs and risk drivers, requiring that relevant arrangements evidence much more granularity in the environment they operate in and the risks they aim to identify, mitigate and manage;[13] and
- applying a more periodic (and prescriptive) review process, prompting firms to undertake much more in the way of periodic as well as ad-hoc reviews of the efficacy of the suitability of the design and the running of relevant arrangements by using KPIs and diagnostics where possible[14] as well as look at their overall operating environment and thus ICT risk management by firms they deal with or rely upon.

The following paragraphs present a summary of BAIT's key principles as embedded in the existing core chapters before turning to an assessment of the impact of the August 2021 amendments.

IT strategy[15]

The management board (i.e., the executive and governance function in most German companies) of a financial services firm is required to establish an ICT strategy that is consistent with that firm's business strategy and contains (at least) the minimum requirements specified in II. 1.2 of BAIT. These requirements include, inter alia, the strategic development of the firm's organisational and operational structure of ICT and concerning the outsourcing of ICT services, the responsibilities and integration of information security into the organisation and the strategic development of the firm's ICT architecture.

IT governance[16]

In scope-firms must put in place a structure to manage and monitor the operation and further development of ICT systems including associated ICT processes on the basis of the ICT strategy (i.e., ICT governance). In doing so the firm must ensure for example, that suitable staff are available, in particular for information risk management, information security management, ICT operations and application development and that conflicts of interest and incompatible activities are avoided within the ICT structure.

[11] See BaFin's letter to the associations from 6 November 2017.
[12] See e.g. II.4.2. of BAIT.
[13] See I.4. of BAIT.
[14] See e.g. II.3.11., II.4.8., II.5.6., II.10.4. of BAIT.
[15] See II.1. of BAIT.
[16] See II.2. of BAIT.

Information risk management[17]

In view of the complexity of cyber threats, BAIT explicitly emphasises the importance of firms keeping themselves informed about current external and internal threats and vulnerabilities as well as informing management about the results of the risk analysis and changes in the risk matrix they are exposed to. The fact that threats and vulnerabilities are also to be taken into account by information risk management, insofar as they may pose risks to the organisation, is now, as a result of the recent updates, made clear in BAIT's chapter on "Information Risk Management".

As such, firms must set up a catalogue or inventory of target measures within the scope of information risk management. Such register should specify and suitably document the firm's requirements for implementing the protection objectives ("integrity", "availability", "confidentiality" and "authenticity") in the various categories of protection requirements.

BAIT also specifies the requirements on the risk analysis and the reporting to the management board on ICT risks more generally.

Information security management[18]

It is the responsibility of the firm's management board to agree on an information security policy and to communicate this within the firm. The information security policy then forms the basis for further measures, in particular the specific information security policies and processes in the firm. Each firm must also have an independent "information security officer" who is responsible for all information security issues within the firm and vis-à-vis third parties. Such officer must also provide an overview of the status of information security to the management body at least once a quarter and on an ad hoc basis. Under certain conditions regionally active firms and small firms can appoint a joint information security officer.[19]

User access management[20]

Pursuant to BAIT's requirements, user access management should be based on a user access rights concept. For firms, this means that they must establish a corresponding technical and organisational concept to ensure that the requirements specified in the user access rights concept cannot be circumvented. The processing of access rights (setting up, changing etc. of access rights) must be documented "in a way that facilitates comprehension and analysis".

Physical security requirements, as described in the EBA's ICT Guidelines, are addressed in several chapters of BAIT. For example, companies must draw up a physical security policy, carry out access controls and establish appropriate perimeter protection in line with the state of the art. Perimeter protection is the protection of the area between the building and the property boundary.

[17] See II.3. of BAIT.
[18] See II.4. of BAIT.
[19] See BAIT, Interpretative Guide, p. 10.
[20] See II.6. of BAIT.

