BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Supervisory Requirements for IT in Financial Institutions

Bankaufsichtliche Anforderungen an die IT – BAIT in the version of 14.09.2018

This English version is provided for information purposes only. The original German text is binding in all respects.

Contents

I. Preliminary remarks

1 The use of information technology (IT) in the institutions, including the use of IT services supplied by IT service providers, is key for the finance industry and its importance will continue to grow. This Circular provides a flexible and practical framework for institutions' technical and organisational resources on the basis of section 25a (1) of the German Banking Act (Kreditwesengesetz) – in particular for IT resource management and IT risk management. Moreover, it specifies the requirements laid down in section 25b of the Banking Act (outsourcing of activities and processes).

2 This is without prejudice to the requirements contained in the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – MaRisk), which are fleshed out in this Circular. The depth and scope of the topics addressed in this Circular are not exhaustive. Hence, pursuant to section 25a (1) number 4 of the German Banking Act in conjunction with AT 7.2 number 2 of MaRisk, the institution 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. These standards include, for example, the IT Baseline Protection manuals (Grundschutz) issued by the Federal Office for Information Security (BSI) and standard ISO/IEC 2700X of the International Organization for Standardization.

3 The principles-based requirements of this Circular enable the principle of dual proportionality to be implemented (see AT 1 numbers 3, 5 and 7 as well as AT 2.1 number 2 of MaRisk in particular).

4 The scope for this Circular is the same as defined in AT 2.1 of MaRisk.

II. Requirements

1. IT strategy

1 The IT strategy shall fulfil the requirements set out in AT 4.2 of MaRisk. This includes in particular the requirement for the management board to define a sustainable IT strategy outlining the institution's objectives and the measures to be taken to achieve these objectives.

2 The management board shall define an IT strategy that is consistent with the business strategy. The IT strategy shall contain as a minimum:

(a) strategic development of the institution's organisational and operational structure of IT and of the outsourcing of IT services;
(b) allocation to IT of the generally established standards by which the institution abides;
(c) responsibilities and integration of information security into the organisation;
(d) strategic development of IT architecture;
(e) statements on contingency management giving due consideration to IT issues;
(f) statements on IT systems developed and/or run by the organisational units themselves (hardware and software components).

Re (a): Description of the role, positioning and philosophy of IT with regard to staffing and budget for the organisational and operational structure of IT as well as overview and strategic classification of IT services. Statements on the outsourcing of IT services may also be included in the strategic information on outsourcing.

Re (b): Selection of generally established standards and application to the institution's IT processes as well as overview of envisaged scope of implementation for each standard.

Re (c): Description of the importance of information security in the institution and of how information security is embedded in the organisational units and in the collaboration model with each IT service provider.

Re (d): Depiction of target IT architecture in the form of an overview of the application landscape.

2. IT governance

3	IT governance is the structure used to manage and monitor the operation and further development of IT systems including the related IT processes on the basis of the IT strategy. The key regulations here are in particular those on the organisational and operational structure of IT (see AT 4.3.1 of MaRisk), information risk management and information security management (see AT 4.3.2 of MaRisk, AT 7.2 numbers 2 and 4 of MaRisk), the appropriateness of the quantity and quality of the institution's IT staffing (see AT 7.1 of MaRisk) as well as the scope and quality of technical and organisational resources (see AT 7.2 number 1 of MaRisk). Regulations governing the organisational and operational structure of IT shall be swiftly amended in the event of modifications to the activities and processes (see AT 5 number 1 of MaRisk).	
4	The management board is responsible for ensuring that the regulations governing the organisational and operational structure of IT are defined on the basis of the IT strategy and are swiftly amended in the event of modifications to the activities and processes. The institution shall ensure that the regulations governing the organisational and operational structure of IT are implemented effectively.	
5	The institution shall ensure that appropriate staff, in terms of both quality and quantity, are available for information risk management, information security management, IT operations and application development in particular.	With regard to measures to ensure that the quality of staff remains appropriate, the institution shall in particular give consideration to technological advancements as well as current and future development of the threat level.
6	Conflicts of interest and activities that are not compatible with each other shall be avoided within the organisational and operational structure of IT.	Conflicts of interest between activities connected, for example, with application development and tasks performed by IT operations can be countered by taking organisation or operational measures and/or by defining roles adequately.
7	The management board shall define appropriate quantitative or qualitative criteria for managing those areas responsible for operations and for the further development of IT systems, and compliance with them shall be monitored.	The following elements can be considered when defining such criteria: quality of performance, availability, maintainability, adjustability to new requirements, security of IT systems or the related IT processes, and cost.

