# 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. Thereby, it ensures access to the capital markets and both the flow of information and money between financial market players. We are the competence center for payments and other banking in Switzerland. 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.

### We invest in our Cyber Security Organization

The systems of SIX are designed for high resilience. The business continuity management ensures that its services remain available and functional or can be rapidly restored – even in a crisis. Business continuity plans for all critical business processes are in place and tested regularly.

### Swiss Financial Sector Cyber Security Centre

SIX is a founding member of the Swiss Financial Sector Cyber Security Centre, founded in April 2022. The association, under the lead of the Swiss National Cyber Security Centre, promotes the exchange of information among financial market actors and improves cooperation on preventive, sector-wide measures and crisis management. SIX will continue to support the Swiss Financial Sector Cyber Security Centre to achieve its goals.

## Security Is Our Business

**SIX is subject to the oversight of several regulatory bodies and is committed to providing its business services in full compliance with regulatory requirements.**

As a high-reliability organization, we are committed to continuous improvement. As a result, we are continuously enhancing our global cyber security posture as part of our security strategy. To ensure business alignment, the Business Information Security Officers (BISO) act as a link between the security units of the various departments. SIX will continue to address the growing cyber threat landscape by continuing the successfully launched initiatives and working in line with the Information Security Strategy.

### SIX takes responsibility:

- for compliance with a number of standards and financial regulations
- for the 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
- to deploy cutting-edge cyber security solutions aimed at preventing cyber attacks, mitigating their impact, and safeguarding critical systems from failure

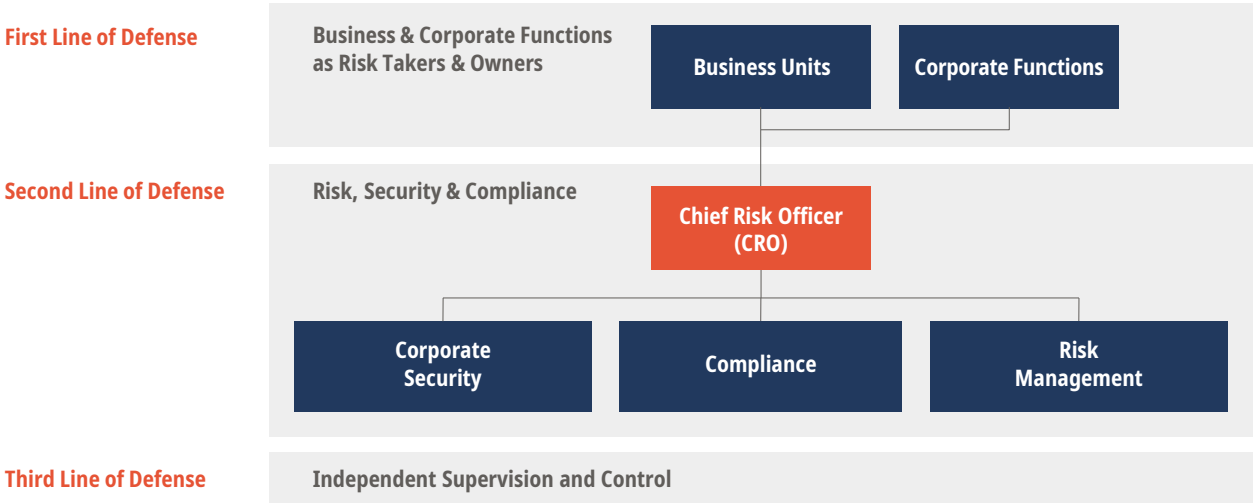
# Three Lines of Defense

**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 that 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/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 department is dedicated to bolstering the defenses of SIX by managing various cyber security projects, initiatives and providing a range of security platforms and services. Our primary focus areas include detection and incident response (SOC), cyber threat intelligence, and vulnerability management. Serving as 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)**
- **Security Monitoring & Incident Response**
- **Cyber Threat Intelligence**
- **Threat Detection & Hunting**
- **Engineering & Operations**
- **Vulnerability Management**
- **Purple Teaming**
- **Forensic Analysis**

**Security Operations Center (SOC)**
services:
- Security Monitoring & Incident Response
- Threat Detection & Hunting
- Vulnerability Management
- Cyber Threat Intelligence
- Forensic Analysis
- Blue Teaming
- International cooperation and engagement

**Cyber Security Technologies**
services:
- Security Information and Event Management (SIEM)
- Logging Platform
- Endpoint Detection and Response (EDR)
- Security Orchestration, Automation and Response (SOAR)
- Security Sandboxing
- Threat Intelligence Sharing Platforms
- Hardening / Security Configuration Baseline & File Integrity Monitoring
- Vulnerability Scanning Platform

**IT Security Strategy & Advisory**
services:
- Security Advisory
- Security Improvement Management
- Cyber Defense Strategy
- Information Security Strategy Management

> 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. Through phishing exercises we continuously leverage awareness among our colleagues and raise the security culture of SIX.

> At SIX, we believe a comprehensive cyber security strategy hinges on anticipation and action. The Cyber Controls team proactively uncovers vulnerabilities and crafts solutions, ensuring our defenses are always a step ahead. Through innovative assessments and strategic guidance, we are committed to substantially reducing cyber security risks as well as enhancing cyber security resilience at SIX.

Alexander Hagenah
Head Cyber Controls

# Cyber Controls

**A Proactive Cyber Security Strategy**
Cyber security threats evolve with alarming speed and complexity. Recognizing this, SIX Group has established an offensive cyber security team, where we actively identify, evaluate, and neutralize potential threats. Our approach is founded on the principle of anticipation, employing ethical hacking methodologies to simulate and understand the tactics of real-world adversaries. This proactive stance ensures that SIX remains resilient against cyber threats, prepared to face tomorrow's challenges today.

