BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Federal Financial
Supervisory Authority

Supervisory Requirements for IT in German Asset Managers (Kapitalverwaltungsaufsichtliche Anforderungen an die IT - KAIT)

Circular 11/2019 (WA) in the version dated 1 October 2019

This translation is furnished for information purposes only. The original German text is binding in all respects.

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Federal Financial
Supervisory Authority

Contents

I. Preliminary remarks

1 The use of information technology (IT) in German asset managers, 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 concretizes the requirements set out in sections 28, 29 and 30 of the German Capital Investment Code (*Kapitalanlagegesetzbuch* – KAGB), sections 4–6 of the Regulation on the Rules of Conduct and Organisational Rules Pursuant to the German Capital Investment Code (*Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsregeln nach dem Kapitalanlagegesetzbuch* – KAVerOV) and Articles 38 to 66 of Commission Delegated Regulation (EU) No. 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council ("AIFMD Level 2 Regulation") with regard to the technical and organisational resources of German asset managers – in particular IT resource management and IT risk management. Additionally, it concretizes the requirements of section 36 of the KAGB and Articles 75 to 82 of the AIFMD Level 2 Regulation (outsourcing) with regard to the outsourcing of IT services and other external procurement of IT services. Because the provisions of the AIFMD Level 2 Regulation apply directly, the requirements relating to organisational requirements, risk management and outsourcing are primarily governed by Articles 38 to 66 and 75 to 82 of the AIFMD Level 2 Regulation. This Circular concretizes elements of these requirements and must therefore only be applied in the second instance to determine the minimum supervisory requirements for IT in German asset managers.

2 This is without prejudice to the requirements for IT contained in the Minimum Requirements for the Risk Management of German Asset Managers (*Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften* – KAMaRisk), which are concretized in greater detail in this Circular. The depth and scope of the topics addressed in this Circular are not exhaustive. Hence, under section 28 (1) sentence 2 number 2 of the KAGB in conjunction with section 8.1 number 3 of KAMaRisk, German asset managers continue to be required to apply generally established standards to the arrangement of the IT systems (hardware and software components) 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 270XX of the International Organization for Standardization.

3 The principle-based requirements of this Circular enable the principle of proportionality to be implemented (see the information in section 1 numbers 2 and 3 of KAMaRisk). Appropriate application of the principle of proportionality and the principle-based requirements also requires German asset managers to take measures that, in individual cases, go beyond the requirements set out in this Circular if this is necessary to safeguard the adequacy and effectiveness of the technical and organisational resources and risk management, in particular in light of the size, complexity, international nature or risk exposure of the German asset manager. To this end, adequate account must also be taken in particular of the technical interfaces to external systems (e.g. depositary, fund administrator, external management company or key outsourcing provider).

4 This Circular applies to German asset managers as defined by section 17 of the KAGB to the extent that they are authorised under section 20 (1) of the KAGB.

This Circular does **not apply** to

- registered German asset managers under section 44 of the KAGB;
- externally managed investment companies;
- branches of EU asset managers under sections 51 and 54 of the KAGB;
- depositaries;
- trustees; and
- valuers.

In the case of externally managed investment companies, the managing German asset manager is responsible for compliance with the requirements of this Circular, whereby the externally managed company must be consulted to the extent necessary and appropriate.

In particular for German asset managers registered under sections 2 (5) and 44 of the KAGB, the requirements of section 28 of the KAGB and, if relevant, the KAMaRisk apply with regard to the technical and organisational resources that adequately reflect the risks.

German asset managers registered under section 44 of the KAGB, are free to apply the KAIT, to the extent that this is appropriate and feasible.

5 All members of the management board of a German asset manager are responsible for the proper and effective system of governance. To the extent that the requirements of this Circular refer to the management board, this refers in all cases to all members of the management board.

II. Requirements

1. IT strategy

1 The IT strategy must fulfil the requirements set out in section 4.2 of KAMaRisk. This includes in particular the requirement for the management board to define a sustainable IT strategy outlining the German asset manager's objectives and the measures to be taken to achieve these objectives.

