Vontobel

Information, IT and cyber security

August 2021

Due to Vontobel's business model, Vontobel operates in a complex technological environment. The protection of confidentiality, integrity and the availability of IT systems and data is therefore of critical importance for Vontobel's operations.

Information, IT and cyber risks form part of Vontobel's operational risk and represent the risk that a technical failure could affect Vontobel's business activities. These risks are not only inherent in the IT infrastructure but also affect the employees and processes that interact with it. It is essential that the data used to support centralized business processes and reporting is secure, complete, accurate and up to date and that it meets appropriate quality standards.

In addition, Vontobel's critical IT systems must be secure and resilient and have the necessary ability, capacity and adaptability to meet Vontobel's current and future business objectives, client needs, and regulatory and legal requirements.

Cyber risk is an integral part of IT risk and involves cases where the functioning of Vontobel's systems is compromised as a result of cyber attacks, security breaches, unauthorized access, loss or destruction of data, unavailability of services, malware, or other security-related events.

To prevent and manage information, IT and cyber risks, various tools are used as part of our comprehensive IT risk management approach, both at operational level and in terms of business continuity and other crisis and emergency plans.

In particular, information, IT and cyber security include the following aspects:

Information, IT and cyber security management

1.	Information security policies	Vontobel's Information Security Policy demonstrates the high level of importance that Vontobel assigns to the security of business information and it sets out the necessary parameters for the management and control of information security. It formulates the overriding objectives and minimum standards that apply to information, IT and cyber security at Vontobel and defines the principles that must be observed to protect information assets during their lifecycle. In the areas of information, IT and cyber security, Vontobel complies with finance industry standards and good business practices, while considering the business needs of its divisions and group companies to the greatest extent possible. In particular, Vontobel complies with laws and regulatory requirements in these areas and thus fulfils its duty towards its various stakeholders – particularly its clients, employees and shareholders. Vontobel reviews all directives and policies at least once a year to ensure they are up to date.
2.	Objective regarding security	Vontobel's overriding security objective is to maintain the entire group's ability to act – both in situations where it faces typical everyday threats and in challenging conditions: – By complying with appropriate and up-to-date safety standards, Vontobel aims to ensure that the trust placed in it by clients is justified; – Appropriate protective mechanisms are intended to ensure that Vontobel's information and IT resources are safeguarded against damage or loss; – If threats affect Vontobel's information or IT resources, it must be ensured that the damage is limited to an acceptable level; – The application of efficient, risk-oriented and up-to-date security measures should contribute to the sustainability of business processes. The aim of information, IT and cyber security is to protect physically and electronically processed information through appropriate and targeted organizational, technical and employee-related measures such as:

		– Ensuring that the requirements resulting from legal, regulatory and internal group specifications are met at all times; – Guaranteeing a high level of reliability of business and operational processes, especially if they are dependent on IT resources; – Ensuring that information is classified according to its importance and suitably protected together with the information systems used for processing and communication purposes; – Preventing, identifying and correcting the loss or falsification of information; – Preventing information from being accidentally, negligently or intentionnally made available to unauthorized persons or used for unauthorized purposes.
3.	ISMS (Information Security Management System)	Vontobel's Information, IT and Cyber Security Management System (ISMS) is based on the ISO/IEC 27001 standard and on normal industry practice according to a peer group comparison. It is compliant with all relevant laws and regulatory requirements. This is verified by independent auditors on a regular basis. Vontobel strives to achieve a balanced level of security, with the ISMS ensuring that security measures are implemented efficiently, i.e. in a risk-oriented manner. Vontobel adheres to normal industry practice ('good business practice') regarding information security. This is achieved by applying a combination of basic protection and special protection, based on risk assessments: – For all information, processes, IT systems and infrastructures, Vontobel strives to put in place basic protective measures in line with normal industry practice, irrespective of the potential risk. These measures are defined in the basic protection requirements; – In the case of systems or applications with a high or very high need for protection, risk assessments are carried out to determine whether additional measures beyond the basic level of protection are required. Vontobel has developed its information, IT and cyber security systems based on the NIST standard and other common standards (e.g. ISO/IEC 27000 series, BSI basic protection), as well as good business practices, and it continuously optimizes them. The security framework includes the following aspects: **Identify:** When analyzing protection requirements, Group Security focuses on the threats listed in the BSI IT Basic Protection Catalogue. Group Security determines the protection needed for Vontobel's own information and assets by means of risk assessments and protection requirement analyses and it documents the overriding risks in an appropriate form. Information, IT and cyber security aspects are identified for all projects and renewal processes at an early stage and are duly documented using suitable risk analyses. The security management system is reviewed periodically using data that is gathered systematically and evaluated on the basis of risks; the data relates to potential new threats, vulnerabilities and trends. If necessary, the security framework is reviewed on a case-by-case basis and adapted where necessary. **Protect:** Vontobel considers the following preventive aspects when developing and implementing security measures to ensure information, IT and cyber security:

