Building Trust

The Security Measures Behind Operations of SIX

Introduction

SIX provides and operates stable and efficient infrastructure for the Swiss and Spanish financial centers, ensuring access to capital markets and facilitating the flow of information and money between financial market players. We are Switzerland's competence center for payments and other banking services and offer reference, pricing, and corporate action data to customers globally, along with regulatory services and indices.

SIX complies with the obligations of the regulatory authorities including FINMA, CNMV, ESMA, and BaFin. Therefore, we adhere to international directives and standards including DORA, CPMI-IOSCO, SWIFT CSP/PSP, PCI-DSS, GDPR, MiFID II, MiFIR, CSDR and EMIR.

We are committed to maintaining the highest standards of security and reliability. Given our complex regulatory & technological environment, the confidentiality, integrity, and availability of our IT systems and information are of critical importance.

SIX's Information, IT and Cyber Security Management System (ISMS) is based on the Standard of Good Practice (SoGP) from ISF which aligns with industry frameworks like NIST Cybersecurity Framework (CSF) and ISO 27001 as well as general good practice. It is compliant with relevant laws and regulatory requirements. This is verified by independent auditors on a regular basis.

This brochure aims to provide insights into our security measures.

Section 1: Security Governance, Risk and Assurance

1 Security Governance

SIX is committed to maintaining a robust information security governance framework to ensure high standards of governance and effective risk management. The governing body sets clear directions and defines the organization's risk appetite, balancing risk, cost, and agility with business outcomes. An integrated information security strategy supports the organization's strategic objectives, while stakeholder engagement fosters a collaborative security culture. This approach, supported by the three lines of defense model, ensures that security management activities consistently support the organization's success and align with its risk tolerance. The three lines of defense include operational management, risk management and compliance functions, and internal audit, providing comprehensive oversight and assurance.

2 Information Risk

We manage information risk effectively and consistently across our organization. Regular, systematic risk assessments of our business environments, processes and applications ensure that risks remain within acceptable limits. Our methodology includes scoping, business impact assessments, threat profiling, vulnerability assessments, risk evaluation, and risk treatment. This approach helps responsible individuals to identify key risks, evaluate them, and select appropriate treatment options. By maintaining a robust framework supported by our governing body, we ensure all risk management activities are aligned with our risk appetite and organizational goals.

3 Security Assurance

At SIX, we have a robust and structured information security assurance program. This includes comprehensive security testing, regular monitoring, and thorough internal and external audits to ensure our security controls are effective. We provide executive management and stakeholders with a clear and comprehensive view of information risks across the organization. Our goal is to facilitate informed decision making and ensure that security measures are diligently implemented to protect against information risks. Regular audits and ongoing monitoring help us maintain high standards of security and compliance.

Section 2: Security Control Framework

1 Security Management

Our comprehensive information security policy is supported by complementary policies, including acceptable use, and communicated with relevant individuals. Consistent application of security policies across the organization is ensured by our dedicated security function, led by our Chief Security Officer (CSO). We continuously improve our security program, aligning business and IT projects with formal security requirements. Business Information Security Officers (BISOs) in each business unit help manage information risk and promote security awareness. Policies are regularly reviewed and approved to ensure they remain effective and up-to-date.

2 Asset Management

The asset management guidelines emphasize maintaining accurate and up-to-date asset registers, regularly reviewed to identify and address discrepancies. Asset owners are assigned to manage and protect assets throughout their lifecycle, ensuring critical and sensitive assets are safeguarded. Regular asset discovery exercises are conducted to identify assets and understand their business context. The program aims to support riskbased decisions.

3 People Management

Embedding information security requirements throughout the employment lifecycle provides robust protection of critical and sensitive information at SIX. We establish clear security agreements with all individuals and external parties accessing our systems, ensuring their obligations are formally accepted. Ownership of IT systems, applications and information is assigned to capable individuals, with clearly defined responsibilities for their protection. Furthermore, agreements and technical controls for employee-owned devices used for business purposes are implemented. Additionally, we have an authorization process for remote work, especially in high-risk areas, to safeguard endpoint devices and information against theft, loss, and cyber-attacks.

4 Security Education and Training

By placing a high priority on a robust security education, training, and awareness program, we empower all individuals with access to our information and systems to exhibit the expected security behaviours. Tailored security messages are communicated regularly and provide comprehensive training on secure system usage and application. Yearly training sessions, which are mandatory, are updated and tailored to meet the specific needs of each function. The goal is the cultivation of a security-positive culture where individuals are equipped with the necessary knowledge and tools to make informed decisions about information risk. We emphasize the importance of developing and applying effective information security controls, especially for those with system development responsibilities.