ICT projects and application development[21]

Firms must establish an organisational framework for ICT projects and their management (including the ICT project portfolio in its entirety) appropriately. Major projects and related risks are subject to reporting to the management body (regularly and on an ad hoc basis).

The processes that develop the applications in the firms must be appropriately defined and adequate. Precaution should be taken to ensure that, once the application is up and running, the confidentiality, integrity, availability and authenticity of the data to be processed are comprehensively guaranteed. Applications must be tested according to a defined testing methodology.

ICT operations[22]

Another part of BAIT concerns specific requirements for ICT operations. The portfolio of ICT systems must be managed appropriately by the in-scope firm. Depending on the type, nature, complexity and risk, procedures must be established for the modification of ICT systems. Further, BAIT specifies the processing of change requests for ICT systems and the setting up of a data backup strategy.

Outsourcing and other external procurement of IT services[23]

Under BAIT, risk assessments must be carried out prior to each instance of "other external procurement of IT services". According to the BaFin's MaRisk Interpretative Guide (Auslegungshilfe) "…other external procurement of ICT services" does not qualify as "outsourcing" within the meaning of the MaRisk. Rather, the term "external procurement" covers e.g., the one-off or occasional external procurement of goods and services, the procurement of services which is typically arranged by the firm (typischerweise bezogen) and which cannot be provided by the firm itself (neither at the time of external procurement nor in future) due to factual circumstances or legal requirements.[24] In addition, the risk assessments of firms are subject to the requirement of review and amendment (on a regular and ad hoc-basis) by the firms. In the case of contractual arrangements with external ICT service providers firms must further take "appropriate account of the measures derived from the risk assessment relating to other external procurement of IT services".

Firms must always adapt and continuously review their ICT regulations and processes. Apart from the technical side, BAIT also has an impact on the general organisational structure and governance regulations. Here, too, firms must make adjustments in line with BAIT. Focus should certainly be placed on the establishment of the ICT security officer function and relevant policies and procedures.

Various requirements in BAIT, such as the need for quarterly reporting to the firm's management board, make it clear that the function of the ICT security officer is particularly important in both the collection and reporting of information across a financial services firm but also to the management body. Furthermore, BAIT emphasises a clear necessity that the management board displays the required ICT competency and assumes the ultimate responsibility for financial institutions' compliance with the supervisory requirements on ICT.

[21] See II.7. of BAIT.
[22] See II.8. of BAIT.
[23] See II.9. of BAIT.
[24] See MaRisk Interpretative Guide, p. 46.

ICT service continuity management[25]

Firms are required to maintain a well-defined business continuity plan with a contingency concept that covers both the restoration of full function and the continuation of business during “emergencies”. Consequently, dependencies in the ICT system(s) and with regard to external service providers must be suitably documented and have sufficient available resources to ensure the limited continuation of time-critical business processes. An annual review of the effectiveness of the plans must also be accounted for.

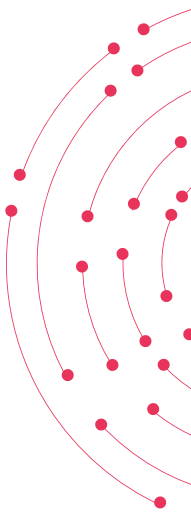
Managing relationships with payment service users[26]

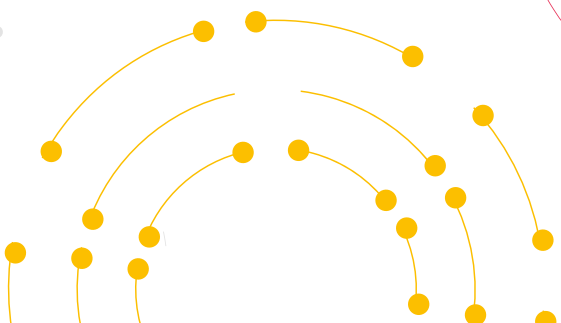
Firms are required to inform payment service users about security risks and provide them with options for adjustment, such as disabling certain functions (e.g., foreign transfers outside the SEPA area) or adjusting limits for transfers. To quickly detect non-authorised access, notifications must be offered for transactions that have been made and failed. In addition, firms must support and advise payment service users on these risks by establishing appropriate communication channels.