3. Information risk management

8	The processing and sharing of information in business and service processes is supported by data-processing IT systems and related IT processes. The scope and quality thereof shall be based, in particular, on the institution's internal operating needs, business activities and risk situation (see AT 7.2 number 1 of MaRisk). The IT systems and related IT processes shall ensure the integrity, availability, authenticity and confidentiality of the data (see AT 7.2 number 2 of MaRisk). The institution shall define and coordinate the tasks, competencies, responsibilities, controls and reporting channels required for the management of information risk (see AT 4.3.1 of MaRisk). To this end, the institution shall set up appropriate monitoring and steering processes (see AT 7.2 number 4 of MaRisk) and define the related reporting requirements (see BT 3.2 number 1 of MaRisk).	
9	The components of an information risk management system shall be implemented in line with the competencies of all the key parties and functions involved and with no conflicts of interest.	The key parties involved also include the organisational units that own the information.
10	The institution shall have an up-to-date overview of the components of the defined information domain as well as any related dependencies and interfaces. The institution shall be guided in this respect in particular by internal operating needs, business activities and the risk situation.	An information domain includes, for example, business-relevant information, business processes, IT systems as well as network and building infrastructures.
11	The method used to determine the level of protection required (in particular, with regard to the protection objectives "integrity", "availability", "confidentiality" and "authenticity") shall ensure that the resulting protection requirements are consistent and comprehensible.	Categories of protection requirements could be "low", "medium", "high" and "very high".
12	The institution shall define and suitably document its requirements for implementing the protection objectives in the various categories of protection requirements (catalogue of target measures).	The catalogue of target measures contains only the requirements and not how these are to be met in practice.
13	The risk analysis on the basis of the defined risk criteria shall be conducted by comparing the target measures and the measures that have been successfully implemented in each case. Other risk-reducing measures due to target measures that have not been implemented completely shall be effectively coordinated,	Risk criteria contain, for example, potential threats, potential for damage, frequency of damage as well as risk appetite.

documented, monitored and managed. The results of the risk analysis shall be approved and transferred to the process of operational risk management.

14 The management board shall be informed regularly, but at least once a quarter, in particular about the results of the risk analysis as well as any changes in the risk situation.

4. Information security management

15 Information security management makes provisions for information security, defines processes and manages the implementation thereof (see AT 7.2 number 2 of MaRisk). Information security management follows a continuous process that comprises a planning, implementation, success monitoring, optimisation and improvement phase. The content of the information security officer's reporting requirements to the management board as well as the frequency of reporting shall be based on BT 3.2 number 1 of MaRisk.

16 The management board shall agree an information security policy and communicate this appropriately within the institution. The information security policy shall be in line with the institution's strategies.

The information security policy defines the objectives and the scope for information security and describes the material organisational aspects of information security management. Regular checks and adjustments to changed conditions are made on a risk-oriented basis. In addition to modifications to the organisational and operational structure as well as to the institution's IT systems (business processes, specialist tasks, organisational set-up), this could also be changes in the external conditions (e.g. legal or regulatory requirements), in the threat scenarios or in security technologies.

17 Based on the information security policy, the institution shall define more specific, state-of-the-art information security guidelines and information security processes for the identification, protection, discovery, response and recovery sub-processes.

Information security guidelines are compiled, for example, for the network security, cryptography, authentication and logging areas.

The primary aim of information security processes is to meet the agreed protection objectives. These include inter alia preventing and identifying information security incidents as well as responding to them appropriately and ensuring adequate communication in due course.

18 The institution shall establish an information security officer function. This function is responsible for all information security issues within the institution and with regard to third parties. It ensures that information security objectives and measures defined in the institution's IT strategy, information security policy and information security guidelines are transparent both within the institution and for third parties, and that compliance with them is reviewed and monitored.