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

(a) strategic development of the German asset manager'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 German asset manager 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 German asset manager'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 German asset manager 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.

Re (e): Reproduction of strategic policies regarding II. number 15.

3 The targets defined in the IT strategy must be formulated in such a way that a rational review of target achievement is possible.

4 The IT strategy must be made available to the German asset manager's supervisory board or comparable supervisory body, and discussed with it if appropriate, when it is initially adopted and in the event of any modifications.

5 The content of and any modifications to the IT strategy must be communicated by suitable means within the German asset manager.

2. IT governance

6	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 section 4.3 numbers 1, 4 and 5 of KAMaRisk), information risk management and information security management (see section 4.3 numbers 6, 7, 9, 12 to 15 of KAMaRisk and section 8.1 numbers 1 and 3 of KAMaRisk), the appropriateness of the quantity and quality of the German asset manager's IT staffing and the scope and quality of the technical and organisational resources (see section 8.1 number 2 of KAMaRisk). Regulations governing the organisational and operational structure of IT must be swiftly amended in the event of modifications to the activities and processes (see section 6 numbers 1 and 2 of KAMaRisk). The requirements governing IT contingency management are also based on section 8.2 of KAMaRisk.	
7	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 German asset manager must ensure that the regulations governing the organisational and operational structure of IT are implemented effectively. This also applies to the interfaces to external systems (e.g. depositary, fund administrator, external asset managers or key outsourcing providers).	
8	The German asset manager must 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 German asset manager must in particular give consideration to technological advancements as well as the current and future development of the threat level.
9	Conflicts of interest and activities that are not compatible with each other must 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.
10	The management board must 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 must be monitored.	The following elements can be considered when defining such criteria: quality of performance, availability, maintainability, adaptability to new requirements, security of IT systems or the related IT processes, and cost.

11	Appropriate monitoring and steering processes must be established for IT risks.	
12	The German asset manager must ensure that the IT-related business activities are managed on the basis of workflow descriptions (organisational policies). The degree of detail of the organisational policies must depend on the German asset manager's risk structure.	With regard to the description of the organisational policies, the most important criterion is that they are appropriate and understandable by the members of the German asset manager's staff. The specific nature of their description is a matter for the German asset manager. IT-related business activities mean all business activities that are implemented or supported using IT.
13	All staff members must at all times also have the necessary knowledge and experience in the field of IT, depending on their tasks, competencies and responsibilities.	Suitable measures must ensure that the skills of the staff members are appropriate.
14	Any absence or departure of staff members may not lead to long-term disruption of operational workflows.	
15	In the event of any disruption, outage or destruction of IT systems, including interfaces and/or online connectivity, suitable contingency measures must be implemented to ensure there is an appropriate level of business continuity, that the German asset manager is capable of acting and that the interests of investors are protected. The proper functioning of the contingency measures must be tested on a regular basis.	

3. Information risk management

16	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 must be based, in particular, on the German asset manager's internal operating needs, business activities and risk situation (see section 8.1 number 2 of KAMaRisk). The IT systems and related IT processes must ensure the integrity, availability, authenticity and confidentiality of the data (see section 8.1 number 3 of KAMaRisk). The German asset manager must define and coordinate the tasks, competencies, responsibilities, controls and reporting channels required for the management of information risk (see section 4.3 number 5 of KAMaRisk). The German asset manager must set up appropriate identification, assessment, monitoring and steering processes (see section 4.3 numbers 7, 9 and 15 of KAMaRisk) and define the related reporting requirements (see section 4.3 numbers 12 to 14 and section 4.9 of KAMaRisk).	
17	The identification, assessment, monitoring and management processes must comprise in particular the definition of IT risk criteria, the identification of IT risks, the determination of the protection requirement and protective measures for IT operations derived from it, and the definition of measures to manage the remaining residual risks. For software procurement, the associated risks must be appropriately assessed.	
18	The components of an information risk management system must be implemented in line with the competencies of all the key parties and functions involved and with no conflicts of interest.	The relevant business units involved also include the organisational units that own the information.
19	The German asset manager must have an up-to-date overview of the components of the defined information domain as well as any related dependencies and interfaces. The German asset manager must 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.
20	The method used to determine the level of protection required (in particular, with regard to the protection objectives of "integrity", "availability", "confidentiality" and "authenticity") must ensure that the resulting protection requirements are consistent and comprehensible.	Categories of protection requirements could be "low", "medium", "high" and "very high".

