Munich RE

Excerpt/public version of:
Information Security Management Policy

Policy of Munich Re Group
Version: June 2021

Objectives

Information Security Management shall contribute to:

Protecting the financial strength of Munich Re

A strong financial position is essential to operate as a (re-)insurance company. ISM aims to safeguard Munich Re from significant financial downfalls, e.g. regulatory fines. A company might face those if sensitive personal data or other highly sensitive information is lost, its Information and Communication Technology (ICT) systems are corrupted, or if financial assets cannot be managed temporarily. The financial impact of managing major security incidents, and recovering data, can also be severe. ISM shall enable Munich Re to make full use of the modern digital technologies that are required to offer and manage modern primary and reinsurance products, to increase our potential to write profitable business, and to guarantee our position in the financial services industry.

Protecting the franchise value of Munich Re

Guaranteeing the franchise value requires the ability to quickly adopt state-of-the art information technology solutions and to cope with the changing expectations of increasingly digitally empowered clients. Thus, the increased dependency on IT-supported processes needs to be managed. At the same time, the risk of system interruptions has to be minimised. The failure of these processes, e.g. inability to assess relevant information, could have a significant negative effect. ISM shall support the required measures in order to guarantee the operation of a fully reliable IT infrastructure and proper access to data.

Protecting the reputation of Munich Re

Munich Re is respected as an insurer and as an expert in managing extreme and special risks. Any significant failure in managing the Group's own risks, e.g. from cyber-attacks, could damage our reputation seriously. Therefore, ISM supports Munich Re in both the prevention and management of security incidents, as well as the business recovery from emergency and crisis situations.

Information Security

Information Security Management (ISM) covers all measures to protect information (digital and non-digital proprietary and personal information) and to make sure that IT systems are handled in accordance with the defined requirements for:

- **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information, as well as all business relevant data that is not meant for public disclosure.

– **Integrity:** Preserving the integrity of information by guarding against improper information modification or destruction which includes ensuring information non-repudiation. It also covers information authenticity (as long the protection objective authenticity is not determined and assessed individually).

– **Availability:** Ensuring timely and reliable access to information, when the information is required and ensuring the readability and editability of the information at that time.

Information Security Management Processes

Munich Re Group IS Risk Management establishes group wide standards to enable common understanding of IS risk, consistent and comparable IS risk assessment results, consistency in risk-based measures, as well as support risk transparency and oversight of the IS risk situation by reporting from the entities, to the Segment to the Group. The defined IS Risk Management framework follows a risk-based approach by implementing security management processes and measures that reflect the risk situation and business model of the entity in scope as well as addresses information security objectives and protection needs of Munich Re Group.

The main components and activities of the overall Group IS Risk Management framework are:

– Within the **Cyber Risk Landscape** threats and information security risk drivers relevant for the organisation are captured, described and monitored.

– The **IS Risk Assessment** methods are established to enable standardised, transparent identification, assessment and management of individual risks.

– Processes for risk mitigating measures and acceptance are established based on the risk assessment results and shall also consider **risk tolerance**.

– The **IS risk repository** provides an up-to-date view on the identified information security risks and serves as a basis for risk reporting.

Risk monitoring, review and improvement applies to all these components. This ensures the continuous improvement and adoption of IS risk management processes.

Information Security Policy Framework

The Group ISM Policy together with the Group IS Strategy and all ISM Guidelines and ISM work instructions constitute the Information Security (Risk) Management Policy Framework, which details the IS risk management processes and specifies IS control requirements. The ISM Policy Framework follows a layered approach and each layer defines a different level of granularity regarding the specifications and requirements defined in these documents. The requirements specified in the ISM Policy Framework are aligned with international IS benchmark standards issued from e.g. ISO[1], NIST[2] or BSI[3] as well as regulatory requirements such as BaFin[4]. The Group ISM Policy Framework is the basis for all subsequent information security management activities within Munich Re business fields and ensures consistency among Munich Re Group.

Three Lines of Defense

Information Security Risk Management is organised according to the three-lines-of-defense approach as stipulated by Solvency II governance requirements: risk takers in the fields of business as the first line of defence; the Compliance Function, Actuarial Function and Risk Management Function as the second line of defence; and the Internal Audit Function as the third line of defence:

1. The **1st LoD** is the operational level and shall (in close cooperation with IT service divisions/service providers) define, implement, maintain, and monitor measures to protect digital, physical and verbal information as well as IT systems.

2. The **2nd LoD** responsibility lies with the risk management function; it designs and maintains a governance system for information security (risk) management and shall independently review, assess, and challenge the 1st LoD design, maintenance and operation of procedures and measures to mitigate information security risks. Furthermore, the 2nd line defines processes and minimum requirements for ISM that are to be adhered to by the 1st LoD.

3. The **3rd LoD** responsibility lies with the audit function (internal as well as external) which shall also assess the appropriateness and maturity of implementation and measures by 1st line as well as respective controls by 2nd line.

Information Security Committees and Roles

The **Board of Management** of Munich Re AG has the overall responsibility to ensure that business and risk management are adequately organised. The **Group Risk Committee (GRC)**, a subcommittee of the Group Committee, is responsible for the independent risk management of the Munich Re Group and decides on information security issues with group-wide relevance. The GRC is supported by the **Group Security Risk Committee (GSRC)** as central body of coordination on information security (risk) management between Munich Re Group and the business fields to ensure a regular body of exchange on the information security status of the Munich Re (Group).

On business field[5] level the **Segment Security Risk Committee (SSRC)** are the central exchange forum and decision-making body regarding information security (risk) management on the Segment level. **Virtual communities** are established permanent or temporary and deal with specific issues or projects related to information security. VCs support to create a Group-wide common understanding, new guidelines and work instructions, and develop the overall information security by the Group.

The Chief Information Security Officer **(Group CISO)** is responsible for the Group-wide information security (risk) management and serves as the central point of contact regarding all concerns of the Groups information security (risk) management.

Segment Chief Information Security Officer **(Segment CISO)** are responsible for information security (risk) management within a Segment of Munich Re Group and serves as the central point of contact regarding all concerns of information security (risk) management for the Segment and all its entities. They support the Group CISO in his mission and implementing IS risk management.

Corporate IT Security Officer **(CITSO)** are responsible for ensuring the implementation of operative information security measures within IT and thereby support the implementation of effective information security governance.

[1] ISO = International Organization for Standardization (http://www.iso.org)
[2] NIST = National Institute of Standards and Technology (http://www.nist.gov)
[3] BSI = Federal Office for Information Security (http://www.bsi.bund.de)
[4] BaFin = Federal Financial Supervisory Authority (http://www.bafin.de)
[5] Business field and Segment is used synonymously. Business field/Segment includes the Reinsurance field of business (RI, including Primary Insurance out of reinsurance/PIRI), the Primary Insurance (ERGO) field of business and Group Investment Management function (MEAG).

Contact

Philipp Südmeyer
Group Information Security Officer
Munich Re Group