BaFin Federal Financial Supervisory Authority

Circular 10/2018

Supervisory Requirements for IT in Insurance Undertakings
(Versicherungsaufsichtliche Anforderungen an die IT – VAIT)

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

Contents

I. Preliminary remarks

1 The use of information technology (IT) in the undertakings, including the use of IT services supplied by IT service providers, is key for insurance undertakings and Pensionsfonds. This Circular contains guidance on interpreting the requirements of the German Insurance Supervision Act (Versicherungsaufsichtsgesetz – VAG) on governance, to the extent that they relate to the technical and organisational resources of the undertakings. It establishes a binding interpretation of these requirements for BaFin and hence ensures consistent application to all undertakings and groups. The Circular provides a flexible and practical framework, in particular for managing IT resources, for information risk management and for information security management.

2 This Circular applies to all undertakings subject to supervision in accordance with section 1 (1) of the VAG, with the exception of special purpose insurance vehicles within the meaning of section 168 of the VAG and guarantee schemes within the meaning of section 223 of the VAG.

3 The Circular applies to groups if all primary insurers and reinsurers belonging to the group are situated in Germany. It also applies to groups with primary or reinsurance undertakings in other EU member states or EEA states in accordance with section 7 no. 22 of the VAG for which BaFin is the group supervisor under the criteria set out in section 279 (2) of the VAG. All undertakings subject to group supervision shall cooperate to ensure that the requirements are met at group level (section 246 (3) of the VAG). In particular the principles set out in section 275 of the VAG shall be observed. The term “undertaking” used in this Circular shall include groups.

4 For undertakings subject to Solvency II, this is without prejudice to the requirements contained in the Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings (MaGo), which are fleshed out in this Circular.

5 The depth and scope of the topics addressed in this Circular are not exhaustive. In accordance with the governance requirements set out in the VAG, the undertaking shall 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 2700X of the International Organization for Standardization.	
6	The principle of proportionality plays a major role in the implementation of the system of governance requirements and hence also in the design of structures, IT systems or processes. The requirements are to be fulfilled in a manner which is proportionate to the nature, scale and complexity of the risks inherent in an undertaking's business activities (referred to in the following as the "risk profile") (section 296 (1) of the VAG). The principle of proportionality is thus based on the individual risk profile of each undertaking. A smaller undertaking may indicate a lower risk profile, while the converse is also true. To the extent that the number of staff can play a role in determining the relevant size, it is not the number of existing staff that is crucial, but the actual requirement for staff. This primarily means that staff capacities which the undertaking benefits from via outsourcing must also be included in the evaluation..	
7	Proportionality affects how requirements can be met. For instance, simpler structures, IT systems or processes may be adequate in undertakings with a lower risk profile. Conversely, the principle of proportionality may require more sophisticated structures, IT systems or processes in undertakings with a more pronounced risk profile..	
8	The assessment of which form may be regarded as proportionate is not static with regard to the individual undertaking, but adjusts to the changing situation over time. In this respect, both undertakings and insurance groups have to examine whether and how the available structures and processes can, or indeed must, be further developed.	
9	The questions of which actual structures, IT systems or processes are appropriate to a particular risk profile, and whether (and if so, which) accompanying measures are required, can only be answered in the relevant context (taking into account criticality, among other factors).	
10	The individual risk profile determined by the undertaking continues to apply provided no changes have been made to it.	
11	All members of the management board are responsible for the proper and effective system of governance[1]. To the extent that the requirements of	

this Circular refer to the management board, this shall mean all members of the management board. They cannot delegate their overall responsibility in this respect, including to one or more members of the management board.	

II. Requirements

1. IT strategy

1 The management board shall define an IT strategy that is consistent with the business strategy, outlining the objectives and the measures to be taken to achieve those objectives. The management board shall review the IT strategy regularly and on an ad hoc basis and shall adapt it if necessary. The management board shall ensure that the IT strategy is implemented.

2 The degree of detail of the IT strategy depends on the undertaking's risk profile. The IT strategy shall contain as a minimum: a) strategic development of the undertaking's organisational and operational structure of IT, the outsourcing of IT services or other service relationships in the area of IT services, and the separate procurement of hardware and/or software (collectively also "IT procurement"); b) allocation to IT of the generally established standards that the undertaking applies; c) responsibilities and integration of information security into the organisation; d) strategic development of the IT architecture; e) statements on contingency management giving due consideration to IT issues; f) statements on IT systems developed and operated by the organisational units themselves.	Sponsoring undertakings of institutions for occupational retirement provision can also be IT service providers in this context. 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; Re b) Selection of generally established standards and application to the undertaking'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 undertaking and of how information security is embedded in the organisational units and in the collaboration model with each IT service provider; Re d) Description of target IT architecture. The outsourcing of IT services or other service relationships in the area of IT services shall be reflected appropriately in the IT strategy.

