BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Circular 10/2017 (BA) in the version of 16.08.2021

To all credit institutions and financial services institutions in the Federal Republic of Germany

Supervisory Requirements for IT in Financial Institutions (BAIT)

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

Contents

I. Preliminary remarks

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

2 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, information risk management and information security management. Moreover, it specifies the requirements laid down in section 25b of the Banking Act (outsourcing of activities and processes).

3 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) sentence 3 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 over and above the specifications in this Circular. These standards include, for example, the IT *Grundschutz* issued by the Federal Office for Information Security (BSI) and the ISO/IEC 270XX international security standards of the International Organization for Standardization.

4 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).

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

II. Requirements

1. IT strategy

1.1. 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.

1.2. The management board shall define an IT strategy that is consistent with the business strategy. As a minimum it shall contain:

(a) strategic development of the institution's organisational and operational structure of IT and of IT services and other significant dependencies on third parties;

(b) allocation to IT and information security of the generally established standards by which the institution abides;

(c) goals, responsibilities and integration of information security into the organisation;

(d) strategic development of IT architecture;

(e) statements on IT service continuity management giving due consideration to information security requirements;

(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, and potential other significant dependencies on third parties (e.g. central bank functions, information services, telecommunication services, supply 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 and information security management 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. This also includes fundamental statements on information security training and awareness.

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

2. IT governance

2.1.	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 numbers 1 and 2 of MaRisk).	
2.2.	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 these regulations are implemented effectively.	
2.3.	The institution shall ensure that appropriate resources, 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 resources (human, financial and other resources) remains appropriate, the institution shall in particular give consideration to technological advancements as well as the current and future threat level.
2.4.	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.

2.5.	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. Compliance with the criteria 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

3.1.	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, the related IT processes and the other components of the information domain 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 number 2 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).	
3.2.	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 or the information risks.
3.3.	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 and support processes, IT systems and related IT processes, as well as network and building infrastructures. Dependencies and interfaces also take account of the networking of the information domain with third parties.

3.4.	The institution shall determine the protection requirements for the components of its defined information domain, in particular with regard to the protection objectives of “integrity”, “availability”, “confidentiality” and “authenticity”, on a regular and event-related basis. The owners of the information and the organisational units that are responsible for the business processes shall be responsible for determining the protection requirements.	
3.5.	The determination of the protection requirements and the related documentation shall be reviewed by information risk management.	
3.6.	The institution shall define and suitably document requirements that are appropriate for achieving the relevant 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.
3.7.	The institution shall compare the target measures with the measures that have already been effectively implemented in each case (actual measures) on the basis of the defined risk criteria.	In addition to the target/actual comparison, the risk analysis takes accounts of potential threats, potential for damage, frequency of damage as well as risk appetite, among other factors. Other risk mitigation measures can be taken into account here. If target measures cannot be implemented (e.g. due to technical restrictions), other risk mitigation measures can be implemented.
3.8.	Other risk mitigation measures, due to target measures not being completely implemented, shall be effectively coordinated, documented, monitored and managed.	

3.9.	Information management shall coordinate and monitor the risk analysis and transfer its results into the operational risk management process. The handling of risks shall be approved in line with the competencies.	
3.10.	The institution shall keep itself informed about all threats to and weaknesses in its information domain, examine their relevance, assess their impact and, if necessary, take appropriate technical and organisational measures.	Internal and external changes (e.g. to the threat level) shall be taken into consideration. Examples of measures include direct warnings to staff, blocking affected interfaces and replacing affected IT systems.
3.11.	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.	The risk situation also includes external potential threats.

4. Information security management

4.1.	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.	
4.2.	The management board shall agree an information security policy and communicate this within the institution. The information security policy shall be in line with the institution's strategies. The policy shall be reviewed in the event of significant changes in the overall conditions and modified promptly if required.	The information security policy defines the key aspects relating to the protection of confidentiality, integrity, availability and authenticity, as well as the scope for information security. It also describes the material organisational

		aspects, as well as the most important roles and responsibilities in information security management. Among other things, the management board uses the policy to define: ■ overall responsibility for information security; ■ the frequency and scope of information security reporting; ■ the competences relating to the handling of information risks; ■ the fundamental information security requirements relating to staffing, contractors, processes, and technologies. Among other things, the overall conditions include internal changes to the organisational and operational structure or IT systems, as well as external changes, such as to threat scenarios, technologies or legal requirements.
4.3.	Based on the information security policy and the results of information risk management, more specific, state-of-the-art information security policies and information security processes shall be defined.	Information security policies are developed, for example, for the areas of network security, cryptography, identity and access management, logging and physical security (e.g. perimeter and building security). The primary aim of information security processes is to meet the agreed protection objectives. These include inter alia preventing or identifying information security incidents as well as responding to them appropriately and ensuring adequate communication in due course.
4.4.	The management board 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	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);

