Vontobel

Information, IT and Cyber Security

January 2024

CISO Office

Technology & Services

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

Information, IT and cyber risks are part of Vontobel's operational risks and represent the threat that a technical failure could affect Vontobel's business activities because of cyber-attacks, security breaches, unauthorized access, loss or destruction of data, unavailability of services, malware or other security-related events. These risks are not only inherent in the IT infrastructure, but they also affect the employees and processes that interact with it. It is essential that the information used to support centralized business processes and reporting is secure, complete, accurate and up-to-date and that it meets appropriate quality standards.

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

Information, IT and cyber security at Vontobel includes the following aspects:

1. Cyber security management

1.1. Information security policy

Vontobel's information security policy demonstrates the high importance that Vontobel assigns to the protection of information. It sets out measures for the management to control the information, IT and cyber security. It formulates the overarching objectives aligned with Vontobel's vision and the minimum safeguards that apply to information, IT and cyber security at Vontobel. It defines the principles that must be observed to protect information assets during their lifecycle.

In the areas of information, IT and cyber security, Vontobel follows the finance industry's standards and good business practices, while considering the business needs of its divisions and group companies to the greatest extent possible. Vontobel complies with laws and regulatory requirements in these areas and thus fulfills its duty toward its various stakeholders – particularly its clients, employees and shareholders.

1.2. Security objectives

Vontobel's overriding security objective is to have resilient computer operations in place even in challenging conditions:

- By complying with appropriate and up-to-date security 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 effective, risk-oriented and up-to-date security measures contributes 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 physical measures such as:

- Complying with legal, regulatory and internal group requirements;
- Continuously identifying and evaluating the threat landscape and adjusting necessary measures;
- Ensuring that information is classified according to its importance and is 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 intentionally exposed to unauthorized stakeholders or used for unauthorized purposes.

1.3. Information security management system (ISMS)

Vontobel's Information, IT and Cyber Security Management System (ISMS) is based on the standard ISO/IEC 27001. Independent auditors verify on a regular basis the adequacy and compliance with relevant laws and regulations of the ISMS and provide assurance to Vontobel's customers with dedicated ISAE 3000 assurance reports.

Security measures are implemented following a risk-based and balanced approach aligned with industry practice. The maturity of the ISMS is regularly assessed and compared with a peer group:

– For all information, processes, 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 an increased need for protection, additional measures beyond the basic level of protection are implemented.

Vontobel has developed its information, IT and cyber security based on the NIST Cybersecurity Framework and other common standards and frameworks (e.g., ISO/IEC 27000 series or BSI basic protection), as well as industry business practices. The ISMS is continuously optimized to address the latest threats and developments and it includes the following aspects.

Identify:

When analyzing protection requirements, the BSI basic protection catalogue is considered to determine the protection needed for processed and stored information and assets by means of risk assessments and protection requirement analyses. It documents the overriding risks in an appropriate form. Information, IT and cyber security aspects are considered at an early stage of projects and renewal processes and they include risk assessments. The security management system is reviewed periodically using data that is gathered systematically, evaluated based on risks and relates to potential new threats, vulnerabilities and trends.

Protect:

In addition to the other aspects, Vontobel considers the following risk-based preventive aspects when developing and implementing security measures:

– Compliance with relevant legal, regulatory and internal requirements relating to security and privacy;
– Organization of information, IT and cyber security;
– Human resources security, such as security reviews of employees and external contractors (before, during and at the end of their engagement);
– 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 management of application and infrastructure changes, protection against cyber risks and malware (Security Operations Center) and implementation of back-ups, logging and monitoring, patching, vulnerability management and auditing;
– Access controls to systems and applications and management of access authorization 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;

– Ensuring the confidentiality of information and its processing through appropriate technical and organizational measures based on its protection requirements or classification;
– Data protection requirements (confidentiality and protection level) are determined by the data owners;
– Appropriate notification and training about information, IT and cyber security and privacy (e.g., security awareness programs) regularly provided to employees and external contractors.