21	The German asset manager must 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.
22	The risk analysis on the basis of the defined risk criteria must 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 must be effectively coordinated, documented, monitored and managed. The results of the risk analysis must be approved and transferred to the process of operational risk management.	Risk criteria contain, for example, potential threats, potential for damage, frequency of damage as well as risk appetite.
23	The management board must 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 status report contains, for example, an evaluation of the risk situation compared to the last report (delta report).

4. Information security management

24 Information security management makes provisions for information security, defines processes and manages the implementation thereof (see section 8.1 number 3 of KAMaRisk). 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 must be based on section 4.3 numbers 12, 13 and 17 and section 4.9 of KAMaRisk.

25 The management board must agree an information security policy and communicate this appropriately within the German asset manager.

The information security policy must be in line with the German asset manager'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 German asset manager'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.

26 Based on the information security policy, the German asset manager must 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.

27 The German asset manager must establish an information security officer function. This function is responsible for all information security issues within the German asset manager and with regard to third parties. It ensures that information security objectives and measures defined in the German asset manager's IT strategy, information security policy and information security guidelines are transparent both within the German asset manager 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 German asset manager's information security process as well as monitoring the involvement of IT service providers and assisting in any related tasks; ■ support for drawing up and amending 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 German asset manager 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.
28	In terms of organisation and processes, the information security officer function must 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 German asset manager and for the personal training of the information security officer and his/her deputy; ■ the information security officer is able to report directly and at any time to the management board; ■ all staff members of the German asset manager as well as IT service providers are required to report any incidents relevant to IT security that concern the German asset manager immediately and in full to the information security officer; ■ the information security officer function must 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.
29	As a rule, each German asset manager must have its own information security officer function in-house.	As a rule, German asset managers may combine the information security officer function with other internal functions. If the function is to be combined with the function of the

		data protection officer, the requirements under data protection law must additionally be examined. The information security officer function may only be located outside the German asset manager in the following cases: German asset managers with a small number of staff and no significant in-house IT operations and at which the IT services are predominantly performed by an external IT service provider may transfer the information security officer function to a professionally qualified third party; German asset managers that are members of a group, that have a small number of staff, that do not have any significant in-house IT operations and at which the IT services are predominantly performed by an external IT service provider may also transfer the information security officer function to a superordinate group company. In both cases, the German asset manager must name an internal contact person for the information security officer. This is without prejudice to a German asset manager's option of obtaining external support by means of a service contract.
30	After an information security incident, the impact on information security must 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 German asset manager's target information security concept is violated in excess of the defined threshold. The definition of "information security incident" must clearly differ from that of "deviation from standard operations" (in the sense of "disruption in daily operations").
31	The information security officer must report to the management board regularly, at least once a quarter, and additionally 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 (delta report).

5. User access management

32 User access management ensures that access rights granted to users are in line with and used as defined in the German asset manager's organisational and operational requirements. The user access management must fulfil the requirements set out in section 8.1 number 3 and section 4.5 number 7 of KAMaRisk.

33 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 must 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.

34 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 must be approved and documented.

Non-personalised access rights are not tied to a specific member of staff and may be used by several members of staff (e.g. "admin" user).

35 All technical users must be assigned to a responsible natural person who must be integrated into the recertification process. Defined technical users must be administered in a central registry.

Technical users are users who are used by IT systems in order to identify themselves to third parties or to perform autonomous IT routines. They are used, for example, in machine-to-machine communication.

36 Approval and control processes must 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 must 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.

