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

SIX

SIX provides and operates stable and efficient infrastructure for the Swiss and Spanish financial centers, thus ensuring access to the capital markets and the flow of information and money between financial market players. We are the Swiss competence center for payments and other banking services. Moreover, we provide reference, pricing, and corporate action data to customers around the world, and also offer regulatory services and indices.

SIX connects financial market participants in Switzerland, Spain, and around the world. We are owned by more than 120 national and international financial institutions. They are the main users of our infrastructure, and our most important clients.

Security Is Our Business

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

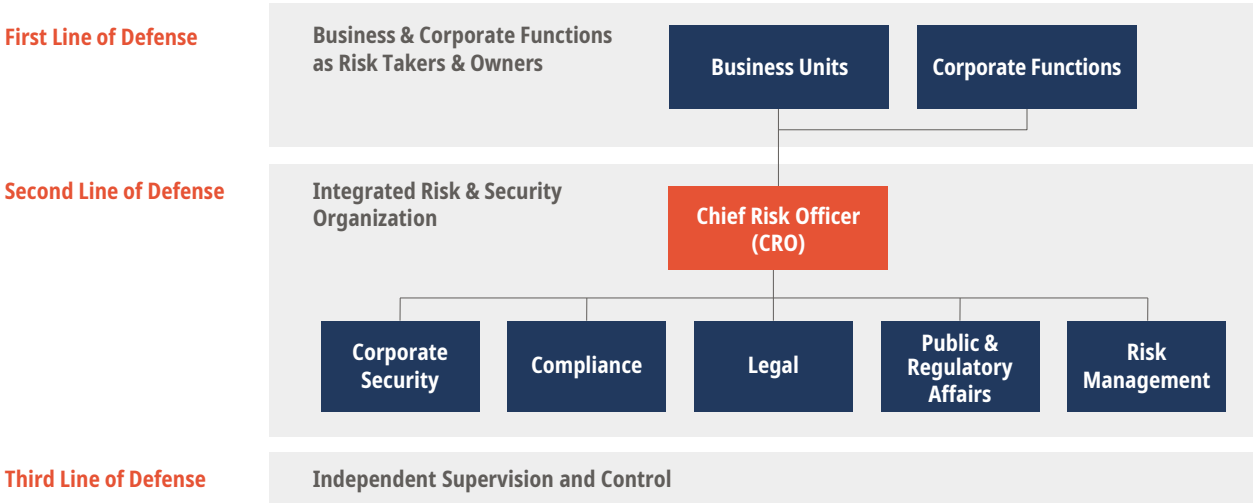
Three Lines of Defense

Our risk and security organization applies to the entire company. The Corporate Function 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.

The first line of defense is found in the Business Units and Operations. In this level, employees of SIX identify risks, threats, and vulnerabilities. Their mission is to ensure the business is informed and that counter-measures are appropriately set in place.

The second line of defense maintains and determines the organization's Risk Management Framework. Core responsibilities include oversight of the first line of defense with the monitoring and control of critical topics. The teams also handle the reporting of financial and non-financial risks, risk analyses, and the central insurance portfolio.

The third line of defense comprises of the Board of Directors and both internal and external auditors. They are responsible for independently monitoring and controlling the risk appetite established by SIX. The third line of defense monitors the internal organizational risk management framework.



↪ **Report a Cyber Security Incident:**
If you believe that you have discovered a vulnerability in a service from SIX or have a security incident to report, please get in touch.
https://www.six-group.com/en/contacts/new-services/soc.html

↪ **SIX SIRT Team Charter RFC 2350:**
https://www.six-group.com/dam/download/cyber-security/six-sirt-team-charter.pdf

> The cyber security organization supports and helps secure SIX through the management of different cyber security programs and the delivery of different security platforms and security services, focusing on detection & incident response (SOC & SIRT), threat intelligence, vulnerability management as well as IT-Security compliance management. We are the international center of competence for cyber security at SIX.