Detect:

Continuous Security Incident and Event Monitoring (SIEM) enables the detection of anomalies (technical and conduct-based), security-relevant events and changes to critical security settings. Events are flagged and analyzed. The defined monitoring use cases are periodically reviewed and adjusted to reflect latest threats.

Respond:

If information is at risk or if an information, IT and cyber security incident occurs, regularly updated processes are implemented and tested to respond to the situation. These processes initiate appropriate measures to address existing risks, especially in the case of incidents involving sensitive information or client data. With regular cyber incident exercises, potential gaps are identified and the plans are adjusted accordingly.

Recover:

In case of a cyber security event, Vontobel is prepared to restore IT resources and information to a defined state and return to normal operation (remediation and recovery). The causes of the security incident are eliminated or mitigated using adequate measures. To manage emergencies and crises, an emergency management process is in place. Suitable preventive measures are defined to increase the resilience of business processes and to enable a rapid and targeted response in an emergency or crisis. The IT organization has developed an emergency concept for this purpose, describing the implementation of the emergency strategy and the planned process. Business continuity and recovery tests and crisis tabletop exercises are regularly carried out to verify the effectiveness of established security incident or crisis management, which include external expertise.

1.4. Organizational responsibility for safety, security and privacy

Vontobel has a Chief Information Security Officer (CISO), who is responsible for group information security and compliance with regulations regarding information, IT and cyber security, and 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 information, IT and cyber security and privacy protection.

Security measures are implemented and operated by specialized IT teams. Each team consists of IT engineers with extensive knowledge in their field of responsibility and who are also responsible for cyber defense and monitoring.

The members of the Vontobel Executive Committee are accountable for all risks related to safety, security and privacy.

1.5. 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. 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.

Some examples of national and international bodies (non-exhaustive list) that partner with Vontobel include:

- The National Cybersecurity Centre (NCSC), the Swiss Confederation's competence center for cyber security – and thus the first contact point for businesses, public administrations, educational institutions and the general public for cyber issues;
- The Information Technology Security Working Group (ASIT), a professional association of Swiss Banking CISOs;
- The Financial Services Information Sharing and Analysis Center (FS-ISAC), a global cyber intelligence sharing community solely focused on financial services;
- The Financial Sector Cyber Security Centre (FS-CSC), a Switzerland-based cyber intelligence and sharing community specifically for financial services.

1.6. Management of risks

Vontobel adheres to the proven "three lines of defense" risk management model and follows industry standards ("good business practices") in managing technology and cyber risks.

For relevant business processes, the expected inherent and residual risk is assessed and reported transparently to decision-makers and risk-takers. They reach a formal decision on whether the residual risk can be accepted, whether further measures to reduce or transfer risks are needed or whether the business process must be stopped or cannot be implemented. The decisions are documented.

In addition, the CISO, with the support of the technical IT security teams, submits 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.

1.7. Compliance

Vontobel has processes in place to assess compliance with relevant regulations and frameworks. 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);
- Relevant and applicable circulars issued by the Swiss Financial Market Supervisory Authority (FINMA);
- 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).

Internal and external audits are regularly performed to assess compliance status.

1.8.	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. At Vontobel, the Operational Risk Control unit is responsible for carrying out periodic quantitative and qualitative risk assessments and reporting on the effectiveness of information, IT and cyber security of the internal control system 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, a Technology Risk Management System assesses the cyber and operational risk resilience of solutions during their lifecycle. To verify the effective implementation of technical measures, security audits, penetration tests or vulnerability scans are performed prior to productive acceptance and on an ongoing basis. The CISO, or an internal body appointed by the CISO or Group Internal Audit, is authorized to check the implementation and compliance with the defined specifications for cyber security.