- Compliance with legal, regulatory and internal requirements relating to all security aspects mentioned above;
- Organization of information, IT and cyber security;
- Human Resources Security, such as security reviews for internal and external employees (before, during and at the end of their employment);
- Management of Vontobel's own assets, i.e. protection of its own intellectual and tangible assets – and of such assets entrusted to it – against damage or theft, including responsibility for data and information and their classification and handling;
- Physical safety and security, which encompasses all measures that are necessary to prevent unauthorized access or damage to Vontobel facilities;
- Operational security, including application and infrastructure change management, protection against cyber risks and malware (Security Operations Center), back-ups, logging and monitoring, vulnerability management and auditing;
- Access controls to systems and applications as well as the management of access authorizations according to the 'need to know/have/do' principle;
- Procurement, development and maintenance of information systems (systems acquisition, development and maintenance);
- Management of third parties (supplier relationships) as well as outsourcing, online and cloud services.

Preventive forms of protection are risk-oriented to reduce information, IT and cyber security risks to an acceptable minimum through preventive organizational, technical and employee-related measures, in particular:

- The confidentiality of information and its processing is ensured through appropriate technical and organizational measures based on its protection requirements or classification;
- Data owners must determine the protection requirements (confidentiality and protection level) of their information;
- Employees receive the data access rights they require to carry out their work ('need to know/have/do' principle);
- All internal and external employees regularly receive appropriate notification and training (e.g. security awareness programs) about information, IT and cyber security.

Detect:

Continuous Security Incident and Event Monitoring (SIEM) enables anomalies (technical and conduct-based) and security-relevant events as well as changes to critical security settings to be detected, analyzed and flagged as automatically and promptly as possible.

The evidence, benefits and efficiency of the defined monitoring use cases are reviewed periodically.

Respond:

If information is at risk or if an information, IT and cyber security incident occurs, a suitable, planned process is implemented. Sustainable and tested incident processes are defined for this purpose; these processes initiate appropriate measures to address existing risks, especially in the case of incidents involving sensitive information or client data. The Security Incident Handling Process is adapted continuously on the basis of new findings.

		Recover: In the case of small and medium-scale information, IT and cyber security events, affected IT resources are restored to a defined state and returned to normal operation (remediation and recovery). The causes of the security incident (e.g. patching) are eliminated or mitigated using compensatory measures. To prevent emergencies and crises, an Emergency Management Process has been put in place and is operational. Suitable preventative measures must be defined to increase the robustness and reliability of business processes on the one hand, and to enable a rapid and targeted response in an emergency or crisis on the other. The IT organization has developed an emergency concept for this purpose, describing the implementation of the emergency strategy and the planned process. Regular tests and emergency exercises are carried out to verify the effectiveness of Emergency Management.
4.	Organizational responsibility for information security and privacy	Vontobel has a Chief Information Security Officer (CISO) who is responsible for group information security and compliance with regulations regarding data security. It also has a Data Protection Officer (DPO) who is responsible for compliance with data privacy regulations. The CISO and DPO report to the Vontobel Executive Committee and oversee the conceptual and strategic design of data security and privacy. Data security measures are implemented by several specialized IT teams. Each team consists of IT engineers with individual knowledge in their field of responsibility and who are also responsible for cyber defense and the monitoring of data security. The members of the Vontobel Executive Committee have overall accountability for all risks related to information security and privacy.
5.	External expertise on cyber security	Vontobel is a member of commercial and non-commercial information, IT and cyber security committees, which work together to strengthen preventive measures on a targeted basis, to continuously expand the detection of security incidents using efficient measures, and to act quickly and purposefully if incidents occur. This is a regulatory requirement imposed on banks by FINMA. The main purposes of these working groups are to: – Maintain active networks for the exchange of experience and information within each working group; – Evaluate approaches, technologies and methods; – Be willing to cooperate and engage in a dialogue with other organizations and bodies about information security issues; – Develop centers of expertise for information, IT and cyber security; – Promote standardization in the areas of information, IT and cyber security; – Maintain a dialogue with manufacturers, suppliers and service providers. Examples of national & international bodies (non-exhaustive list): – The National Cybersecurity Centre (NCSC) is the Swiss Confederation's competence centre for cybersecurity and thus the first contact point for businesses, public administrations, educational institutions, and the general public for cyberissues. The Reporting and Analysis Centre for Information Assurance (formerly known as MELANI), together with the national Computer Emergency Response Team (GovCERT), has been integrated into the NCSC as a technical expertise hub and expanded further;