The information security officer function has in particular the following tasks:

- supporting the management board when defining and changing the information security policy and advising on all issues of information security; this includes helping to resolve conflicting goals (e.g. economic aspects versus information security);
- compiling information security guidelines and, where appropriate, any other relevant regulations as well as checking compliance;
- managing and coordinating the institution's information security process as well as monitoring the involvement of IT service providers and assisting in any related tasks;
- supporting to draw up and amend the contingency plan with regard to IT issues;
- initiating and monitoring the implementation of information security measures;

		■ participating in projects relevant to IT; ■ acting as a contact for any questions relating to information security coming from within the institution or from third parties; ■ examining information security incidents and reporting these to the management board; ■ initiating and coordinating measures to raise awareness of and training sessions on information security.
19	In terms of organisation and processes, the information security officer function shall be independent to avoid any potential conflicts of interest.	The following measures, in particular, are applied to avoid any potential conflicts of interest: ■ a description of the information security officer's (and his/her deputy's) function and duties; ■ determination of resources required by the information security officer function; ■ a designated budget for information security training sessions within the institution and for the personal training of the information security officer and his/her deputy; ■ information security officer is able to report directly and at any time to the management board; ■ all employees of the institution as well as IT service providers are required to report any incidents relevant to IT security that concern the institution immediately and in full to the information security officer; ■ the information security officer function shall be independent of those areas that are responsible for the operation and further development of IT systems; ■ the information security officer may on no account be involved in internal audit activities.
20	As a rule, each institution shall have its own information security officer function in-house.	In the case of regionally active institutions (in particular those that belong to an association) as well as small institutions (in particular those that belong to a group) that do not have material, internally run IT operations but do have a similar business model and shared IT service providers for bank-specific processes it is permissible, with regard to the regular (association-wide or group-wide) control mechanisms available, for multiple institutions to appoint a joint information security officer as long as contractual conditions are in place to ensure that this joint information security officer can fulfil the relevant tasks for all the institutions in question at all times. However, in such cases, each institution shall name a competent contact person for the information security officer.

		As a rule, institutions may combine the information security officer function with other internal functions. This is without prejudice to an institution's option of obtaining external support by means of a service contract.
21	After an information security incident, the impact on information security shall be analysed and appropriate follow-up measures approved.	The definition of "information security incident" in terms of nature and scope is based on the protection requirement for the business processes, IT systems and relevant IT processes in question. An event may also be deemed an information security incident if at least one of the protection objectives ("availability", "integrity", "confidentiality", "authenticity") as specified in the institution's target information security concept is violated in excess of the defined threshold. The definition of "information security incident" shall clearly differ from that of "deviation from standard operations" (in the sense of "disruption in daily operations").
22	The information security officer shall report to the management board regularly, at least once a quarter, and on an ad hoc basis on the status of information security.	The status report contains, for example, an evaluation of the information security situation compared to the last report, information about information security projects, information security incidents and the results of penetration tests.

5. User access management

23 User access management ensures that access rights granted to users are in line with and used as defined in the institution's organisational and operational requirements. User access management shall meet the requirements set out in AT 4.3.1 number 2, AT 7.2 number 2 as well as BTO number 9 of MaRisk.

24 User access rights concepts define the scope and the conditions of use for access rights to IT systems in a manner that is consistently in line with the determined protection requirements and can be completely and comprehensibly deduced for all access rights for an IT system. User access rights concepts shall ensure that users are assigned access rights according to the need-to-know principle, that the segregation of duties is observed and that staff conflicts of interest are avoided.

One possible condition for use is limiting the time for which access rights are granted. Access rights can be granted for personalised, non-personalised and technical users.

25 It must be possible for non-personalised access rights to be unequivocally traced back to an active person at all times (wherever possible, automatically). Any departures from this in justifiable exceptional cases and the resultant risks shall be approved and documented.

26 Approval and control processes shall ensure compliance with the requirements contained in the user access rights concept when setting up, changing, deactivating or deleting access rights for users. The responsible organisational unit shall be appropriately involved, thus enabling it to fulfil its organisational responsibilities.

Setting up, changing, deactivating or deleting access rights requires an access rights application to be implemented in the target system.

