Federal Financial Supervisory Authority

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

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

Supervisory Requirements for IT in Insurance Undertakings

Versicherungsaufsichtliche Anforderungen an die IT – VAIT in the version of 3 March 2022

This translation is furnished 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 Circulars 02/2017, “Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings (MaGo)”, 08/2020 "Minimum Requirements under Supervisory Law on the System of Governance of Institutions for Occupational Retirement Provision as well as 01/2020 “Minimum Requirements under Supervisory Law on the System of Governance of Small Insurance Undertakings under section 211 of the VAG (MaGo for small insurance undertakings)”, this is without prejudice to the requirements of the above Circulars, which are specified in this Circular.

5 In the case of outsourcing to IT service providers, undertakings shall also document appropriate arrangements in the outsourcing agreement to ensure compliance with the requirements of this Circular by the IT service provider. IT service providers within the meaning of this Circular can also be sponsoring undertakings of IORPs.

6 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 the international security standards ISO/IEC 2700XX of the International Organization for Standardization.

7 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)[1]. The principle of proportionality is thus based on the individual risk profile of each

[1] The requirements shall be implemented for institutions for occupational retirement provision (IORPs) in a way that reflects the nature, scale and complexity of their activities (see section 296 (1) sentence 2 of the VAG und paragraphs 12 *et seq*. of the Circular “Minimum requirements under supervisory law of the system of governance of institutions for occupational retirement provision (MaGo for IORPs]). Collectively, the criteria are termed a “profile”.

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.

8 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.

9 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.

10 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).

11 The individual risk profile determined by the undertaking continues to apply provided no changes have been made to it.

12 All members of the management board 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 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

1.1. 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 ensure that the IT strategy is implemented. The management board shall establish a process to monitor and measure implementation of the objective of the strategy, as well as of its assessment and amendment. This process shall be reviewed regularly and on an event-driven basis and shall be adapted if necessary.

1.2. The degree of detail of the IT strategy depends on the undertaking's risk profile. It shall contain as a minimum:

(a) strategic development of the undertaking's organisational and operational structure of IT, the outsourcing of IT services as well as other important dependencies on third parties, and the separate procurement of hardware and/or software (collectively also “ separate IT procurement”);
(b) allocation to IT and information security of the generally established standards that the undertaking applies;
(c) objectives, responsibilities and integration of information security into the organisation;
(d) strategic development of the IT architecture;
(e) statements on IT business continuity management giving due consideration to information security issues;
(f) statements on IT applications developed and operated by the organisational units themselves.

Re (a) Description of the role, positioning and philosophy of IT with regard to staffing and budget for the organisational and operational structure of IT as well as overview and strategic classification of IT services and potential other important dependencies on third parties (e.g. information, telecommunication and utility providers, etc.);

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. This shall also include fundamental statements about information security training and sensitisation;

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.

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

1.4. 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.

1.5. The content of and any modifications to the IT strategy shall be communicated promptly by suitable means within the undertaking.

2. IT governance

2.1. 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 resources (human, financial and other resources), as well as the scope and quality of technical and organisational resources. Policies governing the organisational and operational structure of IT shall be swiftly amended in the event of material modifications to the activities and processes.	
2.2. The management board is responsible for ensuring that the policies 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 policies 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 these policies are implemented effectively. This shall also apply to the interfaces with important outsourced elements.	The management board shall approve the policies governing the organisational and operational structure of IT at least when they are initially adopted and in the event of material modifications. The undertaking shall define in advance which modifications are to be considered material. The requirements relating to IT governance are a component of the regular reviews by internal auditors with sufficient IT-related qualifications.
2.3. 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.	
2.4. The undertaking shall ensure that appropriate resources, in terms of both quality and quantity, are available for information risk management, information security management, IT operations and application development in particular.	With regard to measures to ensure that the quality of resources (human, financial and other resources) remains appropriate, the undertaking shall in particular give consideration to technological advancements as well as the current and future threat level.
2.5. 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.
2.6. Any absence or departure of staff members may not lead to long-term disruption of operational workflows.	