		– The Information Technology Security Working Group (ASIT) is a professional association of CISO bank representatives; – The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a global cyber intelligence sharing community solely focused on financial services.
6.	Management of risks	Vontobel adheres to the proven 'Three Lines of Defense' risk management model and follows industry standards ('good business practice') regarding information security. This is achieved by applying a combination of basic protection and special protection, based on risk assessments: – For all information, processes, IT systems and infrastructures, Vontobel strives to put in place basic protective measures in line with normal industry practice, irrespective of the potential risk. These measures are defined in the basic protection requirements; – In the case of systems or applications with a high or very high need for protection, risk analyses are carried out to determine whether additional measures beyond the level of basic protection are required. For all business processes with increased or high risk potential, the expected residual risk is assessed as far as possible and reported transparently to the decision-makers. They reach a formal decision on whether the residual risk should be accepted, whether further measures to reduce or transfer risk are needed, or whether the business process must be stopped or cannot be implemented. The decisions are documented in a comprehensible and appropriate manner. In addition, the CISO submits with support by the technical IT security teams a semi-annual report to the Vontobel Executive Committee and the Risk and Audit Committee of the Board of Directors. These reports cover relevant cyber security risks, issues, and updates to the cyber security strategy, as well as immediate measures taken.
7.	Compliance	Vontobel ensures that it is compliant with all relevant regulations. This is verified by independent auditors on a regular basis. This includes the regulatory requirements listed below and normal industry practice based on a peer group comparison (non-exhaustive list): – Swiss Federal Act on Banks and Savings Banks; – Swiss Data Protection Act; – EU General Data Protection Regulation (GDPR); – FINMA Circular 2008/10 'Self-regulation as a minimum standard', information on Business Continuity Management; – FINMA Circular 2008/21 'Operational risks - banks'; – FINMA Circular 2017/01 'Corporate governance – banks'; – FINMA Circular 2018/3 'Outsourcing – banks and insurers'; – Recommendations of the Swiss Bankers Association of November 2007 on Business Continuity Management (BCM); – Information paper of the Swiss Bankers Association of October 2012 on 'Data Leakage Protection' (Circular 7752); – Banking supervisory requirements for IT (BAIT) issued by the German Federal Financial Supervisory Authority (BaFin); – U.S. Securities and Exchange Commission (SEC) Guidance on Public Company Cybersecurity Disclosures;