Critical infrastructure[27]

This chapter is not aimed at all financial institutions, but at those that are classified as critical infrastructures under the KRITIS module of BAIT. These firms are free to follow international standards in implementing appropriate security standards or to have their own or industry-specific approach certified. Therefore, the specifications included here are not mandatory, but serve at providing an alternative way to provide evidence of protection.

Essentially, the requirements defined here are about observing the KRITIS “protection goal” in information risk and information security management, as well as contingency measures. The protection goal is to ensure that payment transactions and the supply of cash are maintained throughout, which must also be guaranteed in the event of an emergency.





[25] See II.10. of BAIT.
[26] See II.11. of BAIT.
[27] See II.12. of BAIT.

Summary of the August 2021 amendments to BAIT

Although there are no fundamental changes as to BAIT's core concepts and supervisory expectations the requirements have been expanded and adapted in some places. In the new chapter "Operational Information Security", for example, the BaFin has set requirements concerning the design of effectiveness controls for information security measures already implemented in the form of tests and exercises. Such effectiveness controls include use of gap analyses, vulnerability scans, penetration tests and simulations of attacks (including "red teaming" – see standalone coverage from our RegCORE on the ECB's own rules and expectations on this) are an essential part of any effective and sustainable information security management system. Institutions must monitor the security of IT systems regularly and on an ad hoc basis. In doing so, they must avoid conflicts of interest. For example, anyone who was involved in the design and implementation of security measures must not audit them afterwards. Institutions must analyse the results of such effectiveness checks, identify any need for improvement, and manage risks appropriately.

In-scope firms are expected to evidence their compliance in the form of an "Internal Guideline", which the BaFin has included as a concept in BAIT's "Information Security Management" chapter. The chapter also includes requirements for logging and monitoring, i.e., the logging of events and monitoring in real time, and for the detection and analysis of security-relevant events. For example, potentially security-relevant information must be evaluated in an appropriately timely, rule-based and centralised manner and must be available for a reasonable amount of time for subsequent evaluation. Consequently, firms should consider implementing a portfolio of rules for identifying security-relevant events. Moreover, the expanded requirements set in the AT 7.3 "Contingency management" rules in MaRisk forms the basis for the new BAIT chapter "IT Service Continuity Management". For time-critical processes and activities, it provides for the establishment of restart, contingency operation and recovery plans and thus firms should consider greater granularity in setting both recovery point objectives (RPOs) and recovery time objectives (RTOs). According to BAIT, in-scope firms must equally, on at least an annual basis, test whether these types of IT contingency plans are effective.

The third new chapter of BAIT that has been introduced as part of the August 2021 amendments is called "Managing Relationships with Payment Service Users." It stems from the new BaFin's rulemaking instrument, i.e., a circular (Rundschreiben) titled "Payment Services Supervisory Requirements for the IT of Payment and Electronic Money Institutions" (Zahlungsdienstliche Anforderungen an die IT – ZAIT).[28]

[28] Available here.

BAIT's three new chapters in more detail

Information security management[29]

This new chapter aims to ensure that in-scope firms maintain a strong, resilient ICT-specific risk identification and control framework. For this, definitions of ICT risk drivers, ICT risk readiness and tolerance levels, escalation and fallback measures, and remediation plans must be put in place. The focus of these efforts apply not only to firm-internal but equally to group specific ICT solutions as well as to those provided by outsourced services and third-party service providers more generally, including externally hosted ICT systems as well as data hosting, management and storage solutions.