	The undertakings have the option to summarise the content of the IT strategy in a separate document or to integrate it as a sub-chapter into the business or risk strategy.
3 The targets defined in the IT strategy shall be formulated in such a way that a rational review of target achievement is possible.	
4 The IT strategy shall be made available to the undertaking's supervisory board, and discussed with it if appropriate, when it is initially adopted and in the event of any modifications.	The question of whether there is a need for discussion is a decision for the supervisory board.
5 The content of and any modifications to the IT strategy shall be communicated by suitable means within the undertaking.	

2. IT governance

6	IT governance within the meaning of this Circular 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, information risk management and information security management, the appropriateness of the quantity and quality of the undertaking's IT staffing, as well as the scope and quality of technical and organisational resources. Regulations governing the organisational and operational structure of IT shall be swiftly amended in the event of modifications to the activities and processes.	
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. These regulations shall be adopted in the undertaking in accordance with the risk profile. Processes and the related tasks, competencies, responsibilities, controls and reporting channels shall be defined clearly and coordinated. The management board shall ensure that the regulations governing the organisational and operational structure of IT are implemented effectively. This shall also apply to the interfaces with important outsourced elements.	The management board shall approve the regulations governing the organisational and operational structure of IT at least when they are initially adopted and in the event of more than minor modifications. If minor modifications are to be removed from the approval requirement, the undertaking shall define in advance which modifications are to be considered minor.
8	The processing and sharing of information in business and service processes is supported by data processing IT systems and related IT processes. Their scope and quality shall be governed by the risk profile.	
9	The undertaking shall ensure that appropriate staff, in terms of both quality and quantity, are available for information risk management, information security management, IT operations and application development in particular.	With regard to measures to ensure that the quality of staff remains appropriate, the undertaking shall in particular give consideration to technological advancements as well as the current and future development of the threat level.
10	All staff members shall at all times also have the necessary knowledge and experience in the field of IT, depending on their tasks, competencies and responsibilities.	Suitable measures shall ensure that the skills of the staff members are appropriate.

11 Any absence or departure of staff members may not lead to long-term disruption of operational workflows.	
12 Conflicts of interest shall be avoided within the organisational and operational structure of IT.	When designing the organisational and operational structure of IT, it shall be ensured that activities that are not compatible with each other are performed by different staff members. Conflicts of interest between activities connected, for example, with application development and tasks performed by IT operations can be countered by taking organisational or operational measures and/or by defining roles adequately.
13 The management board shall define appropriate quantitative or qualitative criteria for managing those areas responsible for operations and for the further development of IT systems, and compliance with them shall be monitored.	The following elements can be considered when defining such criteria: quality of performance, availability, maintainability, adaptability to new requirements, security of IT systems or the related IT processes, and cost.
14 The scope and quality of technical and organisational resources shall be governed by the risk profile.	
15 The IT systems and related IT processes shall ensure the integrity, availability, authenticity and confidentiality of the data. To achieve this, generally established standards shall be applied to the arrangement of the IT systems and the related IT processes; in particular, processes for appropriate assignment of access rights shall be established to ensure that all staff members only have the rights they need for their work; access rights may be combined into a role model. The suitability of the IT systems and the related IT processes for achieving the protection objectives shall be reviewed regularly by the staff members responsible for specialist and technical aspects.	
16 The undertaking shall 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 shall depend on the risk profile.	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 undertaking's staff. The specific nature of their description is a matter for the undertaking. The current version of the organisational policies shall be put into effect by the responsible decision-maker.

