FMA

Document Number: 02 / 2018
Publication Date: 03.07.2018

FMA GUIDE

IT Security
in insurance and reinsurance undertakings

July 2018

TABLE OF CONTENTS

AIMS AND NOTES

The advance in digitalisation, while presenting many advantages for business life, also exposes companies, including insurance and reinsurance undertakings (hereinafter: (R)IUs) to new hazards and risks. Consequently the risk situation has also become more marked for (R)IUs, who (are having to) become increasingly reliant on digitalisation.

The Austrian Financial Market Authority (FMA) is aware of the ever growing opportunities and risks that emerge from information technology (IT), and therefore considers itself duty-bound to conduct more intensive IT supervision as a result of the heightened risk situation. For this reason the FMA provides (R)IUs with this guidance that contains an overview about the design, requirements and provisions regarding IT security in (R)IUs.

This guide does not constitute a legal regulation. It is intended to provide supervised undertakings with know-how and to promote the development of a common understanding. No rights and obligations extending over and above the provisions of the law can be derived from this guideline.

This guide is addressed to all insurance undertakings (Article 5 no. 1 VAG 2016), reinsurance undertakings (Article 5 no. 2 VAG 2016) as well as the branch establishments of a third-country insurance undertaking or third-country reinsurance undertaking (Article 5 no. 18 VAG 2016) and shall apply accordingly at consolidated level (Article 222 para. 1 VAG 2016).

The explanations contained in this guide are to be viewed in accordance with the principle of proportionality. The application in accordance with this principle is commensurate to the nature, scope and complexity of the risks associated with the activities of the (R)IU. In so doing, the respective (R)IU itself determines which methods, systems and processes are appropriate in relation to IT security. The legal basis remains unaffected by this guideline.

I. LEGAL BASES

This guide is based in particular on Article 110 para. 2 no. 5 VAG 2016 (risk management of operational risks) and Article 111 para. 1 no. 1 VAG 2016 (overall solvency needs) in conjunction with the EIOPA Guidelines on Systems of Governance, EIOPA-BoS-14/253 as well as the EIOPA Guidelines on own risk and solvency assessment, EIOPA-BoS-14/259. In any implementation for addressing IT risks it is recommended to refer to any established standards that exist. Such standards include:

- **ISO 27001:**[1] The ISO 2700X series is a series of IT security standards. ISO 27001, for example, was drawn up for establishing, implementing, maintaining and ongoing improvement of an information security management system (ISMS).
- **Austrian Information Security Handbook (Österreichisches Informationssicherheitshandbuch):**[2] The Handbook describes and supports the approach to establish a comprehensive information security management system (ISMS) within companies and public authorities. The handbook is suitable for example as an implementation aid for ISO 27001-compliant implementation.
- **ITIL:**[3] The IT Infrastructure Library (ITIL) is an established quality standard, covering pre-defined processes, functions and roles for corporate IT infrastructures (a collection of best practices for service management).
- **COBIT:**[4] The Control Objectives for Information and related Technology (COBIT) framework allows the management to govern and manage IT operations. COBIT was formed from a collection of IT standards, frameworks, policy guides and best practices.
- **BSI-Grundschutz**:[5] BSI-Grundschutz is a collection of documents by the German Federal Office for Information Security (BSI), that are intended for the detection and reaction of security-related weaknesses in IT environments.

II. DEFINITIONS

For the purpose of this guide, the following relevant definitions in relation to IT security are explained below. Otherwise the definitions contained in the ISO standards are generally used.

- **Information Technology (IT):** IT covers all technical means that are used for the processing or transmission of information. The processing of information consists of the collection, capturing, usage, saving, submitting, program-based processing, internal presentation and outputting of information.

[1] https://www.iso.org/standard/54534.html.
[2] https://www.sicherheitshandbuch.gv.at.
[3] See e.g. https://www.etc.at/itil/ or https://www.axelos.com/best-practice-solutions/itil.
[4] https://www.isaca.org/cobit/pages/default.aspx.
[5] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html.