	third parties, and that compliance with them is reviewed and monitored regularly and on an event-driven basis.	■ preparing information security policies 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 the preparation and updating of the contingency plan with regard to information security issues; ■ initiating and monitoring the implementation of information security measures; ■ monitoring and working to ensure compliance with information security in projects and procurement; ■ 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. The information security officer may be supported by an information security management team.
4.5.	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 function and duties of the information security officer, his/her deputy and if necessary other organisational units;

		■ 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 immediately and comprehensively any incidents relevant to information security that concern the institution 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.
4.6.	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.
4.7.	After an information security incident, the impact on information security shall be analysed promptly 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 affected components of the information domain. 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. The definition of an "information security incident" shall clearly differ from that of a "security-related incident" (in the sense of operational information security) and an "unplanned deviation from standard operations" (in the sense of a "disruption").
4.8.	The institution shall introduce a policy on testing and reviewing measures to protect information security and shall review it regularly and on an event-driven basis and modify it if necessary.	Among other things, the policy shall cover: ■ the general threat level; ■ the institution's individual risk situation; ■ categories of test and review subjects (e.g. the institution, IT systems, components); ■ the nature, scope and frequency of tests and reviews; ■ responsibilities and arrangements for avoiding conflicts of interest.

4.9.	The institution shall define a continuous and appropriate awareness and training programme for information security. The success of the defined awareness and training measures shall be reviewed.	As a minimum, the programme should take account of the following aspects, depending on the target group: ■ personal responsibility for own actions and omissions as well as general responsibilities to protect information; ■ fundamental information security procedures (such as reporting information security incidents) and generally applicable security measures (e.g. regarding passwords, social engineering, preventing malware and procedure if malware is suspected).
4.10.	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. Operational information security

5.1. Operational information security implements information security management requirements. The IT systems, related IT processes and other components of the information domain shall ensure the integrity, availability, authenticity and confidentiality of the data. To ensure this, the design of the IT systems and related IT processes shall generally be based on established standards (see AT 7.2 number 2 of MaRisk). Appropriate monitoring and steering processes shall be established for IT risks, comprising in particular the definition of IT risk criteria, the identification of IT risks, the determination of the protection requirement, protective measures for IT operations derived from it, and the definition of measures to manage and mitigate risks (see AT 7.2 number 4 of MaRisk).

5.2.	Based on the information security policy and the more specific information security policies, the institution shall implement state-of-the-art operational information security measures and processes.	Among other things, information security measures and processes include: ■ vulnerability management for identifying, assessing, managing and documenting vulnerabilities;

		■ network segmentation and control (including compliance of terminal equipment with policies); ■ secure configuration of IT systems (hardening); ■ data encryption for data storage and transmission in line with the protection requirements; ■ multilevel protection of IT systems in line with the protection requirements (e.g. against data loss, manipulation or denial-of-service attacks, or against unauthorised access); ■ perimeter protection, e.g. of properties, data centres and other sensitive areas.
5.3.	Threats to the information domain shall be identified as early as possible. Potentially security-related information shall be evaluated suitably promptly, using a rule-based approach, and centrally. This information shall be protected during transport and storage and shall be held available for an appropriate period for subsequent evaluation.	Examples of potentially security-related information include log data, reports and disruptions that could indicate breaches of protection objectives. As a general principle, the rule-based evaluation (e.g. using parameters, correlation of information, deviations or patterns) of large data volumes requires the use of automated IT systems. Subsequent evaluations include forensic analyses and internal improvement measures. The period of time should be appropriate to the threat level.
5.4.	An appropriate portfolio of rules for identifying security-related events shall be defined. Rules shall be tested before being put into operation. The rules shall be reviewed for effectiveness and updated regularly and on an event-driven basis.	Rules identify, for example, whether there have been increased cases of unauthorised access attempts, whether expected log data is no longer delivered or if the times of the delivering IT systems differ.