3. Information risk management

17 As part of its risk management process, the undertaking shall define and coordinate the tasks, competencies, responsibilities, controls and reporting channels required for the management of information risk. The undertaking shall set up appropriate identification, assessment, monitoring and steering processes and define the related reporting requirements.	
18 The identification, assessment, monitoring and steering processes shall comprise in particular the definition of IT risk criteria, the identification of IT risks, the determination of the level of protection required and protective measures for IT operations derived from it, and the definition of measures to manage the remaining residual risks.	
19 IT Risk management shall be implemented in line with the competencies of all relevant business units and functions involved and with no conflicts of interest.	The relevant business units involved also include the organisational units that own the information.
20 The undertaking shall have an up-to-date overview of the components of the defined information domain as well as any related dependencies and interfaces.	An information domain includes, for example, business-relevant information, business processes, IT systems as well as network and building infrastructures.
21 The method used to determine the level of protection required (in particular, with regard to the protection objectives of “integrity”, “availability”, “confidentiality” and “authenticity”) shall ensure that the resulting protection requirements are consistent and comprehensible.	Categories of protection requirements could be “low”, “medium”, “high” and “very high”.
22 The undertaking shall define and suitably document its requirements for implementing the protection objectives in the various categories of protection requirements (catalogue of target measures).	The catalogue of target measures contains only the requirements and not how these are to be met in practice.

23 A risk analysis shall be conducted on the basis of the defined risk criteria. Risk-reducing measures due to target measures that have not been implemented completely shall be effectively coordinated, documented, monitored and managed. The results of the risk analysis shall be approved and transferred to the process of operational risk management.	IT risk criteria contain, for example, potential threats, potential for damage, frequency of damage as well as risk appetite. Among other things, the risk analysis can be conducted by comparing the target measures and the measures that have been successfully implemented in each case.
24 The management board shall be informed regularly, but at least once a year, and ad hoc if appropriate, in particular about the results of the risk analysis in a written report. Within the year, the management board, or if appropriate the responsible member of the management board, shall be informed at least once a quarter in a status report.	The status report contains, for example, an evaluation of the risk situation compared to the last report.

4. Information security management

25 Information security management makes provisions for information security, defines corresponding processes and manages the implementation thereof. Information security management follows a continuous process that comprises a planning, an implementation, a performance monitoring and an optimisation phase.	
26 The management board shall agree a written information security policy and communicate this appropriately within the undertaking. The information security policy shall be in line with the undertaking'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 IT structure as well as to the undertaking'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.
27 Based on the information security policy, the undertaking shall define more specific, state-of-the-art information security guidelines and information security processes for the identification, protection, discovery, response and recovery sub-processes.	Information security guidelines are compiled, for example, for the network security, cryptography, authentication and logging areas.

	The primary aim of information security processes is to meet the agreed protection objectives. These include inter alia preventing and identifying information security incidents as well as responding to them appropriately and ensuring adequate communication in due course.
28 The undertaking shall establish an information security officer function. This supervising function comprises responsibility for all information security issues within the undertaking and with regard to third parties. It ensures that information security objectives and measures defined in the undertaking's IT strategy, information security policy and information security guidelines are transparent both within the undertaking and – to the extent necessary –for third parties, and that compliance with them is reviewed and monitored.	This supervising function can by performed by one or more natural persons, whereby one of those persons must hold responsibility for ensuring that the function performs its tasks properly. That responsibility may not be split over several natural persons. 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 undertaking'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; • suitable participation in projects relevant to IT (depending on the individual case, suitable participation can range from informing the information security officer about the IT project down to the active participation of the information security officer); • acting as a contact for any questions relating to information security coming from within the undertaking or from third parties; • examining information security incidents and reporting these to the management board (prior to this, the undertaking shall define suitable criteria for informing the management board about information security incidents); • initiating and coordinating measures to raise awareness of and training sessions on information security.

29 In terms of the organisational and operational structure, the information security officer' function shall be adequately independent in order to avoid any potential conflicts of interest.	Undertakings may combine the information security officer function with other internal functions if this is in line with the risk profile. The following measures, in particular, are observed to avoid any potential conflicts of interest: • a description of the information security officer's function and duties; • determination of resources required by the information security officer function; • a designated budget for information security training sessions within the undertaking and for the personal training of the information security officer; • the information security officer is able to report directly and at any time to the management board; • all staff members of the undertaking as well as IT service providers are required to report any incidents relevant to IT security that concern the undertaking immediately and in full to the information security officer; • the information security officer function shall be organisationally and operationally independent of those areas that are responsible for the operation and further development of IT systems; • the information security officer may not be involved in internal audit activities.
30 Each undertaking should have its own information security officer function in-house.	If the information security officer function is outsourced, the relevant applicable requirements for this shall be met. When deciding for or against outsourcing, the undertaking shall consider the extent to which IT-related business activities are managed internally in the undertaking or by external service providers. Building on this analysis, the question of how an appropriate exercise of the information security officer function can be ensured shall play a role.
31 After an information security incident, the impact on information security shall be analysed and appropriate follow-up measures approved.	The definition of "information security incident" in terms of nature and scope is based on the protection requirement for the business processes, IT systems and relevant IT processes in question. An event may also be deemed an information security incident if at least one of the protection objectives ("availability", "integrity", "confidentiality", "authenticity") as specified in the undertaking's target information security concept is violated in excess of the defined threshold. The definition of "information security incident" shall clearly