2.7. 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.
2.8. The management board shall define appropriate quantitative or qualitative criteria for managing those areas responsible for operations and for the further development of IT systems. Compliance with these criteria 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.
2.9. The scope and quality of technical and organisational resources shall be governed by the risk profile.	
2.10. 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.	
2.11. 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

3.1. 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.	
3.2. 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 derived from it, and the definition of measures to manage the remaining residual risks.	The risk criteria take into account the criticality of the business processes and activities as well as known threats and incidents that have already affected the undertaking in the past.
3.3. 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 or the information risks.
3.4. 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 and support processes, IT systems and the related IT processes, as well as network and building infrastructures. Dependencies and interfaces also take account of the networking of the information domain with third parties.
3.5. The undertaking shall determine the protection requirements for the components of its defined information domain, in particular with regard to the protection objectives of "integrity", "availability", "confidentiality" and "authenticity", regularly and on an event-driven basis. The owners of the information or the organisational units that are responsible for the business processes shall be responsible for determining the protection requirements.	
3.6. The determination of the protection requirements and the related documentation shall be appropriately reviewed by information risk management.	

3.7. The undertaking shall define and suitably document requirements that are appropriate for achieving the relevant protection requirements (catalogue of target measures.	The catalogue of target measures contains only the requirements and not how these are to be met in practice.
3.8. The undertaking shall conduct a risk analysis on the basis of the defined risk criteria. The risk analysis shall be coordinated and documented. 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 transferred to the process of operational risk management. The handling of risks shall be approved in line with the competencies.	Risk criteria contain, for example, potential threats, potential for damage, frequency of damage as well as risk appetite. The risk analysis is conducted by comparing the target measures and the measures that have been successfully implemented in each case (target/actual comparison).
3.9. The undertaking shall keep itself informed about threats to and weaknesses in its information domain, examine their relevance, assess their impact and, if necessary, take appropriate technical and organisational measures.	Internal and external changes (e.g. to the threat level) shall be taken into consideration.
3.10. 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. The risk situation also includes external potential threats.

4. Information security management

4.1. 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.

4.2. The management board shall agree a written information security policy and communicate this within the undertaking. The information security policy shall be in line with the undertaking’s strategies. The policy shall be reviewed in the event of material changes in the overall conditions and modified promptly if required.

The information security policy defines the key aspects relating to the protection of confidentiality, integrity, availability and authenticity as well as the scope for information security. It also describes the material organisational aspects of information security management, as well as the most important roles and responsibilities in information security management. Among other things, the management board uses the policy to define:

- its overall responsibility for information security;
- the frequency and scope of information security reporting;
- the competences relating to the management of information risks;
- the fundamental information security requirements relating to staffing, contractors, processes, and technologies;
- suitable criteria for informing the management board about information security incidents, to the extent that these criteria are not documented in an information security policy.

Among other things, the overall conditions include internal changes to the organisational and operational structure or IT systems of the insurance undertaking as well as external changes (e.g. threat scenarios, technologies or legal requirements).

4.3. Based on the information security policy and the results of information risk management, the undertaking shall define more specific information security policies and information security processes that reflect the state of the art.

More specific information security policies are compiled, for example, for the areas of network security, cryptography, identity and access management, logging and physical security (e.g. perimeter and building security).

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

	The results of information risk management include amongst other things the defined target measures (see 3.7).
4.4. The undertaking shall introduce a more specific information security policy on testing and reviewing measures to protect information security and shall review it regularly and on an event-driven basis and modify it, if necessary. The necessary qualifications of the testers shall be ensured.	Among other things, the policy shall cover: ▪ the general threat level; ▪ the undertaking’s individual risk situation; ▪ categories of test and review subjects (e.g. the undertaking, IT systems, components); ▪ the nature, scope and frequency of tests and reviews; ▪ responsibilities and arrangements for avoiding conflicts of interest.
4.5. The management board 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 the more specific information security policies are transparent both within the undertaking and – to the extent necessary –for third parties, and that compliance with them is reviewed and monitored regularly and on an event-driven basis.	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 objectives (e.g. economic aspects versus information security); ▪ compiling more specific information security policies 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 information security issues; ▪ initiating and monitoring the implementation of information security measures; ▪ monitoring and working to ensure compliance with information security requirements in projects and procurement; ▪ 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; ▪ initiating and coordinating measures to raise awareness of and training sessions on information security.