5.5.	Security-related events shall be analysed promptly and information security management shall be responsible for responding appropriately to any resulting information security incidents.	Security-related events result, for example, from the rule-based evaluation of potentially security-related information. Prompt analysis and response may require a permanently staffed central unit, for example in the form of a Security Operations Centre (SOC).
5.6.	The security of the IT systems shall be reviewed regularly, on an event-driven basis while avoiding any conflicts of interest. Results shall be analysed to establish any necessary improvements and risks shall be managed appropriately.	The frequency, nature and scope of the review should be based in particular on the protection requirements and the potential vulnerability of the IT system (e.g. extent to which it can be reached from the internet). Examples of types of reviews include: ■ variance analysis (gap analysis); ■ vulnerability scans; ■ penetration tests; ■ simulated attacks.

6. Identity and access management

6.1.	Identity and 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. Identity and 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. All forms of access rights to components of the information domain should be subject to standardised processes and controls.	
6.2.	User access rights concepts define the scope and the conditions of use for access rights to IT systems (access to IT systems and access to data) and access rights to premises in a manner that is consistently in	One possible condition for use is limiting the time for which access rights are granted.

	line with the determined protection requirements and can be completely and comprehensibly derived from the concept for all access rights provided. User access rights concepts shall ensure that users are assigned access rights according to the need-to-know and least-privilege principles, that the segregation of duties is observed across user access rights concepts and that conflicts of interest are avoided. User access rights concepts shall be reviewed regularly and on an event-driven basis and updated if necessary.	Depending on their nature, access rights can be granted for personalised and for non-personalised users (including technical users). Access rights to the IT systems may be present at all levels of an IT system (e.g. operating system, database, application). Examples of technical users are users who are used by IT systems in order to identify themselves to other IT systems or to perform IT routines autonomously.
6.3.	It shall be possible for access to IT systems to be unequivocally traced back to an active or responsible natural person at all times (wherever possible, automatically).	For example, automated activities shall be capable of being allocated to responsible persons. Any deviations from this in justifiable exceptional cases and the resultant risks shall be assessed, documented and subsequently approved by the responsible organisational unit.
6.4.	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 also requires timely or immediate implementation in the target system. Reasons for immediate deactivation or deletion of access rights include the risk of abuse (e.g. if an employee is terminated without notice).
6.5.	The control bodies responsible for setting up, changing, deactivating or deleting access rights shall 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 unauthorised access rights have been granted, they shall be removed in line with the standard procedure and other measures shall be taken if necessary (e.g. analysis of causes, incident report).

6.6.	The setting up, changing, deactivating and deleting of access rights and recertification shall be documented in a way that facilitates comprehension and analysis.	
6.7.	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. Owing to the associated far-reaching intervention options, the institution shall in particular set up appropriate processes to log and monitor the activities with privileged (particularly critical) access rights.	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. As a rule, privileged access rights include the rights to access data centres, technology rooms and other sensitive areas.
6.8.	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 (including strong authentication in the case of remote access); ■ implementation of a policy to use secure passwords; ■ screen saver that is automatically secured with a password; ■ data encryption; ■ tamper-proof implementation of logging; ■ measures to raise staff awareness.

7. IT projects and application development

7.1.	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 number 1 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.	
7.2.	Rules shall be defined for the organisational framework of IT projects and the criteria for its application.	The organisational framework includes: ■ integration of involved persons concerned (in particular the information security officer); ■ project documentation (e.g. project application, project final report); ■ provision of quantitative and qualitative resources; ■ management of project risks; ■ information security requirements; ■ quality control measures not related to the project; ■ lessons learned.
7.3.	IT projects shall be managed appropriately, taking account of their objectives and risks in relation to duration, use of resources, and quality. To this end, model procedures shall be defined and compliance with them shall be monitored.	For example, the decision to transition between project phases or sections can depend on clear quality criteria set out in the relevant model procedure.
7.4.	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.
7.5.	Material IT projects and IT project risks shall be reported to the management board regularly and on an event-driven basis. Material project risks shall be taken account of in the risk management.	