2. Employee security

2.1.	HR security	Vontobel performs screening and background checks on new Vontobel employees and periodically performs background checks on key employees. Employees must sign a non-disclosure or confidentiality agreement when joining Vontobel.
2.2.	End-user responsibility	In accordance with the policies, all permanent or temporary employees of Vontobel and external persons who have access to or are users of Vontobel's IT resources within the scope of their mandate are personally responsible for complying with policies, compliance regulations and laws. This responsibility applies irrespective of their function and rank and cannot be delegated.
2.3.	Responsibility of line manager	In the context of their supervisory role, line managers ensure that their teams behave in accordance with policies, compliance regulations and laws. Leading by example, they raise awareness of security aspects in their area of responsibility. In addition, they set annual goals and support and promote the training of their employees in information, IT, cyber security and aspects of data privacy.
2.4.	Awareness and security training	Security and privacy training is provided as part of employee onboarding and periodically thereafter. Dedicated employee groups such as developers, administrators, managers, etc. must attend specific training sessions. When significant cyber risks emerge or policies are introduced or changed, the CISO conducts targeted training or briefings in a timely manner. A comprehensive concept has been created on how to instruct and train end users in the secure, safe and lawful use of IT resources and other relevant aspects of it. Special attention is paid to raising user awareness in order to improve security and reduce cyber and technology risks. To meet the conceptual requirements, Vontobel defines the content for the awareness program in a multi-year roadmap. The content of the training course is updated continuously to address the current threat landscape and successful completion of training is monitored. Phishing simulations are carried out at regular intervals.
2.5.	Return of IT resources	Upon termination of their employment contract, Vontobel employees are required to return Vontobel IT resources, which refers to all means of electronic data processing. This includes all hardware, all data storage options, standard and individual software, all forms of electronic data and all other types of IT technologies.

3. Data classification and handling

3.1	Data classification	Information is classified according to its criticality or sensitivity and is suitably protected together with the information systems used for processing and communication purposes. The classification and handling of information is defined in a group directive. Data owners are responsible for the handling of information in the area assigned to them. They determine the protection level and therefore the classification of their information and adequate security measures (e.g., access management in accordance with the “need-to-know/have/do” principle). Depending on their classification, data and information are additionally protected by technical measures (e.g., encryption).
3.2.	Data Leakage Prevention	Employees may only use authorized online services and cloud applications made available and officially approved by Vontobel in performing their business activities. Vontobel has a Data Leakage Prevention (DLP) system in place, which identifies and monitors information. The system checks against the policies to ensure the best possible protection against intentional or inadvertent transmission of sensitive data.
3.3.	Secure information exchange	To exchange information with external stakeholders, Vontobel provides tools for secure information exchange, namely, secure web storage and secure email. When exchanged, information is scanned by DLP and anti-malware solution.
3.4	End Using Application	Vontobel, in certain rare cases, uses End Using Applications (EUA) for non-standardized business cases. A centralized inventory of the relevant EUAs is maintained and integrated into the risk management processes in order to monitor compliance with Vontobel policies.

4. Access management

4.1.	Access control policy	Vontobel has a group policy 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 review of access rights and authorization roles. This ensures that: – Access rights to premises and to Vontobel’s IT systems/applications, communication services, programs, directories or files are only granted to authorized employees; – Roles are aligned with the activities performed by the user (business roles) at Vontobel and are linked to the IT services and applications (application roles) that are provided or available; – The 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); – Access rights are reviewed regularly and privileges that are no longer needed are revoked in a timely manner.
4.2.	Approval process	Access to premises, systems, services and data is only granted after approval from the authorized functions, depending on the criticality. Identity and Access Management (IAM) is responsible for managing user accounts, application/business roles and special authorizations. Exceptions are

approved by the information or application owner, in close cooperation with the CISO.

Integration into the IAM system mainly involves:

- processing appointments, terminations and transfers of employees and external contractors on behalf of Human Resources (HR) and the responsible line managers;
- Coordinating, processing and implementing authorization requests in cooperation with the responsible line manager, application or business role owner;
- 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 user;
- Performing the annual User Entitlement Review (UER) and coordinating the upstream review of application and business roles that are managed in IAM.

