Excerpt/public version of:
Information Security Management & Business Continuity Management

Policy of Munich Re (Group)
Version: April 2018

Objectives

Information Security Management and Business Continuity Management, jointly referred to as Security Risk 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 and BCM 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 and BCM 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 and BCM support Munich Re in both the prevention and management of security incidents, as well as the business recovery from emergency and crisis situations.

Management disciplines

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, which means preserving the restrictions on authorised access to information and IT systems and preventing unauthorised disclosure of information and unauthorised use of IT systems,
- integrity, which means ensuring accuracy, completeness, authenticity and non-repudiation (origin and content cannot be denied) of information and accompanying metadata and
- availability, which means ensuring timely and reliable access to and use of information and IT systems as required for business purposes.

Business Continuity Management (BCM) shall increase the resilience of areas and processes within Munich Re Group and its local entities in order to ensure the continuation of business operations through pre-defined procedures in possible emergency or crisis scenarios by ensuring that adequate recovery processes are in place.

Therefore, BCM includes all measures to ascertain the ability of a location

- to act during an emergency (emergency management),
- to recover essential business operations within specified timescales, and to restore operations and office space, IT infrastructure, information and all other necessary resources (recovery management).

Three Lines of Defence (LoD)

Munich Re applies the concept of "Three Lines of Defence (LoD)" to manage Information Security Risks and Business Continuity Management.

The 1st LoD responsibility lies with the operational units (e.g. underwriting, claims handling) and central service units (e.g. IT, facility management). These are generally the primary process owners, have budget responsibility, are the information owners and manage the security relevant processes. They are in charge of the assessment of specific security requirements and make sure that appropriate organisational and technical protection measures are applied.

The 2nd LoD responsibility lies with the risk management function; it designs and maintains the governance system for Information Security Risks and Business Continuity Management. It independently reviews, assesses, and challenges the 1st LoD design, maintenance and operation of procedures, and measures to mitigate information security risks. The 2nd LoD is also responsible to define procedures and measures needed for the emergency and crisis management.

The 3rd LoD responsibility lies with the audit function.

Management Bodies and Roles

The Board of Management of MR AG has the overall responsibility to ensure that business and risk management are adequately organised. A Group Committee decides on fundamental questions of cross-segmental strategic and financial management and on general principles of business policy and administration within Munich Re Group. This importantly includes risk management and risk strategy. Part of its scope is to approve directives for ISM and BCM for the entire Munich Re Group.

The executive board has delegated some responsibilities in the context of ISM and BCM to a Security Risk Committee (SRC). It shall ensure an effective and sound management of Information Security Risks and Business Continuity Management across Munich Re Group.

A Chief Information Security Officer (CISO) and a Chief Business Continuity Officer (CBCO) are nominated. The role owners are primarily responsible for managing the 2nd LoD tasks of ISM and BCM on a day-to-day basis.

A Corporate IT Security Officer (CITSO) and deputy are appointed. The CITSO reports about the activities to the Security Risk Committees in each meeting.

Depending on the organisational necessities, at least one individual is appointed as officer, delegate, or coordinator to carry out the tasks of ISM and BCM for a business/service unit or a local entity.

Information Security Management (ISM) and Business Continuity Management (BCM) Strategy

The Chief Information Security Officer maintains an ISM and BCM strategy. It is regularly updated and describes the core components and the priority topics to assure ISM and BCM as set out by the Security Risk Committees.

The overall objectives of the strategy are to achieve a degree of security maturity that is consistent with the risk appetite Munich Re is ready to take and to provide value to the corporation.

Contact

Michael Lardschneider
Group Security Risk Officer
Munich Re Group
mlardschneider@munichre.com

Disclaimer
Münchener Rückversicherungs-Gesellschaft (Munich Reinsurance Company) is a reinsurance company organised under the laws of Germany. In some countries, including in the United States, Munich Reinsurance Company holds the status of an unauthorised reinsurer. Policies are underwritten by Munich Reinsurance Company or its affiliated insurance and reinsurance subsidiaries. Certain coverages are not available in all jurisdictions.

Any description in this document is for general information purposes only and does not constitute an offer to sell or a solicitation of an offer to buy any product.

Münchener Rückversicherungs-Gesellschaft
Königinstrasse 107, 80802 München