27 The control bodies responsible for setting up, changing, deactivating or deleting access rights shall also be involved in reviewing whether access rights granted are still required and whether these comply with the requirements contained in the user access rights concept (recertification).

If during recertification it is discovered that access rights have been granted in breach of the prescribed procedure, these access rights shall be removed in line with the standard procedure for setting up, changing and deleting access rights.

28 The setting up, changing, deactivating and deleting of access rights and recertification shall be documented in a way that facilitates comprehension and analysis.

29	The institution shall set up logging and monitoring processes consistent with the protection requirements and the target requirements that enable checks to be carried out to ensure that access rights are used only in the manner intended.	Overarching responsibility for the processes used to log and monitor access rights shall be assigned to a party that is independent of the authorised user in question and his/her organisational unit. Owing to the far-reaching intervention options of privileged users, the institution shall in particular set up appropriate processes to log and monitor their activities.
30	Accompanying technical and organisational measures shall be implemented to ensure that the requirements contained in the user access rights concepts cannot be circumvented.	Examples of such measures are: ■ a selection of appropriate authentication procedures; ■ implementation of a policy to use secure passwords; ■ screen savers that are automatically secured with a password; ■ data encryption; ■ tamper-proof implementation of logging; ■ measures to raise staff awareness.

6. IT projects, application development (including by end users in the organisational units)

31	Material modifications to the IT systems in the course of IT projects, their impact on the organisational and operational structure of IT and on the related IT processes shall be evaluated as part of an impact analysis (see AT 8.2 of MaRisk). With respect to their first use and material modifications to IT systems, the requirements set out in AT 7.2 (in particular numbers 3 and 5) of MaRisk, AT 8.2 number 1 of MaRisk and AT 8.3 number 1 of MaRisk shall be met.	
32	Rules shall be defined for the organisational framework of IT projects (including quality assurance measures) and the criteria for its application.	
33	IT projects shall be managed appropriately, particularly taking account of risks in relation to the duration, use of resources, and quality of IT projects. To this end, model procedures shall be defined and compliance with them shall be monitored.	For example, the decision to transition between project phases can depend on clear quality criteria set out in the relevant model procedure.
34	The portfolio of IT projects shall be monitored and managed appropriately. Due account shall be taken of the fact that risks can also stem from interdependencies between different projects.	The portfolio view facilitates an overview of the IT projects together with the relevant project data, resources, risks and dependencies.
35	Major IT projects and IT project risks shall be reported to the management board regularly and on an ad hoc basis. Material project risks shall be taken account of in the risk management.	
36	Appropriate processes shall be defined for application development which contain specifications for identifying requirements, for the development objective, for (technical) implementation (including coding guidelines), for quality assurance, and for testing, approval and release.	Application development includes, for example, the development of software to support bank-specific processes or the applications developed internally by end users in the organisational units (e.g. end-user computing, EUC). The processes are designed in a risk-oriented way.
37	Requirements for the functionality of the application must be compiled, evaluated and documented in the same way as for non-functional requirements. The	Examples of requirements documents include:

organisational units shall be responsible for compiling and evaluating the requirements.

- Functional specifications (user requirements specification or user story);
- technical specifications (target specification document or product backlog).

Examples of non-functional requirements for IT systems include:

- results of the protection requirements analysis;
- access rules;
- ergonomics;
- maintainability;
- response times;
- resilience.

38 In the context of application development, appropriate arrangements shall be made, consistent with the protection requirement, such that after the application goes live the confidentiality, integrity, availability and authenticity of the data to be processed are comprehensibly assured.

Suitable arrangements may include:

- checking of input data;
- system access control;
- user authentication;
- transaction authorisation;
- logging of system activity;
- audit logs;
- tracking of security-related incidents;
- handling of exceptions.

39 In the context of application development, arrangements shall be made to enable the identification of whether an application was unintentionally modified or deliberately manipulated.

A suitable arrangement, taking account of the protection requirement, may be reviewing the source code during application development. Source code review is a systematic examination in order to identify risks.

40 The application and its development shall be documented in a clearly structured way and in a manner that is readily comprehensible for competent third parties.

The application documentation includes the following content as a minimum:

- user documentation;
- technical system documentation;
- operating documentation.

