Security
Is Our Business
Security is important at SIX. We handle risks with great focus and care. One of the main (cyber) risks is to think they don’t exist. Trying to cover all potential risks is itself a main risk. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think about data, but also business service integrity, awareness, customer experience, compliance, and reputation.

Thomas Koch
Chief Security Officer

“Security is Our Business

SIX is the Swiss financial center’s backbone and of central importance for the Swiss financial value chain, which represents a highly integrated infrastructure consisting of the trading platform (Swiss Exchange), the central counterparty for clearing, securities settlement, payment settlement and its contributing units, such as for the dissemination of financial information.

Powerful platforms, state-of-the-art technology, and lightning-fast systems. This is infrastructure of SIX. The result is information and data where you need it, when you need it. For securities valuation, exchange trading, securities processing, payments and financial information dissemination, we provide you with speed and efficiency. The systems of SIX process vast quantities of information quickly and reliably every single day. As a customer, you can rest assured that SIX and its systems can withstand extreme stress situations, which means you can continue with your business uninterrupted.

SIX is subject to the supervision of several regulatory bodies and aims to run its business services fully compliant to the corresponding requirements.

SIX is a high-reliability organization and is committed to continuous improvement. The self-driven optimization of existing processes and preparations and the invention of new ones in order to adapt in an ever-changing environment are prerequisites for success, not only in the field of Business Continuity Management.

SIX takes responsibility:
- for compliance with a number of standards and financial regulations
- for implementation of Privacy by Design
- for guaranteeing a secure and private financial market infrastructure and operation
- for ensuring the identification and evaluation of technology risks
- for implementation of leading cyber security solutions to avoid cyber attacks, minimize their impact and prevent the failure of key systems
Three Lines of Defense

Our risk and security organization applies to the entire company. The organizational unit Risk, Legal & Compliance, led by the Chief Risk Officer (CRO), defines areas of responsibility, methods, processes and reporting for risks at SIX. At the same time, the team acts as the second line of defense in a “three lines of defense” model, which has become standard practice in the financial sector.

**First Line of Defense**
The first line of defense lies with the business units. It is at this level that employees need to recognize risks and weigh them up appropriately in their day-to-day work.

**Second Line of Defense**
The uniform company-wide risk and security organization forms the second line of defense. It assists and supports the first line with the monitoring and control of critical topics. The team handles the reporting of financial and non-financial risks, risk analyses and the central insurance portfolio.

**Third Line of Defense**
The Board of Directors and the internal and external auditors constitute the third line of defense. They are responsible for independently monitoring and controlling the risks faced by SIX. At the same time, they monitor the internal organization of risk management.
Cyber attacks are a reality that we face in our daily business. It is not a matter of whether threat actors can successfully attack, but rather when they will. The crucial factors are whether we are prepared to react timely and correctly. Our company-wide dedication to maintaining a high-level, cyber security-driven risk management framework is of strategic value for successfully defending the assets of SIX against such threats. The ‘digital crown jewels’ are at stake here. Technical counter-measures alone are not enough to protect us from cyber threats. Our goal is to develop a resilient risk management framework that shapes the company risk culture. The key points for setting cyber security standards are collaboration within the company and adequate risk awareness within the organization’s employees.
Cyber Defense

Cyber Defense (CD) assists in the ability to protect, monitor, analyze, detect, and respond to unauthorized activity within the managed enterprise assets of SIX. CD protection activity employs information assurance principals and includes deliberate actions taken to modify an assurance configuration or condition in response to a cyber alert or threat information. CD development of the Security Incident Response Team (SIRT) furthers the organization’s assurance level by providing oversight and monitoring of all serious and above incidents.

Cyber Defense (CD) actively contributes to SIX by minimizing the impact of cyber attacks and assisting in preventing cyber security incidents. CD supports the governance process, while maintaining oversight of security investigations, vulnerability management, use case development, and compliance assurance. Other areas of responsibilities include oversight of cyber security processes for the second line of defense, as well as the examination of security baselines and security gaps for continuous improvement. CD specializes in techniques and requirements for the organization’s cyber security monitoring processes.

