Julius Bär

INFORMATION SECURITY MANAGEMENT FRAMEWORK AT JULIUS BAER

Current cyber risk landscape

The ever-changing cyber risk landscape affects individuals and organisations alike due to today's dependency on information technology and its integral link to critical infrastructure, making these systems attractive targets for cyberattacks.

Security risks in information technology have always existed, however, in recent years threats from the cyber realm have dramatically increased in number and sophistication. Attackers use the internet as an entry point to compromise organisations. Such attacks may utilise a variety of activities such as social engineering via communication channels (such as e-mail and voice phishing), technical means (e.g., malware) or leveraging existing vulnerabilities and weaknesses within systems and applications. The underlying motives can be diverse in nature, ranging from financial gains, espionage, to ideology and grievances.

Organization and governance of information and cyber security

Julius Baer has consistently invested in organisational and technical security measures, to be able to identify, manage, and address current and future cyber risks.

All employees receive regular updates on current threat situations and are trained on how to identify and deal with security risks, particularly with social engineering attacks. Technical components are maintained by Information Technology professionals and are regularly updated and hardened against cyberattacks. This approach allows user awareness and the security posture to remain at a high level.

The Information Security and Technology Risk organisation is led by the Group Chief Information Security Officer (CISO), who is in the reporting line of the Chief Risk Officer (CRO).

Julius Baer is operating a dedicated Cyber Fusion Center (CFC). In its global approach, the CFC combines the assurance and continuous improvement of detective and protective security measures with the professional detection of and response to cyber threats by its Security Operations Center (SOC). Julius Baer's attack surface and new developments in the threat landscape are continuously assessed by the Cyber Threat Intelligence (CTI) team. All security professionals of Julius Baer hold relevant qualifications, possess long-term experience in risk management, information and cyber security and maintain a high level of know-how by participating in continuous education and training.

Physical access to data centres and office spaces is based on an employee's authorisation level and responsibilities, regulated by the Physical Security team.

By maintaining close contact and collaboration with peer organisations, security user groups, threat intelligence providers and law enforcement agencies on a local, national and international level, Julius Baer stays ahead in the race against cybercrime.

Like any organisation, Julius Baer also relies on services from third-party providers. Before their engagement, these providers undergo a rigorous due diligence process, ensuring each provider is vetted to meet Julius Baer's high security requirements. Additionally, providers must comply with reassessments of their security posture on a regular basis.

Information security management framework

A well-defined and maintained risk management process aims to identify cyber threats in a timely manner, implement effective mitigating measures and appropriately evaluate and deal with newly evolving threat scenarios. This includes the monitoring of known threats on a daily basis by dedicated systems and specialised people, as well as the analysis of long-term developments and trends (e.g., political, legal, economic, sociocultural, and technical aspects).

Regulatory frameworks require a high level of maturity in ensuring the security and privacy of data and provide guidance for organisations like Julius Baer on how to respond to cyber threats.

On this basis and with reference to the international security standard ISO/IEC 27001, Julius Baer has implemented an information security management framework which allows for an effective and efficient execution of security measures. These measures are constantly monitored, and corrective action is initiated if a measure does not meet its defined objectives.

The overall framework and its components (e.g., policies, processes, security controls) are subject to regular reviews and assessments as mandated by law and regulators and executed by internal and external auditors as well as certified security firms. This is also reflected in the annual ISAE 3000 type 2 report, demonstrating Julius Baer's commitment to security, transparency and accountability.

IMPRINT
This content has been produced by Bank Julius Baer & Co. Ltd., Zurich, which is authorised and regulated by the Swiss Financial Market Supervisory Authority (FINMA).

IMPORTANT LEGAL INFORMATION
The information and opinions expressed were valid at the date of writing, and may be based on numerous assumptions and, thus, subject to change without notice.

This content serves for information purposes only and is not intended as a legal, accounting, or tax advice, or an offer, or an invitation to buy or sell any financial instruments and/or products. Furthermore, it does not constitute a personal recommendation or take into account specific personal circumstances (e.g., investment objectives, financial situation, or investment strategies). Although the information is trusted to be accurate and complete and data has been obtained in good faith from sources believed to be reliable, no representation or warranty, expressed or implied, is made in this respect. To the extent permitted by applicable laws and/or regulations, Julius Baer accepts no liability whatsoever for any claims for loss or damages of any kind arising directly or indirectly from this content (including acts or omissions by third parties such as auxiliary persons and/or agents of Julius Baer).

© Julius Baer Group, 2025