37	The control bodies responsible for setting up, changing, deactivating or deleting access rights must 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 must be removed in line with the standard procedure for setting up, changing and deleting access rights. This also applies to non-personalised and technical users.
38	The setting up, changing, deactivating and deleting of access rights and recertification must be documented in a way that facilitates comprehension and analysis.	
39	The German asset manager must 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 must 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 German asset manager must in particular set up appropriate processes to log and monitor their activities.
40	Accompanying technical and organisational measures must 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 on choosing 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)

41	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 must be evaluated in advance as part of an analysis of their risk content. In doing so, the German asset manager must also analyse in particular the impact of the planned changes on the control methods and the intensity of controls and on portfolio and risk management. The organisational units integrated into the workflows must be subsequently involved in these analyses. With respect to their first use and material modifications to IT systems, the requirements set out in section 8.1 numbers 4 and 5 of KAMaRisk must be met.	
42	The IT systems must be tested before they go live and approved by the staff members with functional and technical responsibility. The production and testing environments must generally be kept separate. These requirements generally also apply to material modifications of IT systems.	A standard process of development, testing, approval and implementation in the production processes must be established. If modifications of IT systems are performed automatically by third parties and cannot be tested before they go live in the German asset manager, the German asset manager must satisfy itself regularly that the necessary tests are conducted in advance at that third party.
43	Rules must be defined for the organisational framework of IT projects (including quality assurance measures) and the criteria for its application.	IT projects are projects involving modifications to IT systems. The starting point may be in both the organisational unit and in IT.
44	IT projects must 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 must be defined and compliance with them must be monitored.	For example, the decision to transition between project phases can depend on clear quality criteria set out in the relevant model procedure.
45	The portfolio of IT projects must be monitored and managed appropriately. Due account must 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.
46	Major IT projects and IT project risks must be reported to the management board regularly and on an ad hoc basis. Material project risks must be taken account of in the risk management.	

47	Appropriate processes must 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 specialist 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.
48	Requirements for the functionality of the application must be compiled, evaluated and documented in the same way as for non-functional requirements. The responsible organisational units must be responsible for compiling and evaluating these specialist requirements.	Examples of requirements documents include: ■ functional specifications (requirements specification); ■ user story; ■ product backlog; ■ technical specifications (target specification document). Examples of non-functional requirements for IT systems include: ■ results of the protection requirements analysis; ■ access rules; ■ ergonomics; ■ maintainability; ■ response times; ■ resilience.
49	In the context of application development, appropriate arrangements must be made, consistent with the protection requirement, to ensure 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.

50	In the context of application development, arrangements must 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.
51	Both applications developed by third parties for the German asset manager and applications developed in-house and their development must be documented in a clearly structured way and in a manner that is readily comprehensible for competent third parties.	The application and development documentation includes the following content as a minimum: ■ what has been developed?; ■ user documentation; ■ technical and process 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.
52	A methodology for testing applications prior to their first use and after material modifications must be defined and introduced. The scope of the tests must include the functionality of the application, the security controls and system performance under various stress scenarios. If system performance is important for an application, it must also be tested under various relevant stress scenarios. The organisational unit responsible for the application must be tasked with performing the technical acceptance tests. Test environments for performing the acceptance tests must correspond to the production environment in aspects material to the test. Test activities and test results must 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.
53	After the application goes live, any deviations from standard operations must be monitored, their causes must be investigated and, where appropriate, measures for subsequent improvement must be taken.	Monitoring must be increased temporarily after the application goes live. Indications of serious shortcomings may include, for example, repeated incidences of deviations from standard operations.

54	An appropriate procedure must be defined for the classification/categorisation (protection requirements category) and handling of the applications developed or run by the organisational unit's end users.	Compliance with coding standards must also be ensured for the applications developed by end users in the organisational units (e.g. EUC application). Each of these applications must be assigned to a protection requirements category. If the identified protection requirement exceeds the technical protection capability of these applications, protective measures must be taken contingent on the results of the protection requirements classification.
55	Rules must 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). The requirements set out in II. numbers 17 and 42 must also be applied for the use of applications developed by the organisational units themselves (end-user computing – EUC) in line with the criticality of the supported business processes and the importance of the application for those processes. The definition of measures to safeguard information security must be governed by the protection requirement of the data being processed.	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)

56 IT operations must fulfil the requirements resulting from the implementation of the business strategy, from the requirements of section 8.1 number 1 of KAMaRisk as well as from the IT-supported business processes (see section 4.3 number 17 and section 8.1 numbers 2 and 3 of KAMaRisk).