- **IT risk:**[6] This is the existing or future risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability, integrity, accessibility and security of such infrastructures and of data. The risk may emanate from IT availability and continuity, IT security, IT modifications, IT data integrity and IT outsourcings.

III. GOVERNANCE

A. THE ROLE OF THE MANAGEMENT BOARD

The management board[7] should ensure compliance with the applicable regulations for the provision of contractual insurance and recognised principles for the orderly pursuit of business pursuant to Article 106 VAG 2016, with regard to IT security, in particular:

- being responsible for the defining, reviewing and as necessary adaptation of the IT strategy,
- being responsible for the defining, implementation and as required the timely adaption of the IT structure and procedures,
- determining criteria for IT controlling (for example with regard to availability, the ability of IT to adapt to new requirements, and general quality),
- deciding upon written IT risk management guidelines (as part of the overall risk management guidelines) and standards on information security,
- ensuring the coherence of strategies and procedures in relation to IT risk with the organisation's strategic objectives.

B. IT STRATEGY

IT strategy and business strategy are coordinated with one another. IT strategy includes:

- the strategic development of IT structures and IT procedures, in particular with regard to the allocation of staff and budget,
- an overview about the planned application environment,
- the defining of standards, towards which the (R)IU is oriented, including a presentation of the current and planned level of implementation,
- the general organisational approach for information security into account in the company,
- a basic strategy about IT emergency management,
- a positioning about the permissibility of and the requirements in the relation to the local deployment of specific IT systems (hardware and software components) in the individual organisational units,

[6] The synonymous terms "IT risk", "information and communication technology (ICT) risk" or "information systems risk" all address the same risk.
[7] For the purposes of this Guide "management board" also includes the administrative board (Cf. Article 1(43) L2-R (EU) 2015/35 in conjunction with Article 106 VAG 2016).

- principles for lifecycle management for hardware and software.

The IT strategy must be adapted to changes in the strategic objectives, business activities, operating environment or the risk situation of the (R)IU within an appropriate time frame. The risk awareness of employees with regard to IT risk should be promoted throughout the entire company.

C. IT GOVERNANCE

IT governance based on the IT strategy guarantees the orderly pursuit of business as well as where required the necessary adaptations to IT systems and processes. The **technical/organisational infrastructure** is adequate and corresponds to the criteria based on the IT strategy prescribed by the management board. The (R)IU has sufficient staffing resources, both in terms of their quantity and quality, with regard to IT-specific requirements.

Conflicts of interest within the operational and organisational IT structure should be avoided or should be adequately addressed. Clearly delineated roles and responsibilities should be defined regarding the identification, evaluation, monitoring, minimising, reporting and oversight of the material IT risks.

IT governance is subject to regular internal audit inspections.

The provisions of Article 109 VAG 2016 are to be observed in the case of IT services being outsourced.

IV. CONTROLLING

A. RISK MANAGEMENT OF IT RISKS

IT risks are addressed within the risk management framework for operational risks or the assessment of the overall solvency needs. Risks relating to the processing, onward transmission and storage of information that are supported by adequate IT systems and processes should be covered. The risk management of IT risks is facilitated by means of an overview about the information network that covers, for example, information, IT systems, network and building infrastructures as well as interfaces.

The assessment of the overall solvency needs relating to IT risks consists of the following procedural steps:

- **Risk identification**: potential causes of IT risks are:
  - inadequate safeguarding of interfaces to the Internet,
  - insufficient measures for the promotion of risk awareness among employees,
  - outsourcings,
  - material changes/migrations of the IT system, IT processes or IT functions.

Identified IT risks should be described and systematically presented as part of the classification of risks. The necessary level of detail depends on company-specific circumstances.

- The **risk assessment** that is determined on the basis of the probability of occurrence of the risk and the extent of the damage forms the basis for the **risk review**, which, for example, may be depicted by means of a risk matrix. For example, cyber risks are addressed by conducting penetration tests (exploiting of software weaknesses and security vulnerabilities in the IT infrastructure, to receive unauthorised access to this infrastructure).
- To ensure adequate **risk controlling** the (R)IU should have a methodology in place for identifying the need for protection of components in the information network. There should be a specific focus on the objectives of protection of integrity, availability, confidentiality and authenticity of information. Findings in relation to emergency management are also taken into consideration. Catalogues of measures for risk mitigation are determined and implemented depending on the security requirements category.