Daniel Coray
Head Cyber Security
soc@six-group.com

Cyber Security

- **Security Operations Center (SOC)**
- **Incident Response**
- **Threat Intelligence**
- **Threat Hunting**
- **Engineering & Operations**
- **Vulnerability Management**
- **Purple Teaming**
- **IT-Security Compliance**
- **Forensic Analysis**
- **Use Case Development**

Security Operations Center (SOC)
services like:
- Monitoring & Triage
- Security Incident analysis
- SOC Platform Engineering & Operations
- Security Information and Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Security Orchestration, Automation and Response (SOAR)
- Malware detection and Sandboxing
- Threat Intelligence & Sharing Platforms

Security Incident Response Team (SIRT)
services like:
- Incident Response
- Threat Intelligence
- Threat Detection & Hunting
- Forensic Analysis and Security Advisory

Platform Security Services
services like:
- Log Management
- Intrusion Detection Systems (IDS)
- Vulnerability Management and Baseline Security (SCB) & File Integrity Monitoring (FIM)

IT Security and IT Compliance Management
services like:
- Information Security Program & Roadmap
- IT Security Reporting
- PCI DSS Compliance Service Delivery
- Reporting and Control Testing
- IT Security/Compliance Operational Assurance

> In cooperation with Business Units and Corporate Functions we support the security policy framework 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.

Alexander Bösch
Head Information
Security Partner

Information Security – the Partnership to Business

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 security related topics as the interface between business and IT. 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.

Security Awareness, Penetration Testing, Security Assessments and Exceptions at a Glance

SIX performs regular penetration testing by internal team or independent external companies. 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 Chief Security Officer (CSO) and the Corporate Security teams maintain a security awareness strategy and training activity plans for all SIX employees that contain 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, awareness campaigns, security related lectures 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. Through phishing exercises we continuously leverage awareness among our colleagues and raise the security culture of SIX.

> A cyber security program must have many parts to be effective. The most robust will feature a mature Offensive Security team to identify issues before someone else does and find effective solutions to address problems. Ultimately the Cyber Controls Team provides high-quality, innovative cyber security assessments, solutions & guidance that will reduce (cyber security) risk across SIX.

Alexander Hagenah
Head Cyber Controls

Cyber Controls

At SIX, it's our mission to ensure that our customers' data is kept secure from adversaries internally and externally. To support this mission, we employ a robust, multi-faceted Security Team, part of which is made up of an Offensive Security Team. Offensive Security is focused on discovering vulnerabilities within SIX's infrastructure, vendors, and people.

Offensive Security takes a more holistic view of the company from an outsider's perspective, not just looking at one service but across the entire organization to find various routes into our environment.

In short, it's the Offensive Security Team's job to assume the mindset of a hacker, and find vulnerabilities before an adversary can.

Cyber Security

Review
- Conducting of internal penetration tests to review application and system security
- Coordination of global penetration testing through trusted external partner
- Implementation of a reward program to eliminate security vulnerabilities within SIX

Enhancements
- Participate in and setting up exercises in collaboration with SIX cyber defense departments to strengthen their cyberthreat monitoring, detection and response capabilities
- Assess the maturity of our application and infrastructure security through technical deep dive assessments
- Guide and sharpen the security processes based on outcomes during reviews

Advisory
- Development of a holistic approach to cyber security and securing SIX assets
- Review of security strategies
- Being a trusted & independent interdepartmental security advisor

> The IT and Security Risk 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 and security risks as well as the definition of appropriate measures and controls to meet the business objectives of SIX. The comprehensive framework is designed to protect the confidentiality, integrity and availability (CIA) of our sensitive information and environments.

Roberto Ranaldo
Head IT & Security Risk and Governance

IT and Security Risk Management

The IT and Security Risk 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). The IT & Security Risk and Governance team enables the Corporate IT function to maintain a central risk repository for IT and security risks (including Cyber, Physical Security, BCM and Crisis Management). 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 and security risks within SIX, supervising the mitigation measures and report a holistic view of these risks to senior executives.