57 The components of the IT systems and their connections with each other must be administered in a suitable way, and the inventory data collected for this must 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.

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

59 The processes for changing IT systems must be designed and implemented depending on their nature, scale, complexity and riskiness. This also applies 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.

60	Change requests for IT systems must 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).
61	Reports of unscheduled deviations from standard operations (disruptions) and their causes must, 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, must 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, must be monitored and managed. The German asset manager must 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.
62	The provisions governing the data backup procedures (excluding long-term data archiving) must 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	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.

them must 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 must be tested regularly, at least once a year, as part of a sample as well as on an ad hoc basis.

8. Outsourcing and other external procurement of IT services

63 IT services encompass all forms of IT procurement; in particular, this includes the provision of IT systems, projects/computer-aided construction projects or staff. These also include IT services that are provided to the German asset manager by a services firm via a network (e.g. processing, storage, platforms or software) and that are supplied, used and invoiced, if applicable dynamically, and tailored to requirements via defined technical interfaces and protocols (cloud services). Outsourcing of IT services must meet the requirements set out in section 10 of KAMaRisk and BaFin's FAQs "Frequently asked questions about outsourcing under section 36 of the KAGB". The German asset manager must still comply with the general requirements relating to a proper business organisation under sections 28 to 30 of the KAGB in the case of other external procurement of IT services (see section 10 number 1 – Explanations – of KAMaRisk). For each software procurement, the associated risks must be appropriately assessed (see section 4.3 numbers 7, 9 and 15 of KAMaRisk).

64 Outsourcing is the commissioning of another undertaking to perform functions (outsourcing provider) that would otherwise be provided by the German asset manager itself.

A distinction is made between outsourcing IT services and other external procurement of IT services.

As a rule, isolated procurement of standard commercial software, i.e. software without any undertaking-specific modifications (including automatic updates and patches) and the related use of software providers for ad hoc support for the operation of these systems (see Recital 82 of Delegated Regulation EU 231/2013) is considered to be other external procurement. As a rule, the provision of staff to support the German asset manager is considered to be other external procurement if the activity is performed on the German asset manager's systems, in accordance with its instructions and subject to its control.

As a rule, the following activities are considered to constitute the outsourcing of IT services:

- adapting software to the German asset manager's requirements (parameterisation and customising);
- the technical development of programs and elements of programs and the implementation of modification requests (programming);
- testing, release and implementing software in the production processes the first time it is used and in the case of material changes, in particular of programming requirements;
- resolving errors in accordance with the description of requirements/errors of the client or manufacturer;
- other support services (such as the operation and maintenance of IT systems by third parties);

		to the extent that these are established to be performed for longer periods or have or could have a considerable or critical impact on portfolio management, risk management or other business-critical processes. In other respects, it is not possible to easily define rigid, pragmatic criteria to enable a distinction between outsourcing and other external procurement. When commissioning third parties, German asset managers are therefore required to make this distinction themselves, in particular taking into account the importance of the contract and the resulting risks to portfolio management, risk management and other business-critical processes. Additional information: BaFin's Guidance Notice "Guidance on outsourcing to cloud providers" should additionally be considered when outsourcing to cloud providers.
65	Given the fundamental importance of IT to the German asset manager, a risk assessment must also be performed prior to each instance of other external procurement of IT services.	The German asset manager can flexibly define the nature and scope of a risk assessment, taking account of proportionality aspects, in line with 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 German asset manager responsible for information security and contingency management are to be involved.
66	Other external procurement of IT services must be managed in line with the strategies, taking account of the German asset manager's risk assessment. The rendering of the service owed by the service provider must 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.
67	The contractual arrangements must take appropriate account of the measures derived from the risk assessment relating to other external procurement of IT services. Appropriate account must 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 German asset manager'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.
68	The risk assessments relating to other external procurement of IT services must be reviewed and amended regularly and on an ad hoc basis, together with the contractual details, where appropriate.	