  Possible measures are:

  - the wholescale replacement of manual interfaces by automated ones,
  - the logging of user and administrator activities,
  - Password standards e.g. regarding the length and form of passwords to ensure the necessary level of safety where username/password procedures are used.
  - Switchover to a replacement server in the event of the management server failing.

  Transparent presentation of the IT residual risk consciously taken on by the R(IU).
- **Risk reports** also contain statements about the risk management of IT risks.

B. INFORMATION SECURITY MANAGEMENT

Processes are established and their implementation managed to protect information. Information security in particular refers to the following aspects:

- integrity, i.e. information is only allowed to be modified by the persons and processes prescribed to do so,
- confidentiality, i.e. information is only allowed to be made available to the prescribed persons and processes,
- availability, i.e. information must be made available for the prescribed persons and processes, where they require this information.

The specific objectives and scope of information security management should be defined. The security requirement should be specified further within the framework on the management of IT risks. The **security measures** taken for achieving information security objectives in particular include technical precautionary measures and organisational procedures and processes. Potential examples are:

- training courses on information security,

- data backups and regular checks that data backup procedures are fully functional (backup and restore),
- centralised and decentralised antivirus scans,
- intrusion detection/prevention systems (e.g. checking of log data for evidence of cyber attacks, continuous checking of firewall concepts using internal or external testing methods, e.g. port scans),
- systematic patch management,
- evaluation of security measures in particular in relation to new technologies (e.g. regarding the using of cloud services, as well as in relation to new types of cyber attacks).

Once security incidents have occurred their effects on information security should be analysed and appropriate follow-up measures taken. Due to the constantly increasing significance of IT and the increasingly interconnected nature of information, particular significance is placed upon the organisation of information security management as a **continuous improvement process**. The requirement to name an information security officer, who is responsible for all information security matters within the (R)IU and towards third parties, should be reviewed and should be established on the basis of the findings of the evaluation. In this case roles and responsibilities should be clearly distributed and conflicts of interest addressed and in particular the continuous information and advising of the management board guaranteed.

C. IT EMERGENCY MANAGEMENT

IT risks are closely associated to the risk of business interruption. The purpose of IT emergency management (Business Continuity Management) is to take appropriate precautions to guarantee the continuity and the orderly nature of the performance of the IT-supported activities of the (R)IU. Emergency management generally ensures in the case of an unforeseen disruption to systems and procedures that significant data and functions remain intact and insurance and reinsurance activities are maintained or, where this is not possible, that the data and functions in question are restored promptly and contractual insurance operations are resumed quickly. Appropriate emergency management increases the resilience of the business processes of the company and the continuity of insurance and reinsurance activities, and therefore also protects the interests of the insured persons in relation to the continuous provision of services.

A coordinating committee should be established for implementing emergency management, consisting of members of various organisational units (**emergency team**).

The **phases** of emergency management:

- **Development**
  - Time-critical business processes, their dependencies and the required IT resources should be identified within the **Business Impact Analysis**, to be able to ensure that that they are safeguarded against accordingly. The effects of resource-based issues (in any case in relation to IT systems, data, staffing and contractual parties) or business process failures are to be estimated. A classification as "critical" in relation to the achieving of the (primary) business objectives and the respective time-sensitivity regarding the prioritisation of their restoration.

- The **risk assessment**, which draws on the established risk management processes, is used for assessing hazards that cause vulnerabilities to arise as a result of the interplay of threats of interruptions of business processes. The (R)IU's most significant risks are defined and prioritised. When conducting the risk assessment there is a particular emphasis on the time-critical IT processes and resources identified in the Business Impact Analysis. A broad spectrum of IT emergencies is taken into account. Typical such examples include cyber attacks, malware, data theft, and risks in relation to the use of cloud services or the exploitation of security vulnerabilities to gain unauthorised access to IT infrastructure.