	differ from that of “deviation from standard operations” (in the sense of “disruption in daily operations”).
32 The information security officer shall report to the management board, or if appropriate to the responsible member of the management board, regularly, at least once a quarter, and on an ad hoc basis if necessary, on the status of information security.	The status report contains, for example, an evaluation of the information security situation compared to the last report, information about information security projects, information security incidents and the results of penetration tests.

5. User access management

33 The undertaking shall establish a user access management that ensures that access rights granted to users are in line with and used as defined in the undertaking’s organisational and operational requirements. The design of user access management shall take appropriate consideration of the requirements for process design (see II. numbers 7 and 15).	
34 In the user access management system, 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. In terms of assigning access rights to users, user access rights concepts shall ensure that all staff members only have the rights they need for their work; access rights may be combined into a role model. In addition, user access rights concepts shall ensure that the segregation of duties is observed and that staff conflicts of interest are avoided. In the case of IT-supported processing, the segregation of duties shall be ensured by corresponding procedures and protective measures.	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. Access rights: Access rights that have been set up may not conflict with the organisational assignment of staff members. In particular, when access rights are assigned in role models, it shall be ensured that the segregation of duties is preserved and that conflicts of interest are avoided.
35 It must be possible for non-personalised access rights to be unequivocally traced back to an active natural person at all times (wherever possible, automatically). Any departures from this in justifiable exceptional cases and the resultant risks shall be approved and documented.	

36 All technical users must be assigned to a responsible natural person.	
37 Approval and control processes shall ensure compliance with the requirements contained in the user access rights concept when setting up, changing, deactivating or deleting access rights for users. The responsible organisational unit shall be appropriately involved, thus enabling it to fulfil its organisational responsibilities.	Setting up, changing, deactivating or deleting access rights requires an access rights application to be implemented in the target system. Setting up and changing access rights requires the prior approval of the responsible organisational unit; it shall be informed promptly when access rights are deactivated or deleted.
38 Access rights shall be modified promptly if required. This shall also comprise the regular and ad hoc review, within appropriate time limits, of whether the access rights granted are still required and whether they comply with the requirements contained in the user access rights concept (recertification). The control bodies responsible for setting up, changing, deactivating or deleting access rights shall also be involved in recertification.	Significant access rights shall be reviewed at least once a year, and all other access rights at least once every three years. Especially critical access rights, for example for administrators, shall be reviewed at least once every six months. If during recertification it is discovered that access rights have been granted in breach of the prescribed procedure, these access rights shall be removed in line with the standard procedure for setting up, changing and deleting access rights.
39 The setting up, changing, deactivating and deleting of access rights and recertification shall be documented in a way that facilitates comprehension and analysis.	
40 The undertaking shall set up logging and monitoring processes consistent with the protection requirements and the target requirements that enable checks to be carried out to ensure that access rights are used only in the manner intended.	Overarching responsibility for the processes used to log and monitor access rights shall be assigned to a party that is independent of the authorised user in question and their organisational unit. Owing to the far-reaching intervention options of privileged users, the undertaking shall in particular set up appropriate processes to log and monitor their activities.
41 Accompanying technical and organisational measures shall be implemented to ensure that the requirements contained in the user access rights concepts cannot be circumvented.	Examples of such measures are: • a selection of appropriate authentication procedures; • implementation of a policy 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)

42 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 in advance as part of an impact analysis. In doing so, the undertaking shall analyse in particular the impact of the planned changes on the control methods and the intensity of controls. The organisational units integrated into the workflows shall be subsequently involved in these analyses. As part of their duties, the independent risk management function, the compliance function and the actuarial function shall also be involved, to the extent that the undertaking is required by law to establish the relevant function. The internal audit function may be involved in an advisory capacity. Sentences 1 to 5 shall also apply with regard to the initial use and material modifications of IT systems.	
43 The IT systems shall be tested before they go live and approved by the staff members with specialist and technical responsibility. To this end a standard process of development, testing, approval and implementation in the production processes shall be established. The production and testing environments shall generally be kept separate. These requirements shall generally also apply to material modifications of IT systems.	If modifications of IT systems are performed automatically by third parties and cannot be tested before they go live in the undertaking, the undertaking shall satisfy itself regularly that the necessary tests are conducted in advance at that third party.
44 The requirements set out in II. numbers 14, 15, 18 and 43 shall 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 shall be governed by the protection requirement of the data being processed.	This shall also apply to the first use and material modifications of IT systems.
45 Appropriate rules shall 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.