	The information security officer may be supported by an information security management team.
4.6. In terms of the organisational and operational structure, the information security officer's 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 function and duties of the information security officer, his/her deputy and, if applicable, other units; ▪ 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 and his/her deputy and, if applicable, the information security management team.; ▪ 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 information security that concern the undertaking immediately and in full to the information security officer; ▪ the information security officer function shall be independent of those areas that are responsible for the operation and further development of IT systems; ▪ the information security officer may not be involved in internal audit activities.
4.7. 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.
4.8. After an information security incident, the impact on information security shall be analysed promptly and appropriate follow-up measures approved.	The definition of "information security incident" in terms of nature and scope is based on the protection requirement for the affected components of the information domain. An event may also be deemed an information security incident if at least one of the protection objectives ("availability", "integrity", "confidentiality", "authenticity") as specified in the

undertaking's target information security concept is violated. The definitions of "information security incident", "security-related event" (in the sense of operational information security) and "unplanned deviation from standard operations" (in the sense of a "disruption") shall differ from each other in a way that is clearly understandable.

4.9. The undertaking shall define a continuous and appropriate awareness and training programme for information security. The programme shall be reviewed regularly to ensure that it is up-to-date and appropriate.

As a minimum, the programme should take account of the following aspects, depending on the target group:

- personal responsibility for own actions and omissions as well as general responsibilities to protect information;
- fundamental information security procedures (such as reporting information security incidents) and generally applicable security measures (e.g. regarding passwords, social engineering, preventing malware and procedure if malware is suspected).

4.10. The information security officer shall report to the management board, or if appropriate to the responsible member of the management board, regularly, at least once a quarter, and on an event-driven 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. Operational information security

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

5.2. Based on the information security policy and on the more specific information security policies, the undertaking shall implement appropriate state-of-the-art operational information security measures and processes.

Among other things, information security measures and processes include:

- vulnerability management for identifying, assessing, managing and documenting vulnerabilities;
- networking segmentation and control (including compliance of terminal equipment with policies);
- secure configuration of IT systems (hardening);
- data encryption for data storage and transmission in line with the protection requirements;
- multilevel protection of IT systems in line with the protection requirements (e.g. against data loss, manipulation, denial-of-service attacks or against unauthorised access);
- perimeter protection, e.g. of properties, data centres and other sensitive areas.

5.3. Threats to the information domain shall be identified as early as possible. Potentially security-related information shall be evaluated suitably promptly, using a rule-based approach, and centrally. This information shall be protected during transport and storage and shall be held available for an appropriate period for subsequent evaluation.

Examples of potentially security-related information include log data, reports and disruptions that could indicate breaches of protection objectives.

As a general principle, the rule-based evaluation (e.g. using parameters, correlation of information, deviations or patterns) of large data volumes requires the use of automated IT systems.

	Subsequent evaluations include forensic analyses and internal improvement measures. The period should be appropriate to the threat level.
5.4. In the context of information security monitoring, an appropriate portfolio of rules for identifying security-related events shall be defined. Rules shall be tested before being put into operation. The rules shall be reviewed regularly and on an event-driven basis for effectiveness and updated.	Rules identify, for example, whether there have been increased cases of unauthorised access attempts, whether expected log data is no longer delivered or if the times of the delivering IT systems differ. The rules must be suitable for identifying anomalous activities and threats.
5.5. Security-related events shall be analysed promptly and information security management shall be responsible for responding appropriately to any resulting information security incidents.	Security-related events result, for example, from the rule-based evaluation of potentially security-related information.
5.6. The security of the IT systems shall be reviewed regularly, on an event-driven basis while avoiding any conflicts of interest. Results shall be analysed to establish any necessary improvements and risks shall be managed appropriately. Critical systems shall be reviewed at least once a year.	The frequency, nature and scope of the review should be based in particular on the protection requirements and the potential vulnerability of the IT system (e.g. extent to which it can be reached from the internet). Examples of types of reviews include: ▪ gap analysis; ▪ vulnerability scans; ▪ penetration tests; ▪ simulated attacks.

6. Identity and access management

6.1. The undertaking shall establish identity and 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 identity and access management shall take appropriate consideration of the requirements for process design (see 2.2 and 2.10). All forms of access rights to components of the information domain shall be subject to standardised processes and controls.