Firms must provide evidence that advanced systems are used for security information and event management (SIEM) and that a security operations centre (SOC) is permanently staffed. The SOC goes beyond the activities of the ICT security officer. As a result, firms are expected to automate the identification of ICT security related events (notably unauthorised access) and to undertake prompt review and analysis of not only the threats but the exploited weaknesses in systems and controls and take remedial action.

Thus, firms must also shift their focus to ensuring that their ICT systems and processes along with other parts of the information network have high integrity, availability and confidentiality measures with respect to data. Known vulnerabilities must be circumvented or data appropriately encrypted. Appropriate security measures must be put in place to check integrity and resilience on a regular and ad hoc basis, and special measures must be maintained to identify and assess threats as quickly as possible.

IT service continuity management[30]

This new thematic chapter focuses on ICT contingency management procedures and processes, in particular the resilience of outsourced ICT resources and time-critical processes. Firms will have to ensure they can evidence their own resilience with contingency management procedures and the use of back-up sites, but equally implement measures that are coordinated with their outsourced as well as third-party service providers. A particular focus is set out in BAIT on firms' design and implementation of recovery time objective and permitted downtime, as well as recovery plans, along with the related dependencies of internal and external services (including service providers).

Firms will be required to design and maintain an IT-resilience testing strategy and plan and conduct at least annual reviews and testing of measures based on individual threat-based risk scenarios, as well as simulations relating to the disruption of activity at data centres. Firms are expected to evidence that in the event of a failure/disruption of a data centre on which that firm relies, the relevant processes can be serviced for a specific period of time by using an alternative data centre.

[29] See II.4. of BAIT.
[30] See II.10. of BAIT.

Managing relationships with payment service users[31]

This new thematic chapter to BAIT was added to complement PSD 2/ZAG requirements applicable when financial services firms are providing payment services and communicate with payment services users. The new requirements aim to drive increased user awareness concerning the security risks linked to payment services.

The 2021 August amendments in the wider context including for EU-level and German rules

By its own definition, BAIT is not exhaustive in terms of content. This means that financial institutions are still obliged to adapt their security measures to the latest technology and common standards, even if they meet all the requirements it contains.[32] These include, for example, the ISO 27001[33] standard and the BSI IT baseline protection.[34]

Firms may wish to also forward plan how to comply with these immediate changes introduced by BAIT and the relevant supervisory priorities of BaFin for 2022, as well as the range of EU-level changes that have been published to date and which are likely to begin to take effect from 2022 through to 2024 including those beyond DORA.

BAIT is not the only regulation that imposes cybersecurity requirements on financial service providers. Several comparable circulars now exist, each dealing with their own lines of business in the financial sector, and their similar names can easily cause confusion. A brief overview:

- VAIT or insurance supervisory requirements for ICT[35]: is directed to are all insurance firms that carry out activity according to § 1 para. 1 VAG, with the exception of special purpose insurance companies (§ 168) and the security fund (§ 223);
- KAIT or asset management supervisory requirements for IT[36]: which is addressed to management companies of funds (AIFs and UCITS) according to § 17 KAGB; and
- ZAIT or Payment Services Supervisory Requirements for IT: Applies to payment institutions and electronic money institutions pursuant to Section 1 (3) ZAG.

[31] See II.11. of BAIT.
[32] See I.3. of BAIT.
[33] Available for purchase here.
[34] Version February 2022 available here. BSI Standards available here.
[35] Available here.
[36] Available here.

Outlook and next steps for in-scope firms

In-scope firms will want to proactively address compliance with the ICT requirements and supervisory expectations, regardless of their size or complexity. Regulation is expected to evolve continuously, particularly in the area of digital operational resilience and ICT risk, both at the national and EU level.

As a result, financial services firms and other stakeholders affected by the changes discussed above as well as those that are taking place at the EU-27-level as well as those specific to Banking Union supervision, should review and update their ICT arrangements, project governance policies and procedures to ensure that the justification for certain compliance actions and measures can be promptly and clearly demonstrated and explained to relevant supervisory authorities.