46 IT projects shall be managed appropriately, particularly taking account of 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 can depend on clear quality criteria set out in the relevant model procedure.
47 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.
48 Major IT projects and IT project risks shall be reported to the management board regularly and on an ad hoc basis. IT project risks shall be appropriately taken into account in risk management.	
49 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.	For example, application development includes the applications developed externally or internally in the undertaking (e.g. EUC). The processes shall be designed to reflect the risk profile.
50 Both requirements for the functionality of the application and non-functional requirements must be compiled, evaluated and documented appropriately. The organisational units shall be responsible for compiling and evaluating the requirements.	Examples of requirements documents in line with the chosen approach include: • Functional specifications (e.g. user story); • technical specifications (e.g. target specification document or product backlog). Examples of non-functional requirements for IT systems include: • results of the protection requirements analysis; • access rules; • ergonomics; • maintainability; • response times; • resilience.
51 In the context of application development, appropriate arrangements shall 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.
52 In the context of application development, arrangements shall be made to enable the identification of whether an application was unintentionally modified or deliberately manipulated.	A suitable arrangement, taking account of the protection requirement, may be reviewing the source code during application development. Source code review is a systematic examination in order to identify risks.
53 Both applications developed by third parties for the undertaking and applications developed in-house shall be documented in a clearly structured way and in a manner that is readily comprehensible for competent third parties.	The documentation of the application and its development shall as a minimum answer the following questions: • What is to be developed? • How was the application developed, in terms of both technology and process? • How does the application have to be run and deployed? The comprehensibility of the application development is aided by a version history of the source code and requirements documents, for example.
54 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 and the security controls. If system performance is important for an application, it shall also be tested under various relevant stress scenarios. The organisational unit responsible for the application shall be tasked with performing the technical acceptance tests. Test environments for performing the acceptance tests shall correspond to the production environment in aspects material to the test. Test activities and test results shall be documented.	This comprises relevant expertise as well as appropriately structured independence from the application developers. Test documentation contains the following points as a minimum: • test case description; • documentation of the parameterisation underlying the test case; • test data; • expected test result; • actual test result; • measures derived from the tests.
55 After the application goes live, any deviations from standard operations shall be appropriately monitored, their causes shall be investigated and, where appropriate, measures for subsequent improvement shall be taken.	Monitoring shall be increased temporarily after the application goes live. Indications of serious shortcomings may include, for example, repeated incidences of deviations from standard operations.
56 An appropriate procedure shall be defined for the classification/categorisation (protection requirements category) and handling of the applications	Compliance with coding standards will also be ensured for the applications developed by end users in the organisational units (e.g. EUC application). Each

developed or run by the organisational unit's end users.	of these applications will be assigned to a protection requirements category. If the identified protection requirement exceeds the technical protection capability of these applications, protective measures will be taken contingent on the results of the protection requirements classification.
57 Rules shall be defined on the identification of the applications developed or run by the organisational unit's end users, on documentation, on the coding guidelines and on the testing methodology for these applications, on the protection requirements analysis and on the recertification process for authorisations (e.g. in EUC guidelines).	To serve as an overview and in order to avoid redundancies, a central register of critical or material applications shall be maintained. As a minimum, the register shall generally document the applications that are used to identify, evaluate, monitor and manage the risks and to report on these risks, or that are important for performing other activities due to statutory requirements or activities that are necessary for operations. As a minimum, the following information will be collected: • 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)

58 IT operations shall fulfil the requirements resulting from the implementation of the business strategy as well as from the IT-supported business processes (see II. numbers 14 and 15).