6.2. User access rights concepts define the scope and the conditions of use for access rights to IT systems (access to IT systems and access to data) and the access rights to premises in a manner that is consistently in line with the determined protection requirements and can be completely and comprehensibly derived for all access rights provided. User access rights concepts shall ensure that users are assigned access rights in line with the need-to-know and least-privilege principles; access rights may be combined into a role model. In addition, user access rights concepts shall ensure that the segregation of duties is observed, including across the user access rights concepts, and that 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. User access rights concepts shall be reviewed regularly and on an event-driven basis and updated if necessary.

One possible condition for use is limiting the time for which access rights are granted. Depending on the type, access rights can be granted for personalised and for non-personalised users (including technical users). Examples of technical users are users who are used by IT systems in order to identify themselves to other IT systems or to perform IT routines autonomously.

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.

Access rights to the IT systems may be present at all levels of an IT system (e.g. operating system, database, application).

Under the need-to-know principle, the access rights of each individual technical user shall be restricted to the absolute minimum necessary and user accounts no longer required shall be deleted.

6.3. It must be possible for access rights to be unequivocally traced back to an active or responsible person at all times (wherever possible, automatically).

For example, automated activities must be capable of being allocated to responsible persons. Any deviation from this in justifiable exceptional cases and the resultant risks shall be assessed, documented and subsequently approved by the responsible organisational unit.

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

Setting up, changing, deactivating or deleting access rights also requires timely or immediate implementation in the target system. Reasons for immediate deactivation or deletion or access rights include the risk of abuse (e.g. if an employee is terminated without notice).

	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.
6.5. 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.	Material 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 that unauthorised access rights , have been granted, they shall be removed in line with the standard procedure and other measures shall be taken if necessary (e.g. cause analysis, incident report).
6.6. The setting up, changing, deactivating and deleting of access rights and recertification shall be documented in a way that facilitates comprehension and analysis.	
6.7. The 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. Owing to the associated far-reaching intervention options, the undertaking shall in particular set up appropriate processes to log and monitor the activities with privileged (particularly critical) user and access rights.	Overarching responsibility for the processes used to log and monitor access rights shall be assigned to a party that is independent of the authorised user in question and their organisational unit. As a rule, privileged access rights include the rights to access data centres, technology rooms and other sensitive areas.
6.8. Accompanying technical and organisational measures shall be implemented to ensure that the requirements contained in the user access rights concepts cannot be circumvented.	Examples of such measures are: ▪ a selection of appropriate authentication procedures (including strong authentication in the event of remote access); ▪ implementation of a policy on choosing secure passwords; ▪ automatic screen lock with password protection; ▪ data encryption; ▪ tamper-proof implementation of logging; ▪ measures to raise staff awareness.

7. IT projects and application development

7.1. Material modifications to the IT systems in the course of IT projects, their impact on the organisational and operational structure of IT and on the related IT processes shall be evaluated in advance as part of an 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.

7.2. 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 environment shall generally be kept separate from development and testing environments. 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.

7.3. The requirements set out in chapters 2.9, 2.10, 3.2 and 7.2 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 applications.

7.4. Appropriate rules shall be defined for the organisational framework of IT projects 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.
- The organisational framework includes:
- involvement of affected parties (in particular the information security officer);
- project documentation (e.g. project application, project final report);
- provision of quantitative and qualitative resources;
- management of project risks;

	▪ information security requirements; ▪ quality control measures not related to the project; ▪ lessons learned.
7.5. IT projects shall be managed appropriately, taking account of their objectives and risks in relation to duration use of resources and quality. If major changes to processes that impact information security are required in the course of IT projects, the corresponding change requests must be submitted and processed. To this end, model procedures shall be defined and compliance with them shall be monitored.	For example, the decision to transition between project phases or sections can depend on clear quality criteria set out in the relevant model procedure.
7.6. The portfolio of IT projects shall be monitored and managed appropriately. Due account shall be taken of the fact that risks can also stem from interdependencies between different projects.	The portfolio view facilitates an overview of the IT projects together with the relevant project data, resources, risks and dependencies.
7.7. Major IT projects and IT project risks shall be reported to the management board regularly and on an event-driven basis. IT project risks shall be appropriately taken into account in risk management.	
7.8. Appropriate processes shall be defined for application development which contain specifications for identifying requirements, for the development objective, for (technical) implementation (including coding guidelines), for quality assurance, and for testing, approval and release.	Application development includes, among other things, the development of software, for business and support processes (including end-user computing – EUC). The processes are designed to reflect the risk profile.
7.9. Both requirements for the functionality of the application and non-functional requirements must be compiled, evaluated and documented. Appropriate acceptance and test criteria shall be defined for each requirement. Responsibility for compiling and evaluating the requirements (functional and non-functional) lies within the responsible organisational units.	Requirements documents may differ depending on the procedure model and may include, for example: ▪ functional specifications (requirements specification); ▪ technical specifications (target specification document); ▪ user story/product backlog. Examples of non-functional requirements for IT systems include: ▪ information security requirements;

- access rules;
- ergonomics;
- maintainability;
- response times;
- resilience.