CD, through the SIRT capabilities, provides a professional view while challenging testing results and effectiveness. With the establishment and company-wide support of a threat intelligence structure, CD has increased the organization’s observation of the global threat environment. Through red-teaming and penetration testing, CD can provide sound assessments regarding organizational risks and the threat landscape.

In addition, CD-SIRT provides the organization’s overseers with internal forensic analysis and external forensic case management.

* -in implementation
SIX has a solid, trained crisis organization that can deal with a crisis situation in an effective and timely manner. Our crisis organization follows best practice in crisis management and can respond to various crisis scenarios in a flexible manner. In addition, the crisis management organization prepares for potential crises through training sessions with a hands-on, appropriate and realistic approach to potential events or identified shortcomings.

Beni Hurschler
Head Crisis Management, BCM & Physical Security

Crisis and Business Continuity Management

The Business Continuity Management (BCM) framework of SIX covers all elements of the generic model outlined by ISO 22301 standard. The policy is the founding document for all activities, and it outlines the goals and scope of the Crisis and BCM program of a company. Alterations and changes (driven by regulators, technology change, customer needs, market needs) must be integrated into the BCM policy to guarantee the effectiveness of the BCM program.

SIX has developed a dedicated BCM policy, closely aligned to its risk policy and security policy. The primary goal of the BCM policy of SIX is to ensure the continuation or the timely recovery of business services according to the availability requirement and prioritization of SIX and to enable an effective and prompt emergency or crisis management response. Our BCM program is run by the Corporate BC Manager, who reports to the Chief Security Officer. Along the BCM life cycle, SIX works out Business Impact Analyses (BIA). For each business process, we determine downtime and criticality. We systematically identify and align interdependencies with the established business continuity strategies. For all relevant business processes, we prepare business continuity plans and test them on a regular basis.

Physical Security

Physical security as an important component of the integral security concept and risk management framework of SIX distinguishes in general between the two main pillars of personal safety and object security. This covers all aspects of organizational, conceptual, legal, physical, technical and personnel safety issues regarding buildings, assets, and information emanating from and within SIX.

Within this area, the management of physical access plays an essential part. Premises and facilities that are used or operated by SIX are divided into access zones. The degree of compartmentalization reflects the protection need of the business located within the access zone. In regular audits, we check compliance with the guidelines, which are coordinated with the Physical Security Officer. We retain video recordings and access data under consideration of the data privacy act. Access is restricted to authorized personnel.

We have identified all critical locations and business functions, and contingency arrangements are in place. SIX ensures that its services operate in accordance with their availability objectives. For services with very high availability requirements, the necessary organizational and technical prerequisites are put in place to ensure their availability even in emergency and crisis situations.

To guarantee uninterrupted operational work as part of the Swiss financial infrastructure, data centers of SIX feature independent and redundant power lines by default. In case of an outage of both lines, UPS is provided with batteries and diesel generators on premise. In case of a severe long-lasting power outage at one site, we switch operation to the backup data center.
The IT Risk & IT Control Framework supports SIX to comply with regulatory requirements, maintain a strong and secure operational performance and increase shareholder value. As a second line of defense function, we foster the first line of defense in identifying and managing the IT risks and IT controls to meet the business objectives of SIX. The comprehensive SIX IT Control Framework is designed to protect the confidentiality, integrity and availability (CIA) of our sensitive information and environments.

Gaudenz Barblan
Head IT & Security Risk

**IT Risk and IT Control Management**

The IT Risk and IT Control Management of SIX is integrated in the enterprise wide risk management framework, processes and organization built on two pillars:

The main pillar of the concept is owned and maintained by the Chief Risk Officer (CRO). Gaudenz Barblan, the Head IT & Security Risk, maintains a central risk repository for IT and security risks. A team of experienced IT Risk and IT Control specialists oversees the overall IT risk situation, according to the risk appetite of SIX. Furthermore, it is in charge of handling the IT risks within SIX and supervising the mitigation measurements.