		– NIST Cyber Security Framework; – ISO/IEC-27000 series (international standards on information security); – Requirements of the German Federal Office for Information Security (BSI).
8.	Auditing of information systems	As a financial institution, Vontobel is subject to ongoing internal and external audits in accordance with the applicable legal and regulatory requirements (e.g. FINMA commissions the auditor Ernst & Young to review the effectiveness of security concepts and implemented measures on an annual basis). At Vontobel, the Operational Risk Control unit is responsible for carrying out periodic quantitative and qualitative risk controls and reporting on the effectiveness of information, IT and cyber security to the Group Executive Management and the Board of Directors. Relevant implementations, adjustments, changes, proofs of concept, etc. are coordinated with the CISO at an early stage. In addition, IT security concepts are checked and formally approved by the CISO before an application, service or significant change goes live. To verify the secure technical implementation of measures, the CISO can order security audits, penetration tests or vulnerability scans prior to productive acceptance. The CISO, or an internal body appointed by him, is author ized to check the implementation and compliance with the defined specifications for information, IT and cyber security, as well as data protection. This is ensured by means of assessments or security audits at any time covering the effectiveness of the implemented organizational, technical, employee-related and other measures. The CISO can commission security audits, penetration tests and vulnerability scans to check the security management system and to adapt or optimize overall security in view of the current risk situation.
Employee security		
9.	HR security	Vontobel performs screening and background checks on new Vontobel employees. Furthermore, Vontobel periodically performs background checks on key employees. All employees have to sign a non-disclosure or confidentiality agreement when joining Vontobel.
10.	Return of IT resources	Upon termination of employment contracts, Vontobel employees are required to return Vontobel IT resources, which refers to all means of electronic data processing. In particular, it includes all hardware used, all data storage options, standard and individual software, all forms of electronic data and all other types of IT technologies.
11.	End-user responsibility	In accordance with the applicable group directives, Vontobel employees have a duty to ensure information, IT and cyber security; this is regarded as a personal responsibility. For the purpose of this directive, employees are defined as all permanent or temporary employees of Vontobel and external persons who have access to Vontobel's IT resources or are users of Vontobel's IT resources within the scope of their mandate. Employees are personally responsible for the careful use of IT resources. In particular, they are responsible for ensuring that the relevant requirements of data and information security as well as data protection are complied with at their workplace and in their area of responsibility and that the necessary measures are taken (e.g. clear desk). All employees are also instructed to

		classify data and information according to its need for protection (see section 14 below). This responsibility applies irrespective of their function and rank and cannot be delegated. Employees are personally responsible for ensuring that their use of IT resources does not violate group directives or other provisions of the applicable legal system (e.g. banking legislation, criminal law, data protection legislation, intellectual property, personal rights, regulatory provisions, etc.).
12.	Responsibility of line manager	In the context of their supervisory role, line managers must ensure that their employees behave in accordance with security requirements. By providing information, they raise awareness of security aspects in their area of responsibility and use their function to act as a role model. In addition, they support and promote the training of their employees in the area of information security and in aspects of client data security.
13.	Regular security awareness training	Training in the field of information security policy is conducted regularly and also forms part of employee induction days. Vontobel defines the content and method of delivery for the awareness program in a multi-year roadmap. The content of the training course is updated continuously to address the current threat landscape. Successful completion of training is monitored, and repeated if not passed.

Data classification and handling

14.	Data classification	At Vontobel, information is classified according to its importance and is suitably protected together with the information systems used for processing and communication purposes. The classification and handling of classified information is defined in a separate group directive. Data owners are those persons who are responsible for the handling of information in the area assigned to them. They determine the need for protection and therefore the classification of their information, check access rights to their information in accordance with the 'need-to-know/have/do' principle and approve requests for access to their information. Depending on their classification level, data and information are additionally protected by further technical measueres (e.g. encryption).
15	Unintended disclosure of sensitive information	Employees may only use the authorized online services and cloud applications made available and thus are officially approved by Vontobel to perform their business activities. In accordance with the relevant directive, only information classified as 'public' may be stored on systems or services not provided by Vontobel, unless the consent of the data owner has been obtained. Preventing data loss is an important aspect to ensure compliance with regulatory requirements (e.g. FINMA Circular 2008/21, Appendix 3 'Protection of client data'). Vontobel has a Data Leakage Prevention system (DLP) in place which identifies and monitors various categories of sensitive information. Violations of the applicable guidelines are handled in an orderly process. The system protects against the intentional and inadvertent transmission of sensitive data. It not only examines the text of an e-mail or a web upload but also the contents of file attachments sent to any recipient on the Internet.
16.	Intended disclosure of sensitive information	See section 15.