4.3.	Leavers and movers	User entities and the underlying access rights, as well as access to the premises, are promptly deactivated after an employee has left the company or no longer needs access. When a user moves to another role, all rights are revoked and reassigned based on the new role.
4.4.	Review of access rights	As part of the annual User Entitlement Review, all access rights of users are reviewed by the responsible line manager or role owner and are adjusted if necessary. The nominated role owners are responsible for reviewing and modifying annually the functionality and ownership of application and business roles. The access roles in the IAM tool are regularly reconciled with the business applications.
4.5.	Need-to-know/ need-to-have/ need-to-do	Users' access is limited to the privileges they need to carry out their work (according to the "need-to-know/have/do" principle). Vontobel's organizational structure forms the basis of access roles. Employees are assigned to roles based on their function, duties, responsibilities or position at Vontobel.
4.6.	User credentials	Good practice is applied to the management of user entities and credentials: – Strong authentication based on multiple factors is enforced at each login to workstations; – Good business practice is used for the management of user credentials; – Password requirements meet the industry standards and are system-enforced; – All password requirements are set out in a corporate password guideline.
4.7.	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.
4.8.	Privileged Access Management	Vontobel has a Privileged Access Management (PAM) solution in place to manage user accounts with extended access rights. Privileged access roles require additional approvals from the CISO or application, server or service owners and are regularly recertified.

5. Physical security

5.1.	Data centers	Vontobel operates two professionally managed data centers in the Zurich metropolitan area. HVAC is provided by the building service provider, where Vontobel remains responsible for access restrictions. Hardware is physically separated from that of other clients. Regular business continuity tests are performed and the results are analyzed.
5.2.	Clear desks and computer locking	Clear desk requirements are set out in a policy and are part of targeted awareness training. Workstations are automatically locked after a few minutes of inactivity. Group Security carries out random checks to verify compliance with the clear desk policy during and outside working hours; it reports the results to the Group Executive Management.
5.3.	Physical access	Vontobel offices can only be accessed by authorized persons using a personal corporate ID card during office hours. Outside of regular office hours or in sensitive areas (e.g., data centers), a personal PIN is additionally required. There is video surveillance in sensitive areas.
5.4.	Visitors	Visitors on Vontobel premises are registered and accompanied at all times. A security guard is on duty during office hours at the main entrance and maintains a visitor log. Access of visitor badges is limited.
5.5.	Pull-printing	Pull-printing is used on Vontobel premises, where users must authenticate with their personal corporate ID card on the printer before the task begins.

6. Security operations

6.1.	Archiving	Business-relevant documents are archived according to the applicable regulations, retention periods and legal hold requirements.
6.2.	Removable media	Removable media are basically not permitted for use within Vontobel’s infrastructure. Write access to removable media is restricted to those employees who require such access for their work.
6.3.	Portable equipment	Vontobel neither provides nor uses mobile devices at all. However, the requisite safeguards for the use of private portable equipment (BYOD, e.g., laptops or removable media) is governed by appropriate policies. Client data is not stored on portable equipment.
6.4.	Secure destruction	When media devices are no longer used, they are disposed securely after data has been erased, in accordance with Vontobel procedures. Media that cannot be wiped are physically destroyed. The wiping process and the off-site destruction of media is recorded and the records are audited.
6.5.	Malware checks	Workplace computers and servers are protected against malware. Inbound and outbound email and web traffic is scanned for malware. Access to websites is restricted based on regularly updated, category-based blacklists.
6.6.	Patching and vulnerability management	Available security and functional patches are assessed and implemented if relevant as part of Vontobel’s patch management process. Regular vulnerability scans identify missing patches or misconfigurations, which are then addressed.