7.10. In the context of application development, appropriate arrangements shall be made, depending on the protection requirement, to ensure that the confidentiality, integrity, availability and authenticity of the data to be processed are also comprehensibly assured during productive operations.

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.

7.11. The integrity of the application (especially the source code) shall be appropriately safeguarded. In addition, arrangements shall be made to enable the identification of whether an application was unintentionally modified or deliberately manipulated, among other things.

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

7.12. 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 an application includes the following content as a minimum:

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

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

7.13. 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 measures implemented to protect information. If system performance is important for an application, it shall also be tested

Performing the test requires relevant expertise on the part of the persons responsible for the test as well as appropriately structured independence from the application developers. The protection requirements of the data used for the test shall be taken into account.

under various relevant stress scenarios. The responsible organisational unit shall be responsible for performing 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.	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. If required to protect information, penetration tests shall be included in the test activities.
7.14. After an 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.
7.15. An appropriate procedure shall be defined for the classification/categorisation (protection requirements category) and handling of the applications developed or run (EUC) by the organisational unit's staff.	Compliance with coding guidelines will also be ensured for EUC applications. Each application will be assigned to a protection requirements category. If the identified protection requirement exceeds the technical protection capability of an application, protective measures will be taken contingent on the results of the protection requirements classification.
7.16. Rules shall be defined on the identification of the applications developed or run by the organisational unit's staff, 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.

8. IT operations

8.1. IT operations shall fulfil the requirements resulting from the implementation of the business strategy as well as from the IT-supported business processes (see chapters 2.9 and 2.10).

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

Inventory data include, in particular:

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

8.3. The portfolio of IT systems shall be managed. IT systems should be regularly updated. Risks stemming from outdated IT systems or systems no longer supported by the vendor shall be managed (lifecycle management). Hardware components no longer used shall be disposed of securely.

Hardware components include in particular data carriers.

8.4. 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).

Changes to IT systems also include the maintenance of IT systems. Examples of changes include:

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

8.5. Changes to IT systems and major process changes that impact information security shall be requested for. The requests 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. Appropriate processes shall also be established for time-critical changes to IT systems.

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

- risk analysis relating to the existing IT systems (particularly including the network and the upstream and downstream IT systems), including in respect of possible security or compatibility problems, as a component of the change request;
- testing of changes prior to going live for possible incompatibilities of the changes as well as possible security-critical aspects for existing IT systems;
- testing of patches prior to going live taking account of their criticality;
- data backups for the IT systems concerned;
- reversal plans to enable an earlier version of the IT system to be restored if a problem occurs during or after going live;
- alternative recovery options to allow the failure of primary reversal plans to be countered.

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

8.6. Reports of unscheduled deviations from standard operations (disruptions) and their causes shall, in a suitable way, be recorded, evaluated, prioritised with particular regard to potentially resulting risks, and escalated according to defined criteria. To this end, standard procedures shall be defined, e.g. for measures and communication as well as responsibilities (e.g. for malicious code on end-user devices, malfunctions). The processing, analysis of causes, and identification of solutions, including follow-up, shall be documented. An orderly process for the analysis of possible correlations between disruptions and of their causes 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 those involved (e.g. the management board, competent supervisory authority) 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.

8.7. The provisions governing the data backup procedures (excluding data archiving) shall be set out in writing in a data backup strategy. The requirements contained in the data backup strategy for the availability, readability and timeliness of the customer

The requirements for the measures for safeguarding data availability, readability and timeliness as well as for the tests to be performed stem from related risk analyses. With

and business data as well as for the IT systems required to process them shall be derived from the requirements for the business processes and from the business continuity plans. The procedures for recovery and safeguarding the readability of data shall be tested regularly, at least once a year, as part of a sample as well as on an event-driven basis.	regard to the locations for the storage of data backups, one or multiple additional locations may be required.
8.8. The current performance and capacity requirements of the IT systems shall be captured. The future performance and capacity requirements shall be estimated. Performance delivery shall be planned and monitored, in particular in order to identify bottlenecks promptly and to respond to them appropriately. The performance and capacity requirements of information security measures shall be taken into account in the planning.	