Access management

17. Access control policy	Vontobel has a group directive governing access rights and roles, the procedure and process for creating, modifying and deleting access rights and authorization roles in IT systems and applications, as well as the regular control of access rights and authorization roles. This ensures that: – Access rights to buildings and to Vontobel's IT systems/applications, communication services, programs, directories or files are only granted to authorized employees; – Roles are compatible with the activities performed by the user (business roles) at Vontobel and are compatible with the IT services and application systems (application roles) that are provided or are available; – The unwanted accumulation of access rights is prevented; – Only authorized employees can create, modify or delete access rights; – Employees are given those rights they need to perform their work (according to 'need-to-know/have/do' principle); – Existing rights can be event-driven and periodically reviewed and modified as needed.
18. Approval process	Access to buildings, systems and data is only granted once the necessary approvals have been obtained from the authorized units. Identity and Access Management (IAM) manages users, application/business roles and special authorizations. Exceptions must be approved by the information or application owner, in close cooperation with the CISO. Vontobel has established an IAM system to manage access rights. Its main duties are as follows: – Processing appointments, terminations and transfers of internal and external employees on behalf of Human Resources (HR) and the responsible line managers; – Coordinating, processing and implementing authorization requests in cooperation with the responsible line, application and business role managers; – Defining, implementing and managing IT access rights for business functions using business roles in collaboration with the business role managers in the divisions; – Documenting and archiving (in accordance with auditing requirements) authorization requests and updates for each employee; – Performing the annual User Entitlement Review (UER) and coordinating the upstream review of application and business roles that are managed in IAM.
19. Review of access rights	As part of the annual User Entitlement Review (UER), all access rights of employees are checked by the responsible line manager and adjusted if necessary. The functionality and ownership of application and business roles are also reviewed annually and modified if necessary. The nominated role owners are responsible for this. IAM is also responsible for coordinating review activities.

20. Leavers	User entities and the underlying access rights are immediately deactivated if an employee's relationship is terminated.
21. Need-to-know / need-to-have / need-to-do	Employees receive the rights they need to carry out their work (according to the 'need-to-know/have/do' principle). Vontobel's organizational structure forms the basis for the development of roles. The assignment of employees to roles is based on their function, duties, responsibilities, or position at Vontobel.
22. Good practice	Good practice is applied to the management of user entities and passwords: – Strong authentication with a personal Corporate ID Smart Card is always used when authenticating to workstations; – Good business practice is used for the management of user credentials; – Password requirements meet the industry standard and are system-enforced; – All password requirements are set out in a corporate password guideline.
23. Logging and monitoring of activities	Administrative activities are logged and reviewed on a regular basis to ensure compliance with the applicable guidelines. In addition, Vontobel reviews its access control reports to detect any irregularities.
Physical security	
24. Clear desk and locking of computers	Clear desk requirements are set out in a policy. As a result of targeted measures to raise awareness among employees, they know that sensitive documents, portable media and devices must be locked away whenever they are away from their workstation. Access to Vontobel's buildings and authentication at workstation PCs is carried out by means of strong authentication, i.e. using a personal Corporate ID Smart Card. When leaving the building, employees must take their Smart Card with them, thus automatically locking their PC. Group Security carries out random checks to verify compliance with the Clear Desk Policy during and outside working hours and it reports the results to the Group Executive Management.
25. Physical access	The personal Corporate ID Smart Card must be used to gain access to Vontobel offices. When leaving the building, employees must take their Corporate ID Smart Card with them. Vontobel offices can only be accessed by authorized persons and access times are role-based dependent on the regular working hours of each individual employee. In sensitive areas (e.g. data centers) and outside normal working hours, authorized employees require a PIN in addition to enter Vontobel offices. Access to buildings and movements within sensitive areas are also recorded using video surveillance.
Security operations	
26. Archiving	All business-relevant documents are archived according to the applicable regulations and the recovery of back-ups is tested periodically.

27. Removable Media	Removable devices and media are subject to controls and are basically not permitted for use within Vontobel's infrastructure. Writing access to removable media is restricted to those employees who require such access for their work.
28. Portable equipment	The requisite safeguards for the use of portable equipment (e.g. laptops, back-up discs, removable media) is governed by appropriate policies. Client data is never stored on mobile devices.
29. Secure destruction	When they are no longer required, all media are disposed of securely after any data has been erased, in accordance with Vontobel procedures. The off-site destruction of media is recorded and the records are audited.
30. Malware checks	All workplace computers and servers (incl. e-mail) are protected against malware. Internet access is managed by a proxy service which checks if any malware is contained in Web traffic and allows access to trusted websites only.
31. Patching and vulnerability management	Vontobel has a patch management process in place to ensure that the latest security patches are installed on its systems. In addition, Vontobel has a vulnerability management process to detect and remediate security vulnerabilities.