6.7.	Back-up/ Restore	Scheduled back-ups of enterprise platform systems are regularly performed and stored offsite in another data center. The back-up solution is protected against cyber attacks and critical data is backed up immutably. Restore procedures are regularly tested.

7. Secure communication

7.1.	Network security	Vontobel has divided its network into zones. Systems and IT equipment are placed in the appropriate zone according to their requirements, the services provided or their protection needs. Communication between systems is limited to what is technically and organizationally necessary. 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 email filters, internet proxy servers and malware scanners, are used in case of end-user access to the internet.
7.2.	Secure internet access	The internet is accessed via a proxy server. Web content that is categorized as illegal, inappropriate or security-critical, as well as risky websites that endanger the security or stability of IT operations, are automatically blocked by using technical filters.
7.3.	Monitoring of internet traffic	All internet usage is monitored regarding security, operational stability and compliance with employment law or ethical requirements; if necessary, it is blocked.
7.4.	DDoS protection	To be adequately protected against Distributed Denial of Service (DDoS) attacks, appropriate measures have been taken together with the Internet Service Providers to enable the continued operation of services that rely on an internet connection, even during such an attack.
7.5.	Secure data transfer	Vontobel maintains a register for internal and external interfaces and APIs. Data transfers take place via encrypted connections and are monitored by the Data Leakage Prevention and malware protection system.
7.6.	Use of mobile devices	Vontobel neither provides nor uses mobile devices at all. However, employees receive limited, secure 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, the intranet, etc.) or via restricted connection to the employee’s private virtual desktop. No business data is stored on BYODs.

8. Compliance and data privacy

8.1.	Data privacy	Vontobel is committed to complying with 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.
8.2.	Management of vendors and third parties	Vontobel carries out third party due diligence, including risk assessments, integrity checks, track record checks, red flag identification and the definition of requirements such as ISO/IEC 27001 certifications or assurance reports.

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. In the event of further sub-outsourcing, the contract data processor must ensure that the fourth parties comply with the agreement reached with Vontobel.

Contracts with data processors include the right for an independent assessment or audit, which is performed in varying levels of detail. The execution of these audits is regularly verified by the regulator.

9. Security incident management and continuous monitoring

9.1.	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 the network level). Security-relevant events are logged. Indicators of such 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 incidents are defined, documented and tested. A recommended course of action is in place for typical attack scenarios. If necessary, the procedure is coordinated with the relevant authorities. Vontobel has procedures in place to promptly report cyber incidents – depending on the impact – to competent regulators and other stakeholders, like clients. The process for handling security incidents is updated continuously to address the changing threat landscape.
9.2.	Notification of affected parties in the event of a data breach or major security incident	Vontobel strives to be fair and proportionate when considering the actions taken to inform affected parties regarding any major security incident or breach of personal data. If a confirmed major security incident or data breach is likely to put the rights and freedoms of data subjects at risk, clients and – if necessary – the competent authorities are informed by the CISO or DPO, in accordance with applicable notification obligations.
9.3.	Cyber insurance	Financial losses resulting from cyber incidents above a threshold agreed with operational risk management are transferred to an insurance company. The cyber coverage is regularly assessed and accordingly adjusted to address Vontobel's needs.

10 Business Continuity Management

10.1.	BCM/BCP processes	Vontobel meets the Swiss regulatory requirements for business continuity management (BCM), as prescribed by the Swiss Financial Market Supervisory Authority (FINMA). An emergency management process is defined in order to manage emergencies and crises. The business continuity process (BCP) is regularly tested and adjusted accordingly.
10.2.	Disaster Recovery Plans (DRP)	Vontobel has prepared an emergency and crisis concept with suitable playbooks and measures, which facilitates a rapid and targeted response in an emergency or crisis and maintains critical business processes even in the event of a crisis. Regular DRP tests, threat intelligence-related scenario cyber exercises and tabletop exercises are carried out to check the effectiveness of crisis management and disaster recovery measures and procedures.