As a result, in-scope firms ought to carefully identify and compile the ICT requirements applicable to them as a result of BAIT and multiple other requirements stipulated in EU and local regulation as well as supervisory guidance. In terms of BAIT, this includes in-scope firms, working together with ICT service providers to:

New requirements following BAIT's August 2021 Amendments

- Operational IT security
- IT emergency management with greater focus on operational resilience and business continuity planning
- Relationships with paymant services users

Existing requirements under BAIT

- IT Strategy
- Outsourcing and external procurement
- IT Projects
- IT Governance
- IT operations
- KRITIS Module
- IT Risk Management
- Information security management
- User access management

Broadening of existing concepts and supervisory expectations

- Expansion of the information network IT process – business process
- IT security measures and processes, threat identification and reaction to security-relevant events
- Emergency management guidelines, emergency plans, emergency test concepts and tests
- Implementation availability and capacity management

Impact on firm

Time and effort

High	☑
Medium	■
Low	■

Impact on

Business units	☑
IT	☑
Processes	☑

Strategic delivery

Near term	☑
Medium term	■
Long term	☑

[1] Very dependent on the state of existing compliance with BAIT and other similar rules

Specific challenges in complying with BAIT´s August 2021 Amendments

- Meeting BSI Information Standards
- Cooperation with IT security and emergency management third party service providers
- Identifying and obtaining necessary information

Moreover, in-scope firms may want to review and update their ICT-relevant contractual as well as other documented arrangements, project governance policies and procedures to ensure that justifications for certain actions and compliance measures can be evidenced and explained to supervisors.

If you have any questions or need help with the implementation of the regulatory requirements, we will be happy to support you. Affected financial services firms' next steps could look like this:

- Performing a global but equally business-line specific gap analysis that maps the extent of global, EU-27, Banking Union specific and national-level driven changes and, absent such changes, assess which areas ought to be prioritised as part of an action plan to meet BAIT's requirements as well as those to be introduced as part of DORA;
- Assessing, especially for smaller and/or less complex firms, whether there are any permitted options to apply the relevant frameworks and supervisory expectations in a proportionate and/or simplified manner;
- Review their ICT strategy and, where relevant, introduce targeted amendments to ensure greater focus on ICT risk and mitigation arrangements including enhancing the role of the ICT security officer, ICT access and control rights along with centralised recording and reporting channels so as to meet the more granular details set in the updated BAIT (as possibly "forward proofed" for DORA's impact) in terms of rules but also KPIs, outputs and quality assurance metrics as applicable to run the business and run the compliance workstreams; and
- Engage proactively with ICT service providers, including third-party, software as a service (SaaS) and/or cloud-based service providers, to ensure that any documentation and non-documentation based changes, which are undertaken within a specific financial services firm (including any individual business units) to meet BAIT compliance are effectively tracked through with those ICT service providers, including through change management requests and evidence that changes mean ICT systems are both sufficiently resilient but equally compliant with what BAIT requires of in-scope financial services firms.

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these reforms including conducting compliance gap analysis and assisting with remedial actions. If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via: de_eufinreg@pwc.com.

Contact

Dr. Michael Huertas LLM., MBA
Partner, Head of Financial Institutions
Regulatory Europe
PwC Legal Deutschland
Mobile: +49 160 9737-5760
michael.huertas@pwc.com

About us

In today's rapidly evolving marketplace, our clients are increasingly concerned with business collaborations, restructuring, mergers and acquisitions, financing and questions of social responsibility. They need legal security when dealing with such complex issues. That is why we work closely with PwC's tax, human resources and finance experts and draw on the resources of our legal network in more than 100 countries to deliver comprehensive advice. Whether a global player, a public body or a wealthy individual, each client can rely on a personal account manager to address his or her specific legal needs. This dedication helps us ensure our clients' long-term business success.

PwC Legal. More than 220 lawyers at 18 locations. Integrated legal advice for the real world.