Security Guidelines

Oct 2020

BAWAG Group Security Guidelines

Introduction

The protection of data / information and ICT systems and safeguarding the interests and privacy of our customers, employees, suppliers, other stakeholders and its good reputation is of utmost importance for BAWAG Group.

We recognize that only a comprehensive control system focusing on people, technology and processes can ensure the security of our group's valuable data / information assets.

BAWAG Group Security organization, controls and processes

BAWAG Group has constantly been committed to high information security standards which has been pursued with the timely implementation of the EBA Guideline on ICT and security risk management.

Executive body *Non Financial Risk and Environmental Social Governance Committee*	*The Non Financial Risk and Environmental Social Governance Committee is the company's executive body responsible for Privacy, ICT and Information Security.* *Voting Members of the committee:* *•All Managing Board Members (Chair: Chief Risk Officer; 1st Deputy: Chief Executive Officer; 2nd Deputy: Chief Financial Officer)* *• Head of Financial Crime Management & Compliance* *• General Counsel* *• Head of Strategic Risk Management* *• ESG Officers* *Non-Voting Members of the committee include representatives of the technology division.* *Other Division Heads or subsidiaries are invited for specific NFR and ESG topics in their entities.*
Chief Risk Officer	*The Chief Information Security Officer reports regularly to the CRO.*
Committee for Information Security (CfIS)	*BAWAG Group has additionally set up interdisciplinary committees and working groups to ensure comprehensive and consistent implementation of security measures, such as the regular Committee for Information Security (CfIS).*
Supervisory & Management Board	*Regular updates on protection of data / information and ICT systems on Supervisory Board and Managing Board level*

Chief Information Security Office	*The Chief Information Security Office (CISO) of BAWAG Group thrives to ensure confidentiality, integrity and availability of the group's ICT systems and information assets.* *BAWAG Group is continuously focusing on implementing and improving efficient and effective security measures. Security experts in a central ICT infrastructure team and IT operation teams in subsidiaries secure BAWAG Group's ICT systems, which are hosted and operated mainly by two ISO27001 certified data center partners.*
Group Chief Information Security Officer *Andreas Schaupp*	*The CISO Office is led by Group Chief Information Security Officer Dipl-HTL-Ing Andreas Schaupp MSc MSc MAS. He has received a Master of Science degree in Information Security Management. In addition, he has got various IT and security certifications like CISA, CISSP, ISO27001 Lead Auditor, CCIE and others.*
Education, certifications and experience	*Andreas has more than 10 years of experience as Group CISO in international banking groups. In addition, Andreas gives information security lectures at universities for applied sciences.*
Policies	*A comprehensive set of security policies aligned to the ISO27000 standards series provides the framework for the security goals, approach and measures of BAWAG Group.*
EBA Guideline aligned policy set	*The security policy documents cover overarching as well as specific securities topics, such as identity & access management or penetration testing. In 2020 the security policy set has been aligned with the 'EBA Guidelines on ICT and Security Risk Management.*
ICT and Security Risk Management	*Well known COBIT is the base for a comprehensive internal controls framework, which is in place to strengthen IT governance, including ongoing control reviews by the Internal IT Audit function, which are reported to the Managing Board.*
EBA Guideline aligned methodology	*To ensure security risk identification and mitigation, an 'EBA Guideline on ICT and Security Risk Management' aligned security risk assessment methodology for new internal and outsourced solutions is carried out.*
Certified Security experts	*The identified ICT security measures are carried out by certified security experts in the CISO Office and in the IT-Security operations teams.*

3rd Party Risk and Outsourcing Management	*External partners are assessed prior to onboarding by a comprehensive cross functional risk assessment. System and data access for external partners are handled very restrictively and is reviewed at least annually.*
Training & Awareness *All employees & contractors* *Professional development CISA, CISSP, ISO 27001*	*Various measures thrive to increase the awareness for security topics, such as security training for new hires, annual security awareness trainings for all employees and security information blogs for employees and customers (on BAWAG P.S.K. security portal). Also, staff from external ICT partners get a specific training on BAWAG Group's information security requirements.* *Regular training is mandatory for specialists in order to stay up-to-date with the changing technology landscape. IT and security staff are trained regularly, and they prove their expertise by holding various certifications including CISA, CISSP, ISO 27001 Lead Auditor CCSP and others.*
Contact to Authorities and Interest Groups *Cyber Threat Analysis*	*BAWAG Group is in regular contact and closely cooperates with authorities and interest groups to stay abreast of the latest IT and security trends and according regulations.* *Specialists collect information about current threat trends, threat agents and security attacks, analyze them and define security controls accordingly.*

Technology

State-of-the-art technology and services are used to keep BAWAG Group's internal and external security status at the expected high level.