Secure communication

32. Network security	Vontobel has divided its network into zones according to the risks involved. All Vontobel systems and IT equipment are placed in an appropriate zone according to their respective requirements, the services provided, and their protection needs. Communication between all systems is limited to what is technically and organizationally feasible. Exposed systems are placed in a multi-tier Demilitarized Zone (DMZ). Networks are monitored continuously by means of an Intrusion Detection and Prevention System. Further security functions such as e-mail filters, Internet proxy servers and malware scanners are used in the case of end-user access to the Internet. To be adequately protected against Distributed Denial of Service attacks (DDoS), appropriate measures have been taken together with the Internet Service Providers to enable the continued operation of services relying on the Internet connection, even during such an attack.
33. Data transfer security	Vontobel maintains a register for internal and external interfaces. Data transfers always take place via encrypted connections. Each data transfer is monitored by the Data Leakage Prevention (DLP) System.
34. Use of mobile devices	Vontobel does neither provide nor use mobile devices at all. However, employees receive limited, secured remote access to the Vontobel network via private devices (BYOD). This access is either provided on mobile devices such as phones and tablets (primarily for accessing emails, intranet, etc.) or via restricted connection to the employee’s private virtual desktop (VD). No business data is stored on BYOD.
35. Secure Internet access	The Internet is accessed via a proxy server. Illegal, inappropriate, or security-critical web content, as well as risky websites that endanger the security or stability of IT operations are automatically blocked using technical filters.

36. Monitoring of internet traffic	All Internet usage is monitored regarding security and operational stability as well as for compliance with employment law or ethical requirements and, if necessary, is blocked consequently.

Compliance and data privacy

37. Data privacy	Vontobel is committed to complying with all relevant data privacy regulations and it outlines the important aspects in its publicly available privacy policy (see https://www.vontobel.com/en-ch/legal-notice/privacy-policy/). The policy covers all personal data of clients and prospective clients and describes the rights of the individuals concerned regarding their data.
38. Management of third parties	Vontobel carries out third-party due diligence, including risk assessments, integrity checks, track record checks, the identification of red flags and the definition of requirements such as ISO 27001 certifications. Vontobel's data processors are required to implement suitable measures to ensure information security, and therefore must comply with Vontobel's technical and organizational measures (TOM). In the event of further outsourcing to third parties, the contract data processor must ensure that the third parties comply with the agreement reached with Vontobel. Furthermore, the data processor must have each subcontractor approved by Vontobel. Contract data processors undergo an assessment. All contracts with data processors include the right to an independent audit. Depending on how critical the contract data processor is, activities are carried out in varying levels of detail. The execution of these audit activities is regularly verified by the regulator.

Security incident management and continuous monitoring

39. Security incident management and continuous monitoring	Based on the NIST Cyber Security Framework, Vontobel maintains its own Security Operations Center (SOC) which uses tools to detect attacks or attempted attacks (e.g. unauthorized activities at network level). Security-relevant events are logged. Indicators of attacks are processed by Vontobel's own Computer Emergency Response Team (CERT) according to a defined and documented process. The roles and responsibilities for handling such incidents are defined and documented. A recommended course of action is in place for typical attack scenarios. If necessary, the procedure is coordinated with the relevant authorities. In the event of an information, IT or cyber incident that has occurred, depending on the scope and area of responsibility selective authorities are informed compliant with relevant laws and regulatory requirements. The Security Incident Handling Process is updated continuously based on new findings.
40. Notification of affected parties in the event of a data breach	Vontobel strives to be fair and proportionate when considering the actions to be taken to inform affected parties regarding any breaches of personal data. If a breach is known to have occurred that is likely to place the rights and freedoms of data subjects at risk, clients and, if necessary, the relevant supervisory authority are informed within the relevant local time period by the responsible DPO, in accordance with applicable laws and regulations.
41. Lessons learned	If security events occur, they are analyzed and evaluated after they have been resolved in order to identify possible risks for Vontobel and to develop new preventive measures, such as improving basic protection or making adjustments in the area of logging and monitoring.

Business Continuity Management	
42. BCM processes	Vontobel meets the Swiss regulatory requirements for Business Continuity Management (BCM) prescribed by the Swiss Financial Market Supervisory Authority (FINMA). An emergency management process has been defined to prevent emergencies and crises.
43. DRP review and tests	Vontobel has prepared an emergency concept with suitable preventive measures, which increase the robustness and reliability of business processes on the one hand and facilitates a rapid and targeted response in an emergency or crisis on the other. Regular tests and emergency exercises are carried out to check the effectiveness of emergency management and disaster recovery measures and procedures.