The comprehensibility of the application development is aided by a version history of the source code and requirements documents, for example.

41 A methodology for testing applications prior to their first use and after material modifications shall be defined and introduced. The scope of the tests shall include the functionality of the application, the security controls and system performance under various stress scenarios. The organisational unit responsible for the application shall be tasked with performing the technical acceptance tests. Test environments for performing the acceptance tests shall correspond to the production environment in aspects material to the test. Test activities and test results shall be documented.

This comprises relevant expertise as well as appropriately structured independence from the application developers.

Test documentation contains the following points as a minimum:

- test case description;
- documentation of the parameterisation underlying the test case;
- test data;
- expected test result;
- actual test result;
- measures derived from the tests.

42 After the application goes live, any deviations from standard operations shall be monitored, their causes shall be investigated and, where appropriate, measures for subsequent improvement shall be taken.

Indications of serious shortcomings may include, for example, repeated incidences of deviations from standard operations.

43 An appropriate procedure shall be defined for the classification/categorisation (protection requirements category) and handling of the applications developed or run by the business unit's end users.

Compliance with coding standards will also be ensured for the applications developed by end users in the organisational units (e.g. EUC application). Each of these applications will be assigned to a protection requirements category. If the identified protection requirement exceeds the technical protection capability of these applications, protective measures will be taken contingent on the results of the protection requirements classification.

44 Rules shall be defined on the identification of all applications developed or run by the organisational unit's end users, on documentation, on the coding guidelines and on the testing methodology, on the protection requirements analysis and on the recertification process for authorisations (e.g. in EUC guidelines).

To serve as an overview and in order to avoid redundancies, a central register of these applications will be maintained, and the following information will be collected as a minimum:

- name and purpose of the application;
- version history, date;
- externally or internally developed;
- staff member(s) responsible for specialist aspects;
- staff member(s) responsible for technical aspects;
- technology;
- result of the risk classification/protection requirements classification and, where appropriate, the protective measures derived from these.

7. IT operations (including data backup)

45 IT operations shall fulfil the requirements resulting from the implementation of the business strategy as well as from the IT-supported business processes (see AT 7.2 numbers 1 and 2 of MaRisk).

46 The components of the IT systems and their connections with each other shall be administered in a suitable way, and the inventory data collected for this shall be updated regularly and on an ad hoc basis.

Inventory data include, in particular:

- inventory and specified use of the IT system components with the relevant configuration data;
- location of the IT system components;
- list of the relevant information about warranties and other support agreements (including links where appropriate);
- details of the expiry date of the support period for the IT system components;
- accepted non-availability period of the IT systems as well as the maximum tolerable data loss.

47 The portfolio of IT systems shall be managed appropriately. This shall also take account of the risks stemming from outdated IT systems (lifecycle management).

48 The processes for changing IT systems shall be designed and implemented depending on their nature, scale, complexity and riskiness. This shall also apply to newly procured or replaced IT systems as well as to security-related subsequent improvements (security patches).

Examples of changes include:

- expanding functions of or rectifying errors in software components;
- migrating data;
- changing configuration settings of IT systems;
- replacing hardware components (servers, routers etc.);
- using new hardware components;
- relocating IT systems.

49 Change requests for IT systems shall be accepted, documented, evaluated taking due account of potential implementation risks, prioritised and approved in an orderly way, and implemented in a coordinated and secure way.

Steps to securely implement the changes to live operations include, for example:

- risk analysis relating to the existing IT systems (particularly including the network and the upstream and downstream IT systems), including in respect of possible security or compatibility problems, as a component of the change request;

- testing of changes prior to going live for possible incompatibilities of the changes as well as possible security-critical aspects for key existing IT systems;
- testing of patches prior to going live taking account of their criticality (e.g. for security or emergency patches);
- data backups for the IT systems concerned;
- reversal plans to enable an earlier version of the IT system to be restored if a problem occurs during or after going live;
- alternative recovery options to allow the failure of primary reversal plans to be countered.

For low-risk configuration changes/parameter settings (e.g. changes to the layout of applications, replacement of defective hardware components, installation of processors), different process rules/checks can be defined (e.g. dual control principle, documentation of changes or of downstream checks).