The second main pillar is the definition and governance of the IT Control Framework to ensure adequate governance and company-wide visibility of the IT Risk and Control Framework. The IT & Security Risk team provides support for IT and security risk topics. The team supervises IT projects and initiatives from a project risk point of view. On top of that, it defines and maintains firm-wide IT and security risk management, control processes, related standards as well as methodologies.

**Internal Control System**

The Internal Control System (ICS) is a key management framework for operational risk that comprises systemically structured technical and organizational rules as well as controls to ensure compliance with guidelines. Furthermore, it prevents threats and damage to the company. It documents all business-relevant processes, risks, as well as systems along with controls, and it ensures the adequacy and effectiveness of controls.

As a subset of the Internal Control System, Information Technology controls are specific activities performed by persons or systems designed to ensure that business objectives are met. The IT Control Framework at SIX is based on the ISF SoGP (Information Security Forum, The Standard of Good Practice for Information Security 2018).

The IT control objectives relate to the confidentiality, integrity, availability and non-repudiation of information.

IT Risk Management, in cooperation with various stakeholders (e.g. service – and application owners, project managers), ensures the identification and evaluation of technology risks as well as the definition of appropriate measures and controls. IT Risk Management ensures the transparency of existing risk situations and visualizes risks in an appropriate form for the various stakeholders.
As the Information Security Partner, we develop the security policy framework for SIX. In cooperation with business and corporate functions, we support its implementation by first line of defense through consulting, project advice and reviews. We ensure that the security aspects of the group standards are implemented globally.

The operative processes of SIX are based on best industry practice. Processes for incident, problem, change, performance, configuration and capacity management rely on ITIL standards. Security management is based on the ISF Standard of Good Practice, ISO/IEC 2700x family and NIST recommendations. Per Business Unit or Corporate Function, a dedicated Information Security Officer takes care of all IT Risk and Security Management as the interface between business and IT for all security related topics. He or she ensures that the requirements and pain points of the business are considered within IT projects and operations, as well as transparency on security issues, risks and incidents.

SIX performs regular penetration testing by independent external companies on its perimeter and for critical internal applications. Within the Software Development Life Cycle (SDLC), security is reviewed on various layers, for classic “waterfall” projects as well as for agile development. Besides the constant documentation of security measures, SIX executes security assessments for projects and (repeatedly) during life cycles of applications and infrastructure. Based on risk-oriented decisions, we track mitigation measures and verify their effectiveness. SIX keeps an eye on any deviation from internal or external regulations or policies, with an integrated exception management.

The CSO and the Corporate Security teams maintain a security awareness strategy and training activity plans for all SIX employees. The security awareness program contains multiple means of communication, starting with an introductory meeting upon hiring (the “Welcome Day”) and continued communication, by classroom and computer-based trainings, pocket guides and intranet information. These measures cover topics on security dos and don’ts for daily work, guidance on regulatory topics, among others. e-learning modules on directives and specialized topics may be assigned to all or only to relevant employees. The e-learning tool supports managing attendance, reminders, etc.
SIX is required to adhere to regulatory requirements such as PCI-DSS, FINMA, etc. The needs of its customers, however, are more important. SIX therefore has its principal focus on compliance with customer requirements to offer and deliver the best service quality.

Compliance

Depending on the Business Unit, SIX is required to perform annual assessments and reports for compliance, among others to PCI-DSS or SWIFT. Additional assessments result from regulations of the Swiss National Bank, FINMA and other security-related standards worldwide.
SIX as the operator of a competitive infrastructure for the Swiss financial center has developed holistic and company-wide security solutions to guarantee the highest efficiency and security both for SIX and for clients, who place a trust in solutions of SIX.

Summary