Our mission is straightforward yet ambitious: to deliver comprehensive cyber security evaluations, solutions, and guidance that significantly mitigate risk. By continuously enhancing our expertise and embracing advanced technologies, we aim to not only respond to cyber security threats but to preempt them.

**Penetration Testing and Adversary Simulation**
Central to our strategy is rigorous penetration testing. By emulating real-world attacks on SIX's IT infrastructure, we uncover and address vulnerabilities within applications, platforms, and networks. This process is critical for assessing the resilience of our security measures and guiding the prioritization of vulnerability remediation, thus strengthening SIX's security posture.

We further refine our defense mechanisms through adversary simulation and Purple Teaming exercises. By replicating the actions of cyber threats, including advanced persistent threats (APTs), we test and enhance our preparedness for potential incursions. Purple Teaming, the integration of offensive and defensive strategies, fosters a comprehensive evaluation of our incident response capabilities. This collaboration not only identifies security shortfalls but also enriches our cyber security knowledge.

**Engagement and Advisory**
Our commitment extends beyond internal strategies. Through our Bug Bounty Program, we engage with the global security research community, inviting external ethical hackers to uncover vulnerabilities. This initiative reflects our belief in leveraging collective intelligence to enhance security, offering a cost-efficient method for timely threat resolution.

Our advisory services provide strategic insights and tailored recommendations to strengthen SIX's cyber security posture. By advising on industry best practices and endorsing specific security solutions, we aim to equip SIX with the tools and knowledge necessary to effectively mitigate cyber security threats.

Through our proactive and collaborative approach, we aim to enhance SIX's cyber security resilience, ensuring SIX remains ahead.

“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”.

## 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 to ensure operational resilience. 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 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 addition, the Crisis Management organization prepares for a 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, Operational Resilience & Business Continuity Management

**In order to ensure our services, even during extreme events, SIX operates an Operational Resilience program, which includes Risk Management, Business Continuity Management, IT Service Continuity Management and Crisis Management. These management systems make a significant contribution to the stability, reliability and availability of the Swiss and Spanish financial centers as well as the globally provided services of SIX.**

If an incident makes the orderly processes for decision-making at the level of the entire group impossible, our Crisis Management comes into force.

The Crisis Organization of SIX is responsible for the crisis management until the proper conditions are restored. This includes the coordination with regulators and other bodies of the financial center (e.g., the Interbank Alarm and Crisis Organization (IACO) of the Swiss National Bank (SNB), the Swiss Financial Center Cyber Security Center (FS-CSC) or the Comisión Nacional del Mercado de Valores (CNMV). As an integral part of Operational Resilience, SIX operates a Business Continuity Management (BCM) system as well as a complementary IT Service Continuity Management (ITSCM) system. The policies of these systems are closely aligned to the Risk Policy and Security Policy. The primary goal of our BCM and ITSCM is to ensure the continuation or the timely recovery of critical business services according to their continuity requirements and prioritization. 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 Service Continuity Manager is responsible for implementing the 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, Physical Security is closely aligned with the Risk and Security Policy. Our requirements at group level are aligned to specifications formulated in the ISO/IEC 27001 Standard and the Payment Card Industries Data Security Standard (PCI DSS) in the field of Physical Security. Similarly, our Health, Safety and Environmental Protection specifications align with ISO 45001 and ISO 14001 respectively.**

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

- to guarantee the security of all employees, guests and customers of SIX in all premises and facilities;
- to protect our premises and facilities and safeguard all assets, property and information contained within;
- to ensure uninterrupted business operations and high availability of all infrastructure components.

The Health, Safety and Environmental (HSE) protection system 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, dangers 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 are confident in our security model and by replicating the SIX Security Concept in Spain, we are adding value to our organization from both a local and global perspective.

Jesús Romero de Pablos
Manager of Corporate Security Spain

## Corporate Security Spain

**SIX is replicating the SIX corporative security concept in Spain, integrating the Spanish security teams into the SIX global model. This model is replicated with dedicated teams working in a coordinated manner and in constant communication with the SIX global teams, ensuring responsiveness and leveraging the capacity and experience of the SIX global teams, while ensuring an independent decision-making process.**

**BCM, Physical Security, Health & Crisis Management**
With a dedicated team and in accordance with national and European regulations, we apply the SIX Integrated Security model to protect people, buildings, perimeters and supply systems. In terms of business continuity and crisis management, the BME teams and management bodies (Spanish value chain) are fully integrated into the SIX Crisis & Emergency structure, ensuring the resilience and recovery capacity of critical processes from both a local and global perspective.

**Security, Risk and Governance**
One group, one regulation. In coordination with the SIX Security Risk and Governance team, we participate in the definition of the global SIX regulatory framework to ensure its alignment with national requirements as well as European regulations.

**Information Security**
With a dedicated team in Spain, in constant communication with the global SIX Information Security team, we support the first line of defense in the implementation of the security policy framework, ensuring alignment with the group's security standards through consulting processes, security reviews or the project assurance function among others.

**Supplier Risk Management**
The Spanish Supplier Risk Management (SRM) function is integrated into the SIX SRM team, with dedicated staff focused on tracking and assessing Spanish legal entities' third parties in accordance with Spanish and European requirements and in line with SIX standards.

**Security Testing**
The Security Testing group is also replicated in the Spanish security organization with dedicated staff for the development of penetration tests, red team exercises and other security offensive techniques with the aim of ensuring the security coverage of 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, 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