50 Reports of unscheduled deviations from standard operations (disruptions) and their causes shall, in a suitable way, be recorded, evaluated, prioritised with particular regard to potentially resulting risks, and escalated according to defined criteria. The processing, analysis of causes, and identification of solutions, including follow-up, shall be documented. An orderly process for the analysis of possible correlations between disruptions and of their causes must be in place. The processing status of outstanding reports of disruptions, as well as the appropriateness of the evaluation and prioritisation, shall be monitored and managed. The institution shall define suitable criteria for informing the management board about disruptions.

Risks can be identified by flagging the breach of protection objectives, for example. Causes are also analysed wherever multiple IT systems are used to record and process disruptions and their causes.

51 The provisions governing the data backup procedures (excluding data archiving) shall be set out in writing in a data backup strategy. The requirements contained in the data backup strategy for the availability, readability and timeliness of the customer and business data as well as for the IT systems required to process them shall be derived from the requirements for the business processes and from the business continuity plans. The procedures for recoverability in the required timeframe and for readability of data backups shall be tested regularly, at least once a year, as part of a sample as well as on an ad hoc basis.

The requirements for the structure and storage of data backups as well as for the tests to be performed stem from related risk analyses. With regard to the locations for the storage of data backups, one or multiple additional locations may be required.

8. Outsourcing and other external procurement of IT services

52 IT services encompass all forms of IT procurement; in particular, this includes the provision of IT systems, projects/computer-aided construction projects or staff. Outsourcing of IT services shall meet the requirements pursuant to AT 9 of MaRisk. This shall also apply to the outsourcing of IT services which are provided to the institution by a services firm via a network (e.g. processing, storage, platforms or software) and which are supplied, used and invoiced dynamically and tailored to requirements via defined technical interfaces and protocols (cloud services). The institution shall still comply with the general requirements relating to a proper business organisation pursuant to section 25a (1) of the Banking Act in the case of other external procurement of IT services (see AT 9 number 1 of MaRisk). For each software procurement, the associated risks shall be appropriately assessed (see AT 7.2 number 4 sentence 2 of MaRisk).

53 Given the fundamental importance of IT to the institution, a risk assessment shall also be performed prior to each instance of other external procurement of IT services.	The institution can flexibly define the nature and scope of a risk assessment, taking account of proportionality aspects, pursuant to its general risk management. For equivalent forms of other external procurement of IT services, use can be made of existing risk assessments. The functions of the institution responsible for information security and contingency management are to be involved.
54 Other external procurement of IT services shall be managed in line with the strategies, taking account of the institution's risk assessment. The rendering of the service owed by the service provider shall be monitored in line with the risk assessment.	A complete, structured contract overview will be maintained for this purpose. Outsourcing management can be performed by bundling contracts for other external procurement of IT services on the basis of this contract overview (contract portfolio). Existing management mechanisms can be used for this purpose.
55 The contractual arrangements shall take appropriate account of the measures derived from the risk assessment relating to other external procurement of IT services. Appropriate account shall be taken of the results of the risk assessment in the operational risk management process, primarily in the overall risk assessment for operational risk.	For example, this includes arrangements for information risk management, for information security management and for contingency management, which normally correspond to the institution's objectives. Where relevant, the possibility of the outage of an IT service provider is also taken into account and a related exit or alternative strategy developed and documented. Measures found to be necessary are also taken into account in cases where subcontractors are involved.

56 The risk assessments relating to other external procurement of IT services shall be reviewed and amended regularly and on an ad hoc basis, together with the contractual details, where appropriate.

9. Critical infrastructure

57 Against the backdrop of the other sections of the BAIT and the other relevant supervisory requirements for financial institutions concerned with ensuring that appropriate precautions are taken to guarantee the availability, integrity, authenticity and confidentiality of information processing, this section is directed specifically at operators of critical infrastructure (CI operators[1]).

It adds requirements for the effective implementation of special measures to achieve the critical infrastructure protection (CIP) objective to the Supervisory Requirements for IT in Financial Institutions. The CIP objective shall be understood here as maintaining the society's security of supply for the critical services named in section 7 of the BSI-KritisV (cash supply, card-based payment transactions, conventional payment transactions and the clearing and settlement of securities and derivatives transactions), because the failure or impairment of these services could lead to serious supply disruptions or threats to the public security.