7.6.	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 among other things the development of software, for business and support processes (including end-user computing – EUC). The processes are designed in a risk-oriented way.
7.7.	Requirements for the functionality of the application shall be compiled, evaluated, documented and approved in the same way as for non-functional requirements. Appropriate acceptance and test criteria shall be defined for each requirement. Responsibility for compiling, evaluating and approving the specialist requirements (functional and non-functional) lies with the responsible organisational units.	Requirements documents may differ depending on the model procedure and may include, for example: ■ functional specifications (requirements specification); ■ technical specifications (target specification document); ■ user story/product backlog. Examples of non-functional requirements for IT systems include: ■ information security requirements; ■ access rules; ■ ergonomics; ■ maintainability; ■ response times; ■ resilience.
7.8.	In the context of application development, appropriate arrangements shall be made, depending on the protection requirement, such that after each application goes live the confidentiality, integrity, availability and authenticity of the data to be processed are also comprehensibly assured.	Suitable arrangements 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.
7.9.	The integrity of the application (especially the source code) shall be appropriately safeguarded. In addition, arrangements shall be made to enable the identification of whether an application was unintentionally modified or deliberately manipulated, among other things.	A suitable arrangement, taking account of the protection requirement, may be reviewing the source code. Source code review is a systematic examination in order to identify risks.
7.10.	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.
7.11.	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 measures implemented to protect information and, if relevant, system performance under various stress scenarios. The responsible organisational units shall be responsible for performing acceptance tests.	Performance of the tests requires relevant expertise on the part of the testers as well as appropriately structured independence from the application developers. The protection requirements of the data used for the test shall be taken into account.

	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.	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. In a risk-based approach, the measures to protection information also include penetration tests.
7.12.	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.
7.13.	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 staff (end-user computing – EUC).	Compliance with coding guidelines will also be ensured for the developed EUC applications, for example. Each application will be assigned to a protection requirements category. If the identified protection requirement exceeds the technical protection capability of an application, protective measures will be taken contingent on the results of the protection requirements classification.

7.14. Rules shall be defined on the identification of all applications developed or run by the organisational unit's staff, 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 for 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.

8. IT operations

8.1. 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).

8.2. 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 (e.g. versions and patch levels);
- owners of IT systems and their components;
- 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; ■ protection requirements for IT systems and their components; ■ accepted non-availability period of the IT systems as well as the maximum tolerable data loss.
8.3.	The portfolio of IT systems shall be managed. IT systems should be regularly updated. Risks from outdated IT systems or those no longer supported by the vendor shall be managed (lifecycle management).	
8.4.	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).	Changes to IT systems also include the maintenance of IT systems. 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.

8.5.	Changes to 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. Appropriate processes shall also be established for time-critical changes to IT systems.	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; ■ 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).
8.6.	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. To this end, standard procedures shall be defined, e.g. for measures and communication and re-	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.

	sponsibilities (e.g. for malicious code on terminal devices, malfunctions). 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 shall 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 bodies concerned (e.g. management board, competent supervisory authority) about disruptions.	Standardised incident and problem management solutions can be used for this purpose.
8.7.	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 recovery and safeguarding the readability of data shall be tested regularly, at least once a year, as part of a sample as well as on an event-driven basis.	The requirements for measures for safeguarding data availability, readability and timeliness 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.
8.8.	The current performance and capacity requirements of the IT systems shall be captured. The future performance and capacity requirements shall be estimated. Performance delivery shall be planned and monitored, in particular in order to identify bottlenecks promptly and to respond to them appropriately. The performance and capacity requirements of information security measures shall be taken into account in the planning.	

9. Outsourcing and other external procurement of IT services

9.1.	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 – Explanations – of MaRisk). For each software procurement, the associated risks shall be appropriately assessed (see AT 7.2 number 4 sentence 2 of MaRisk).	
9.2.	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 business continuity management are to be involved.
9.3.	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.
9.4.	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	For example, this includes arrangements for information risk management, for information security management, for business continuity management

	results of the risk assessment in the operational risk management process, primarily in the overall risk assessment for operational risk.	and for IT operations, 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 of the IT service provider are involved.
9.5.	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.	

10. IT service continuity management

10.1.	The institution shall define business continuity management objectives and establish a business continuity management process on this basis. Arrangements shall be made for emergency situations in time-critical activities and processes (contingency plan). The measures defined in the contingency plan shall be suitable for reducing the extent of potential losses (see AT 7.3 number 1 of MaRisk). The contingency plan shall include business continuity and recovery plans. In the event of outsourcing of time-critical activities and processes, the outsourcing institution and the outsourcing provider shall have coordinated contingency plans (see AT 7.3 number 2 of MaRisk). The effectiveness and appropriateness of the contingency plan shall be reviewed regularly. For time-critical activities and processes, it shall be demonstrated at least once a year and on an event-driven basis for all relevant scenarios (see AT 7.3 number 3 of MaRisk).	
10.2.	The objectives and overall conditions of IT service continuity management shall be defined on the basis of the business continuity management objectives.	Among other things, overall conditions include organisational aspects such as interfaces to other areas (including risk management or information security management).