Data Leak / Loss Prevention *Information classification & protection*	*BAWAG Group has a comprehensive information classification policy which considers all three security goals (confidentiality, integrity and availability). This policy is supplemented through strong technological solutions.*
Endpoint Security	*Where appropriate, various cryptographic measures are in place to ensure confidentiality and integrity of data. All end user devices (e.g. hard disk of PCs) are encrypted and the use of external media like USB sticks is restricted in order to prevent data leakage or loss.*
Encryption	*Data in transit over any public networks is encrypted. In addition, eMail, web and cloud usage has got security related restrictions and is continuously monitored.*
Spam and Malware Protection	*Modern Anti-Spam and Anti-Malware solutions combined with frequent awareness campaigns to educate users are in use to detect and prevent malicious software and behavior.*
Phishing Counter Measures	*In addition to awareness campaigns for customers, BAWAG Group uses a global Anti-Phishing service from a strong partner to identify and deactivate Phishing sites and alike.*
Network Security	*Various tools (incl. firewalls and IDS) and organizational processes are in place to secure data in transit through network segmentation, transport encryption and analysis for anomalies.*
Vulnerability and Patch Management	*For all systems BAWAG Group carries out ongoing vulnerability scanning with current tools to detect weaknesses in the large internal and external IT landscape.* *Detected vulnerabilities are handled in time (e.g. by patching) according to their criticality by internal IT experts and outsourcing providers.*
Security Monitoring	*Monitoring systems including a central Security Incidents and Event Monitoring (SIEM) system are in place. Log files from various IT components are sent to the central SIEM for correlation and real-time event notification.*
SIEM	*The SIEM is used to detect, analyze and react to anomalous activities indicating security incidents in real-time.*

Cyber security	To validate its Cybersecurity approach, BAWAG Group engaged a well-known Cybersecurity checking and rating service which confirms a solid Cybersecurity infrastructure of BAWAG Group (including our international entities). BAWAG Group experts monitor the rating results closely and act immediately on detected issues.

Processes

IT related processes in BAWAG Group follow the COBIT framework.

Access Control / Authentication and Authorization	The user lifecycle management includes defined processes for adding, changing and deleting user identities, accounts and their access rights.
Need-to-know or need-to-do principles	Access rights are provisioned according to need-to-know and need-to-do principles.
Password Security	Access to systems and applications is protected by unique user names and passwords which have to be in line with the defined password rules. For remote access multi-factor authentication is mandatory.
Regular reviews	Regular reviews of access rights are conducted at least annually and in the event of organizational changes.
Secure SW Development	A special security focus has been set for developing, implementing, operating, using and maintaining new internal or externally (incl. cloud) sourced ICT solutions to achieve not only an adequate level of security but also compliance with specific regulations like PSD2 and GDPR at any stage of the life cycle of ICT systems and solutions.
Secure coding training	To achieve that goal software developers have been trained in security coding technique and approach.
Data masking	In addition, data in non-productive environments such as test and development environments are masked accordingly to prevent potential misuse.
Security Compliance Security tests	Compliance with internal and external security regulations is checked by the CISO Office on an ongoing base and Internal IT Audit according to the annual audit plan. Such security compliance checks are carried out internally but also at external

	ICT sourcing and support partners (e.g. on-site assessments during data center visits).
Penetration testing	*BAWAG Group uses the specific know-how of (external) ethical hacking experts for regular penetration testing which is required according to financial market regulations and BAWAG Group's internal 'Penetration Testing Standard'-Policy. Results of penetration tests are used to further improve the security of tested systems.*
Incident Management	*Incident management follows a structured process involving all relevant parties and sharpened toward quick resolution.*
Security Incident Handling	*Handling of security incidents starts like other IT related incidents. After identification of a security incident, the incident handling proceeds according to the specifically defined security incident handling and reporting approach.*
Security Incident Reporting	*Security incident reporting in BAWAG Group follows a standardized approach. The CISO Office receives all security incidents, records them, supports incident resolution and reports to Management and authorities (if required).* *Major Cyber Security incidents are to be reported to the European Central Bank (ECB) immediately after detection. In addition, the Financial Market Authority (FMA), as national competent authority according to PSD2 'EBA Guideline on Major Incident Reporting', has to be informed in due time, whenever payment services are seriously affected.*
Lessons learned	*Incident management concludes with a comprehensive root-cause analysis.*

Business Continuity Management

Business Continuity Management (BCM) is the establishment and ongoing maintenance and further development of an efficient emergency and crisis management system. The aim is to ensure that important business processes are not interrupted or are only temporarily interrupted in critical situations and emergencies, thus securing the economic existence of the company in case of an event.

BAWAG Group's BCM framework includes the following points:

- Guidelines: The Business Continuity Policy serves as the main document for the divisions and subsidiaries and defines how critical business processes should be identified and addressed and how they should be planned for in the event of an emergency.
- Planning: In supplementary run books, different scenarios are created in order to be able to react efficiently and effectively in an emergency and take the right measures.
- Implementation and Operations: The emergency preparedness concept holistically includes all infrastructural, technical, organizational and personnel aspects with regard to all phases of the emergency management process.
- Performance evaluation: Regular desktop, emergency and disaster recovery tests ensure that the respective response and procedures can be carried out properly in case of an emergency.
- Improvement: A critical review as well as internal coordination and, above all, lessons learned sessions help to continuously expand and improve the emergency concept and its establishment.

Physical security

The focus of physical security is on the protection of people, values and objects. The integrated management approach and the interweaving of organizational, structural and technical measures result in a three-pillar model that can be flexibly adapted.

Security zones are defined and implemented according to the sensitivity of the values to be protected. By using access systems, authorizations are assigned and maintained as well as accesses are regulated and tracked. Depending on the level of security, the use of access controls is supported by alarm and video systems which indicate, clarify and document a security breach.

The use of security personnel for specific occasions and our own 24/7 security control centre maximize the chance of identifying and averting potential dangers at an early stage. This is supplemented by the training of employees on safety-relevant topics and the correct handling and disposal of sensitive data.

Based on the implementation of structurally relevant security specifications, the requirements for the integration of technical and organizational measures are created.