The second main pillar is the support and challenge of the first line of defense function in defining, implementing and maintaining IT controls for IT and Security risks as part of their IT Internal Control System (IT ICS) to ensure adequate governance and company-wide visibility of the IT and Security Risk Framework. IT controls are specific activities performed by people or systems to ensure that business objectives are met. The goal is to achieve the requirements defined in the SIX Security Policies and Regulations regarding confidentiality, availability, and integrity of applications, IT infrastructures and the involved data. The aim of the IT controls is to have clear roles and responsibilities, avoid control gaps and duplications, increase baseline security and standardize reporting.

The SIX IT controls for IT and Security Risks are deviated from the Information Security Forum (ISF) "The Standard of Good Practice for Information Security 2020".

SIX Security Policy Framework

The IT & Security Risk and Governance team maintains the SIX Security Policy Framework, which contains all documents of the internal law related to integral security, such as the Security Policy, directives and regulations. They provide the basis for adequate protection and specify the essential safeguards for integral security. Furthermore, these documents form the basis for the SIX IT Control Framework.

The team ensures that these documents are reviewed regularly and that SIX employees are familiar with them.

The IT & Security Risk and Governance team provides support for IT and security risk topics in general. The team supervises IT projects and initiatives from a project risk point of view. On top of that, it defines and maintains firmwide IT and security risk management, control processes as well as methodologies.

“Cloud computing, Outsourcing, and Shoring can result in higher efficiency, quality and lower costs. While the benefits are widely recognized the risks such as compliance, legal, reputational, operational or information security risk must be understood and managed properly. To mitigate these risks a robust Supplier Risk Management framework is implemented and maintained.”

Nicolas Berger
Head Supplier Risk Management

Supplier Risk Management

The primary goal of Supplier Risk Management (SRM) is to manage supplier risks throughout the sourcing lifecycle, while enabling the business to make use of the benefits of suppliers and cloud services. The due diligence performed before entering into an engagement ensures that risks are identified early, mitigated and the residual risk is within the risk appetite of SIX. During contract lifecycle a risk-based approach to assessing and managing the engagements helps to focus on the relevant risks.

The increasing use of shoring, outsourcing and cloud computing brings great opportunities for SIX, but it also poses new type of risks. But these can be managed: legal and regulatory requirements as well as risks in the areas of compliance, information or cyber security, and business continuity, as well as strategic, financial, and reputational risks can be identified, evaluated, and managed with a well-established supplier risk management program. The Supplier Risk Management (SRM) team maintains the Supplier Risk Framework and manages the SRM process. The SRM Process assists in managing and monitoring the risk exposure resulting from consuming services or products from 3rd party suppliers, shoring or into the cloud.

The Supplier Governance Board (SGB) provides guidance to the process, defines the required level of supplier due diligence to be met and approves new engagements with suppliers. The SGB consists of various control functions, such as Compliance, Information Security, Enterprise Architecture, Risk, Procurement, Global Business Solutions Head and SRM.

“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 crisis 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 Management & Business Continuity Management

In order to ensure our services even during extreme events, SIX operates a Business Continuity Management Program according to the ISO 22301 standard, which makes a significant contribution to the stability, reliability and availability of the Swiss and Spanish financial centres as well as the globally provided services of SIX. If damage, destruction or loss of important interests and values of SIX are at risk or have already occurred, key tasks cannot be fulfilled or the existence is endangered and/or if the proper management structure and procedure and decision making process are disturbed or made impossible, then our Crisis Management comes into force.

SIX has a crisis organization, with which crisis situations national or abroad, can be dealt with effectively. The crisis organization of SIX is responsible for the crisis management until the proper conditions are restored and is linked with the Interbank Alarm and Crisis Organization (IACO) of the Swiss National Bank (SNB).