10.3.	On the basis of the contingency plan, the institution shall prepare IT contingency plans for IT systems that support time-critical activities and processes.	IT contingency plans include restart, emergency operation and recovery plans as well as the parameters defined for these, and take account of dependencies in order to restore time-critical activities and processes. Among other things, parameters include: ■ recovery time objective (RTO): ■ recovery point objective (RPO); ■ emergency operation configuration. Among other things, dependencies include: ■ dependencies of upstream and downstream business processes and the IT systems deployed by the institution and (IT) service providers; ■ dependencies in the recovery prioritisation of IT processes and systems; ■ necessary resources for ensuring (limited) continuation of business processes; ■ dependencies on external factors (lawmakers, shareholders, public, etc.).
10.4.	The effectiveness of the IT contingency plans shall be verified by IT contingency tests performed at least once a year. The tests shall cover all IT systems that support time-critical activities and processes. Dependencies between IT systems or of jointly used IT systems shall be adequately taken into account. An IT testing concept shall be prepared for this purpose.	The IT testing concept contains both tests of individual IT systems (e.g. components, individual applications) and their combination into integrated networks (e.g. high-availability clusters) and processes (e.g. access management).

10.5. The institution is required to demonstrate that, if a data centre fails, the time-critical activities and processes can be provided from a sufficiently remote data centre and for an adequate time, as well as for the subsequent restoration of normal IT operation.

11. Managing relationships with payment service users

11.1. The risk mitigation measures required by section 53 of the ZAG to manage operational and security-related risks also contain measures with which the payment service users are addressed directly for risk reduction, in particular of the risk of fraud. This requires the establishment of appropriate management of the relationships with the payment service users.

11.2. The institution shall establish and implement processes through which the awareness of the payment service users for security-related risks relating to the payment services will be improved by supporting and advising the payment service users.

This concerns in particular communication processes for sensitising the institution's own payment service users to risks arising when payment services are used. This sensitisation can take the form of general communications (information on the website) or personal approaches if necessary.

The processes are adapted to the specific current risk situation and threat level and may differ from payment service user to payment service user.

11.3. The support and advice offered to the payment service users shall be kept up-to-date and adapted to new risk situations. Amendments shall be communicated to the payment service user in an appropriate format.

Ultimately, this should enable the payment service user to respond appropriately to current risks and use the payment service safely.

11.4. If permitted by the product functionality, the institution shall offer payment service users an option to deactivate individual payment functions available to them.

An example of such a deactivation would be an option to block foreign transfers outside of SEPA. Corresponding applications may be made online or in writing.

11.5.	If the payment service user has agreed upper limits, the payment service user shall be given an option to adapt the agreed limits.	This may involve adapting the daily limit for credit transfers in online banking, for example.
11.6.	To identify fraudulent or unauthorised use of the payment service user's payment accounts, the institution shall give the payment service user the option to receive alerts about successful and failed transactions.	The goal is to give the payment service users an appropriate level of control over their own transactions or transaction attempts so that the payment service users can themselves detect fraudulent transactions or attempted fraud as early as possible. There is no requirement for continuous and immediate explicit alerts about all transactions and transaction attempts. This is without prejudice to the fraud detection measures to be performed by the institution.
11.7.	The institution shall inform the payment service user promptly about updates to security procedures that could impact the payment service user in the context of providing payment services.	The specific communication channel shall be determined by the institution. The payment service users shall be given an option to adapt appropriately to changed processes and to prepare themselves so that they can use the payment services with as little disruption as possible.
11.8.	The institution shall support the payment service users in relation to all questions, support requests, alerts or irregularities or all security-related questions with regard to the payment services. The payment service users shall be informed appropriately how they can receive this support.	Appropriate communication channels that can be used by all payment service users shall be established. These can be announced e.g. via websites, technical communication channels or in written communications.

12. Critical infrastructure

12.1. Against the backdrop of the other chapters 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 chapter 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 chapter 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).

[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).

12.2.	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 shall 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. 3.3 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 shall ensure that the systems needed for the operation of the critical services have a resilient architecture.
12.3.	The information risk management and information security management under chapters 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, measures shall be taken to mitigate risks. This should involve maintaining state of the art technology. 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 shall be taken while ensuring supply security, and not just on the basis of economic considerations. For example, risks relating to critical services shall 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.
12.4.	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 chapter 9 of the BAIT. ■ the emergency preparedness planning shall include measures (AT 7.3 of MaRisk and chapter 10 of the BAIT) to allow critical services to be maintained even in an emergency situation.
12.5.	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”.