- IT-specific **emergency planning strategies** are then determined on the basis of the business impact analysis and the risk assessment. Strategies ranging from the full continuity of IT processes and resources through to desisting from imposing measures also depend on cost/benefit analyses. IT emergency planning strategies are determined in **IT contingency plans**, which describe the approaches, alternative solutions and the necessary substitute resources for the restoration or continuation of critical processes.

- **Implementation:**

  - Trainings are held for raising awareness and **trainings** in relation to IT emergency management.

  - Regular (at least annual) IT continuity plan **tests** should be conducted. In the case of processes being altered, or where new material threats emerge, tests should also be conducted on an ad hoc basis.

- **Maintenance and updates:**

  - Amendments are made to continuity plans on the basis of the findings from the IT continuity plan tests conducted.

V. OPERATIVE IMPLEMENTATION

A. IT OPERATIONS

IT operations are responsible for making the hardware and the software necessary to operate the hardware available to an appropriate extent and to operate it without disruption. The requirements placed on IT operations in an (R)IU are based on the business strategy and can be deduced from the IT-supported business processes.

Lifecycles are monitored and managed for ageing IT systems to ensure that such IT systems are adequately taken into consideration. An **inventory related to all IT systems** exists that details their relationships, dependencies and interfaces. Processes exist in relation to new and replacement purchasing taking into consideration potential implementation risks. Furthermore (R)IUs ensure that their IT systems are constantly maintained, and that the relevant maintenance contracts exist.

A **process about dealing with disruptions** and for capturing their causes is determined. For example the potential correlations of disruptions and their causes, as well as the approaches regarding processing, analysis of their causes, finding solutions and follow-ups are captured.

A **data backup plan** in keeping with the emergency management and business processes should be defined. A test should be conducted regarding the restorability and readability of data backups should be carried out both on a regular basis as well as on an ad hoc basis.

B. USER AUTHORISATION PRIVILEGES

The allocation of user authorisation privileges corresponds to the **need-to-know principle**. In the following areas this principle has particular significance:

- The inadmissibility of incorporating the settlement of claims in an organisational unit that also provides legal expenses insurance activities (Article 99 para. 1 VAG 2016), accordingly requires separate user authorisation privileges.
- In the case of outsourcings, effective access to the service provider's data shall be ensured for the (R)IU itself, for the auditor and the FMA with regard to the outsourced functions or business activities (Article 109 VAG 2016).

Preventive measures should be taken to prevent the circumvention of authorisation privileges. The logging of user and administrator activities, for example in relation to claims processing, prevents the manipulation of data. Authorisation privileges that have been granted should be regularly checked that they are being used for their intended purpose, and also adapted as necessary.

The user authorisation privilege concept and the technical user authorisation privilege systems should be in line with the company-specific risk profile.

C. IT PROJECTS, DEVELOPMENT OF APPLICATIONS AND BOUGHT-IN SOFTWARE[8]

The (R)IU should have a complete overview about all significant IT projects and applications developed. The following should be taken into account when implementing them:

- Material **IT projects** should be investigated in advance involving the risk management function and the compliance function with regard to their effects on IT structures and procedures as well as the accompanying IT processes. An adequate risk controlling function should be established. The controlling of IT projects has a particularly high importance in the case of comparatively old IT infrastructure. Material IT projects and their risks should therefore be reported to the management body both at regular intervals as well as on an ad hoc basis.
- **Applications** and **application developments** should be documented in a systematic manner. Appropriate processes should be determined for application developments such as the development of individual software components. These include a system for generating requirements in the individual organisational units, the technical implementation

[8] The remarks that follow also apply for bought-in software.

as well as a controlled testing and acceptance process. Prior to its initial deployment after go live or following material changes applications should be tested with regard to their functionality, security checks as well as system performance in assumed stress situations.

Ensuring the confidentiality, integrity, availability and authenticity of the data to be processed should have already been addressed during the application development stage.

Applications should be monitored for potential deficiencies during normal operation, and the causes of such deficiencies investigated and improved as required.