59 The components of the IT systems and their connections with each other shall be administered in a suitable way, and the inventory data collected for this shall be updated regularly and on an ad hoc basis.	Inventory data include, in particular: • inventory and specified use of the IT system components with the relevant configuration data; • location of the IT system components; • list of the relevant information about warranties and other support agreements (including links where appropriate); • details of the expiry date of the support period for the IT system components; • accepted non-availability period of the IT systems as well as the maximum tolerable data loss.
60 The portfolio of IT systems shall be managed appropriately. This shall also take account of the risks stemming from outdated IT systems (lifecycle management).	
61 The processes for changing IT systems shall be designed and implemented depending on the risk profile. This shall also apply to newly procured or replaced IT systems as well as to security-related subsequent improvements (security patches).	Examples of changes include: • expanding functions of or rectifying errors in software components; • migrating data; • changing configuration settings of IT systems; • replacing hardware components (servers, routers etc.); • using new hardware components; • relocating IT systems.
62 Change requests for IT systems shall be accepted, documented, evaluated taking due account of potential implementation risks, prioritised and approved in an orderly way. The change shall be 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; • 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).
63 Reports of unscheduled deviations from standard operations (disruptions) and their causes shall, in a suitable way, be recorded, evaluated, prioritised with particular regard to potentially resulting risks, and escalated according to defined criteria. The processing, analysis of causes, and identification of solutions, including follow-up, shall be documented. An orderly process for the analysis of possible correlations between disruptions and of their causes must be in place. The processing status of outstanding reports of disruptions, as well as the appropriateness of the evaluation and prioritisation, shall be monitored and managed. The undertaking shall define suitable criteria for informing the management board about disruptions.	Risks can be identified by flagging the breach of protection objectives, for example. Causes are also analysed wherever multiple IT systems are used to record and process disruptions and their causes.
64 The provisions governing the data backup procedures (excluding data archiving) shall be set out in writing in a data backup strategy. The requirements contained in the data backup strategy for the availability, readability and timeliness of the customer and business data as well as for the IT systems required to process them shall be derived from the requirements for the business processes and from the business continuity plans. The procedures for recoverability in the required timeframe and for readability of data backups shall be tested regularly, at least once a year, as part of a sample as well as on an ad hoc basis.	The requirements for the structure and storage of data backups as well as for the tests to be performed stem from related risk analyses. With regard to the locations for the storage of data backups, one or multiple additional locations may be required.

8. Outsourcing of IT services and other service relationships in the area of IT services; separate procurement of hardware and/or software

65 In cases where IT services are outsourced – irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service – the relevant requirements for the service shall be met in each case; in particular, a risk analysis shall be performed in advance. This shall also apply

to the outsourcing of those IT services that are provided to the undertaking by a services firm via a network (e.g. processing, storage, platforms or software) and that are supplied, used and invoiced dynamically and tailored to requirements via defined technical interfaces and protocols (cloud services).	
66 The undertaking shall also perform a risk analysis in advance for any other service relationship in the area of IT services – irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service.	The undertaking can flexibly define the nature and scope of a risk analysis, taking account of proportionality aspects. Existing risk analyses can be used for equivalent other service relationships in the area of IT. The functions or persons of the undertaking responsible for information security and contingency management are to be involved in the risk analysis.
67 Other service relationships in the area of IT services shall be managed in line with the strategies, taking account of the undertaking's risk analysis. The rendering of the service owed by the service provider shall be monitored in line with the risk analysis.	A complete, structured contract overview will be maintained for this purpose. Outsourcing management can be performed by bundling contracts for other service relationships in the area of IT services on the basis of this contract overview (contract portfolio). Existing management mechanisms can be used for this purpose.
68 The contractual arrangements shall take appropriate account of the measures derived from the risk analysis relating to other service relationships in the area of IT services. Appropriate account shall be taken of the results of the risk analysis 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 undertaking'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.
69 The risk analyses relating to other service relationships in the area of IT services shall be performed again and the content of the contract modified, if necessary, if there are material changes in the risk profile.	

70 II. numbers 66 to 69 shall also apply to the separate procurement of hardware and/or software.	The separate procurement of hardware and/or software by the undertaking is not classified as outsourcing. Support services such as • modifying software to meet the undertaking's requirements, • the technical implementation of modification requests during the development process (programming), • testing, approving and implementing software in the production processes the first time it is used and in the case of material changes, in particular programming requirements, • rectifying errors in accordance with the client's or manufacturer's requirements/error description, • other support services over and above the provision solely of advice, are generally to be classified as outsourcing if they relate to software that is used to identify, evaluate, monitor and manage the risks and to report on these risks, or that is important for performing other activities due to statutory requirements or activities that are necessary for operations. The relevant applicable requirements for outsourcing shall also be applied to these support services.