9. Outsourcing of IT services and other service relationships in the area of IT services

9.1. 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).

9.2. The undertaking shall also perform an analysis and assessment of the requirements and 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.

9.3. 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.

9.4. 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, for contingency management and IT operations, which normally correspond to the undertaking’s objectives (e.g. information security policy and more specific information security policies).

Where relevant, the possibility of the outage of an IT service provider is also taken into account and a related exit or alternative strategy developed and documented.

Measures found to be necessary are also taken into account in cases where subcontractors of the IT service provider are involved.

9.5. The risk 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.

9.6. Chapters 9.2 to 9.5 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.

10. IT business continuity management

10.1. IT business continuity management increases the resilience of areas and processes in the undertaking in order to ensure the continuation of business activities in possible emergency situations through procedures defined in advance. A business impact analysis is used to identify time-critical activities and processes. Activities and processes are generally time-critical if their impairment for defined periods is expected to lead to damage to the undertaking that can no longer be considered acceptable. IT business continuity plans are prepared for the IT systems that support these time-critical activities and processes as part of an IT business continuity concept taking into account the business impact analysis and a risk analysis. These documents record how, in the event of an emergency, normal operation can be restored and time-critical processes can be re-established. As part of IT business continuity management, care must be taken to ensure close coordination with the service providers in the event of outsourcing (taking into account any sub-outsourcing). IT business continuity management is part of general business continuity management.

10.2. The management board is responsible for preparing an IT business continuity concept as part of the IT business continuity management. The measures defined in the business continuity concept shall be suitable for reducing the extent of potential losses. The IT business continuity concept shall be updated on an event-driven basis, reviewed regularly for timeliness and communicated appropriately.

The IT business continuity concept sets out the responsibilities, objectives and measures for continuing or restoring time-critical activities and processes. It also includes organisational aspects such as interfaces to other areas (including risk management or information security management).

The IT business continuity concept considers the following scenarios at a minimum:

- (partial) site failure (e.g. due to flooding, major fire, closures of specific areas, access control failure),
- significant failures of system or communications infrastructure (e.g. due to errors or cyberattacks),
- critical staff shortfall (e.g. in the case of a pandemic, food poisoning or strikes),
- failure or unavailability of service providers (e.g. suppliers, electricity suppliers).

10.3. The undertaking shall use business impact analyses to identify time-critical processes as well as their supporting IT processes, systems, resources and other necessary technical infrastructure.

Business impact analyses examine the potential consequences of impairments of activities and processes for business operations over graduated periods. The business impact analyses should take due account of the following aspects, among other things:

- nature and scale of the (non-)material losses,
- impact of time of the failure on the losses.

10.4. The undertaking shall perform a risk impact analysis for the identified IT processes, systems, resources and other necessary technical infrastructure. The risk impact analysis identifies and evaluates potential hazards that could lead to the impairment of time-critical business processes.

The results of the business impact analysis in conjunction with the risk impact analysis enable the development of suitable measures to ensure the continuity of IT processes, systems, resources and other necessary technical infrastructure. The measures shall serve either to mitigate risk or recover processes.

10.5. Taking into account the business impact and risk impact analyses for IT systems that support time-critical activities and processes, the undertaking shall prepare IT business continuity plans. The individual risk profile shall be taken into account. The IT business continuity plans shall be communicated appropriately and must also be accessible in an in the event of an emergency. The IT business continuity plans and associated documents shall be updated regularly and as on an event-driven basis.

IT business continuity plans include restart, emergency operation and recovery plans as well as the parameters and responsibilities defined for these, and take account of dependencies in order to restore time-critical activities and processes. Furthermore, they also contain the conditions that lead to activation of the IT business continuity plans and all necessary information for ensuring effective communication (taking relevant service providers into account) in the event of an emergency.

The protection objectives (see chapter 3.5) must be adequately taken into account. If the recovery of normal operations is not possible in the short term (e.g. pandemic), other options are also included.

Among other things, parameters include:

- recovery time objective (RTO):
- recovery point objective (RPO);
- emergency operation configuration.