The CI operators concerned (and, where services are outsourced, their IT service providers too) shall describe and effectively implement appropriate measures for critical services to reduce the risks to the secure operation of critical infrastructure to a level appropriate for the CIP objective. To do this, CI operators and their IT service providers shall align themselves with the relevant standards and consider high availability concepts. Thereby state of the art technology shall be adhered to.

Companies may choose to use this section to provide verification under section 8a (3) of the Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI Act) within the context of an audit of the annual financial statements. This requires that all information technology systems, components and processes that are part of the critical infrastructure are covered by the audit in full.

Alternatively, CI operators can adopt a company-specific approach or create an industry-specific security standard (B3S) under section 8a (2) of the BSI Act. In such cases, the verification under section 8a (3) of the BSI Act shall be produced in consultation with a suitable auditing body (see relevant FAQs on the website of the Federal Office for Information Security).

58 The extent of critical infrastructure within the information domain shall be clearly tagged. Thereby all relevant interfaces should be included.

All relevant BAIT requirements and other supervisory requirements shall be applied to all components and areas of the critical service in a clear and comprehensible manner.

Critical services must be monitored appropriately. The potential impact that security incidents could also have on critical services shall be assessed.

For example, this can be achieved by tagging the components and areas of the information domain, that are part of the critical infrastructure within the inventory according to no. 46 of the BAIT (e.g. in a configuration management database - CMDB). This should include information on the relationship with the respective facility classes of the CI operator that are to be audited.

Appropriate measures have to ensure that the systems needed for the operation of the critical services have a resilient architecture.

[1] See the First Regulation Amending the Regulation on the Identification of Critical Infrastructures in accordance with the Act on the Federal Office for Information Security (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz – BSI-KritisV).

59 The information risk management and information security management under sections 3 and 4 of the BAIT shall take the CIP objective into account and adopt measures to ensure that it is achieved. In particular, risks that have the potential to impair critical services to a significant degree shall be reduced using appropriate measures for risk mitigation and risk avoidance to a level appropriate for the CIP objective. Measures which are able to counter the risks to availability when the need for protection is high or very high are particularly suitable for this. Among other things, high availability concepts should therefore be examined and, if appropriate, applied.

In principle, appropriate measures shall be taken to mitigate risks. This should involve maintaining state of the art technology.

However, this shall be kept in proportion: the required effort and expenditure should be proportionate to the consequences of the critical infrastructure concerned failing or being impaired. This means that while risks can be accepted or transferred, this decision must be taken while ensuring supply security, and not just on the basis of economic considerations. For example, risks relating to critical services must not be accepted if precautions against them would be possible and appropriate with state of the art technology. Transferring risk, e.g. using insurance, is not a substitute for appropriate precautions either. This does not preclude the company from concluding an insurance contract, e.g. for economic reasons.

60 The CIP objective shall always be taken into account, from when the protection requirements are determined, during the definition of appropriate measures and through to the effective implementation of these measures, including the implementation and regular testing of relevant emergency preparedness measures.

In particular, this shall be considered in relation to the following aspects:

- The CIP objective shall also be taken into account when services are outsourced under sections 25a and 25b of the German Banking Act (Kreditwesengesetz – KWG) in conjunction with AT 9 and AT 5 number 3f of the MaRisk and section 8 of the BAIT.
- The emergency preparedness planning shall include measures to allow critical services to be maintained even in an emergency situation.

61 The verification under section 8a (3) of the BSI Act regarding compliance with the requirements under section 8a (1) of the BSI Act can be conducted as part of the audit of the annual financial statements. CI operators are to submit the relevant verification documents to the BSI on time, in accordance with the relevant requirements of the BSI.

When providing verification as part of the audit of the annual financial statements, CI operators should reference the compliance with the requirements under section 8a (1) of the BSI Act for the first time in the 2018 annual financial statements and provide verification of this to the BSI at least every two years thereafter.

There are other permissible ways to provide verification aside from the audit as part of the annual financial statements. In this regard, CI operators should take note of the current version of the “Orientation Guide to Verification According to § 8a (3) BSI Act”.