SIX has developed a dedicated Business Continuity Management (BCM) Policy, closely aligned to its Risk Policy and Security Policy. The primary goal of the BCM regulation of SIX is to ensure the continuation or the timely recovery of critical business services according to the availability requirement and prioritization of SIX. The BCM Program of SIX is integrated in the three lines of defense model, which has become standard practice in the financial sector. The Business Units and Corporate Functions form the first line of defense. In each Business Unit and Corporate Function, a Business Continuity Manager, supported by technical staff, is responsible for the implementation of BCM according to company-wide standards. Within Corporate IT, an IT Continuity Manager is responsible for implementing the IT Service Continuity Management (ITSCM). The BCM and ITSCM life cycles are completely run through once a year.

Physical Security & Health, Safety and Environmental Protection

Physical security comprises all organizational, structural and technical safeguarding measures and concepts aimed at protecting people, buildings, perimeters and supply systems as well as the corresponding assets. As an important component of the integral security concept of SIX, it is closely aligned with the Risk and Security Policy. Our requirements at group level are aligned to specifications formulated in ISO/IEC 27001 Standard and the Payment Card Industries Data Security Standard (PCI DSS) in the field of Physical Security as well as for Health, Safety and Environmental Protection Assessment on OHSAS 18001 and ISO 45001 respectively.

Physical Security is an interaction of all organizational, structural, and technical security measures and concepts required

- to guarantee the well-being of all employees, guests and customers of SIX in all premises and facilities;
- to protect valuables and information of our organization as well as premises and facilities themselves as well as all mobile and immobile property contained therein;
- to ensure uninterrupted business operations and high availability of all infrastructure components.

The Health, Safety and Environmental Protection System (HSE) is an important part of the integral safety concept of SIX and

- addresses risks in the context of SIX employees and their workplace environment;
- aims to minimize risks and potential damage regarding the health and integrity of employee, guests and customers of SIX;
- is congruent with the content and objective of personnel security stated in the SIX Security Policy.

“We trust in our Security Model and with the replication of the SIX Security Concept in Spain we add value in our organization both from a local and a global perspective.”

Jesús Romero de Pablos
Manager of Corporate Security Spain

Corporate Security Spain

After the takeover of BME, SIX has replicated the SIX Security Concept in Spain integrating the Spanish Security teams in the SIX Model. This model is replicated with dedicated teams working in a coordinated manner and in constant communication with the central SIX teams to ensure the independency and reaction capacity taking advantage of the capacity and experience of the rest of the teams.

BCM, Physical Security, Health & Crisis Management
With a dedicated team and in alignment with local regulations, we apply the SIX Integrated Security model for the protection of people, buildings, perimeters and supply systems. In terms of Spanish Business Continuity team and BME bodies are fully integrated in the SIX Crisis & Emergency organization to ensure the resilience and recovery capacity of the critical processes both from local and central perspective.

Security Risk and Governance
One group one regulation. In coordination with SIX’s central team, we collaborate in the definition of the regulatory framework to ensure its alignment also with local as with European regulations.

Information Security
With a dedicated local team in constant communication with SIX’s central Information Security team we support the first line of defense in the implementation of the security policy framework and group security standards throgh consulting, security reviews or project assurance between others.

Supplier Risk Management
Spanish Supplier Risk Management function is integrated under SIX one with dedicated staff focused in the following and assessment of the Spanish companies suppliers in accordance with the Spanish Company requirements and following the SIX standards.

Security Testing
New Security Testing group is also integrated in the Spanish security organization with staff dedicated to develop penetration test, red team exercises etc. to ensure the security coverage of the Spanish solutions and infrastructures.

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, CNMV and other security-related standards worldwide.

SIX is required to comply and to adhere to international standards as CPMI-IOSCO, NIS, SWIFT CSP, PCI-DSS, MiFIDii, MiFIR, CSDR and EMIR as well as to regulators obligations (FINMA, CNMV, ESMA and others). The needs of its customers, however, are even more important. SIX, therefore, has its principal focus on compliance with customer requirements to deliver the best and safest service quality.

Summary

SIX, as the operator of a competitive infrastructure for the Swiss and Spanish financial centers, 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.

SIX
Pfingstweidstrasse 110
P. O. Box
CH-8021 Zurich
Switzerland

BME
Plaza de la Lealtad, 1
28014 Madrid
Spain