Among other things, dependencies include:

- dependencies of upstream and downstream business processes and the IT systems deployed by the undertaking and (IT) service providers;
- dependencies in the recovery prioritisation of IT processes and systems;
- necessary resources for ensuring (limited) continuation of business processes;
- dependencies on external factors (driven by the legislature, shareholders, the public, etc.).

10.6. The effectiveness of the IT business continuity plans shall be verified by IT contingency tests performed regularly and on an event-driven basis. The tests shall cover all IT systems that support time-critical activities and processes. Dependencies between IT systems or of jointly used IT systems shall be adequately taken into account. A testing concept shall be prepared for this purpose. The test results shall be documented in writing. The resulting defects shall be analysed and reported to the management board.	As a minimum, the testing concept contains both tests of individual IT systems (e.g. components, individual applications) and their combination into integrated networks.
10.7. The undertaking is required to demonstrate that, if a data centre fails, the time-critical activities and processes can be provided from a sufficiently remote data centre and for an adequate time, as well as for the subsequent restoration of normal IT operation.	

11. Critical infrastructure

11.1. Against the backdrop of the other chapters of the VAIT and the other relevant supervisory requirements for insurance undertakings concerned with ensuring that appropriate precautions are taken to guarantee the availability, integrity, authenticity and confidentiality of information processing, this chapter is directed specifically at operators of critical infrastructure (CI operators[2]).

It adds requirements for the effective implementation of special measures to achieve the critical infrastructure protection (CIP) objective to the Supervisory Requirements for IT in Insurance Undertakings. The CIP objective shall be understood as maintaining society's security of supply for the critical insurance services named in section 7 of the BSI-KritisV, because the failure or impairment of these services could lead to serious supply disruptions or threats to public security.

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

Companies can choose to use this chapter to provide verification under section 8a (3) of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* – BSI Act) via security audits or inspections (within the context of the audit of the annual financial statements, for example). This requires that the requirements of the VAIT are implemented and covered by the audit in full for all information technology systems, components and processes that are part of the critical infrastructure. The verification under section 8a (3) of the BSI Act shall be produced in consultation with a suitable auditing body (see relevant FAQs on the website of the Federal Office for Information Security (BSI)).

Alternatively, to provide the verification under section 8a (3) of the BSI Act, CI operators can adopt a company-specific approach taking into account other appropriate requirements or create an industry-specific security standard (B3S) under section 8a (2) of the BSI Act.

11.2. The facilities as defined in the BSI-KritisV must be fully included in the scope of the provision of verification for critical infrastructure. This shall be clearly tagged within the information domain. Thereby all relevant interfaces should be included.

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

For example, this can be achieved by tagging the components and areas of the information domain that are part of the critical infrastructure within the inventory according to chapter 8.2 of the VAIT (e.g. in a configuration management database – CMDB). This should include information on the relationship with the respective facility classes of the CI operator that are to be audited.

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

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

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

11.3. The information risk management and information security management under chapters 3 and 4 of the VAIT shall take the CIP objective into account and adopt measures to ensure that it is achieved. In particular, risks that have the potential to impair critical services to a significant degree shall be reduced using appropriate measures for risk mitigation and risk avoidance to a level appropriate for the CIP objective.

Measures which are able to counter the risks to availability when the need for protection is high or very high are particularly suitable for this.

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

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

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

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

- The CIP objective shall also be taken into account when services are outsourced under section 7 no. 2 and section 32 of the Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG) in conjunction with chapter 8 of the VAIT.
- The emergency preparedness planning shall include measures to allow critical services to be maintained even in an emergency situation.

11.5. The verification under section 8a (3) of the BSI Act regarding compliance with the requirements under section 8a (1) of the BSI Act can be conducted via security audits or inspections (as part of the audit of the annual financial statements, for example).

CI operators are to submit the relevant verification documents to the BSI on time, in accordance with the relevant requirements of the BSI.

There are other permissible ways to provide verification aside from security audits or inspections (for example as part of the annual financial statements) on the basis of the VAIT. In this regard, CI operators should take note of the current version of the "Orientation Guide to Verification According to § 8a (3) BSI Act".

CI operators are to provide verification to the BSI regarding compliance with the requirements under section 8a (1) of the BSI Act for the first time by 30 June 2019 at the latest and at least every two years thereafter.