5 Information Management

The establishment of a comprehensive data governance framework, which includes data management processes, an enterprise-wide data inventory, and data quality management, demonstrates our commitment to maintaining the highest standards of information management and security. Our information classification scheme applies to all formats of information and protects us against corruption, theft, loss, and unauthorized disclosure throughout the information lifecycle. This framework addresses the confidentiality, privacy, integrity, and availability of data. Responsibility for managing data confidentiality/privacy is assigned to data owners, supported by privacy impact assessments and specialized security solutions like encryption and data leakage prevention. This approach guarantees that critical and sensitive information is consistently protected and compliant with legal and regulatory requirements.

6 Hardware and Endpoint Devices

It is of the utmost importance to guarantee the secure management of all hardware and endpoint devices throughout their entire lifecycle. These devices are fundamental to our operations and, as a result, represent potential points of vulnerability for security breaches. Examples include workstations, laptops, servers, office equipment, and specialized devices. Stringent security measures are enforced for their acquisition, configuration, maintenance, and disposal. Mobile devices are centrally managed to protect against loss, theft, and unauthorized disclosure. Our goal is to deploy robust hardware that safeguards critical and sensitive information, ensuring compliance with defined security requirements.

7 Internal Control System

The security of our Internal Control System (ICS) is effectively managed by a structured governance program. This program ensures that ICS are regularly assessed for risks and protected with tailored security controls. The goal is to identify, categorize, and safeguard these systems, managing information risks effectively. Through the conduction of specialized risk assessments, we maintain safety, reliability, and effectiveness of our ICS. By applying appropriate security measures, we ensure these systems operate securely within their specific environments.

8 System Development

All business applications and systems are developed using a secure system development lifecycle (SDLC), incorporating good industry practices and security at every stage. We apply secure development principles, version control, and quality management to all development activities, including agile iterations. Each project is supported by comprehensive project initiation documents and plans, covering key management requirements and security needs. Prior to deployment, systems are subjected to comprehensive testing to verify compliance with strict acceptance criteria, thereby guaranteeing their intended functionality and preventing any potential security breaches. Post-implementation reviews are conducted to evaluate the effectiveness of security controls and reduce risks associated with obsolete systems.

9 Business Applications

Our business applications are fortified with effective security controls to protect sensitive information throughout its lifecycle. We manage customer access, conduct risk assessments and enforcing risk-based strong authentication mechanisms. Our goal is to ensure business applications operate reliably, safeguard against unauthorized access, and maintain data integrity. By adhering to these guidelines, we ensure secure and consistent customer connections in line with contractual obligations.

10 User Applications

The establishment of a comprehensive data governance framework, which includes data management processes, an enterprise-wide data inventory, and data quality management, demonstrates our commitment to maintaining the highest standards of information management and security. Our information classification scheme applies to all formats of information and protects us against corruption, theft, loss, and unauthorized disclosure throughout the information lifecycle. This framework addresses the confidentiality, privacy, integrity, and availability of data. Responsibility for managing data confidentiality/privacy is assigned to data owners, supported by privacy impact assessments and specialized security solutions like encryption and data leakage prevention. This approach guarantees that critical and sensitive information is consistently protected and compliant with legal and regulatory requirements.

11 Access Control

As part of our measures to secure our systems and data, we prioritize stringent access control measures to ensure the security of our systems and data. The restriction of access to business applications, mobile devices, systems, and networks to authorized individuals and entities follows a formal access control policy based on the principle of least privilege. This policy includes a formal approval process to grant access privileges. Access privileges are granted according to roles and assisted by multifactor authentication mechanisms. We implement a privileged account management process to tightly control and regularly review privileged accounts. Additionally, our identity and access management system ensure consistent user administration, identification, and authentication across all approved systems, with periodic access reviews to maintain security and compliance.

12 Third Party Risk Management

Third-party risk management (TPRM) ensures that SIX effectively identifies, assesses, and mitigates risks associated with its external partners, vendors and sub-vendors. The process involves evaluating the potential risks that third parties may pose to the organization's operations, security, and regulatory compliance. Continuous monitoring and regular assessments of third-party relationships are essential to maintain a secure and resilient business environment.

13 Cloud Services

Our tailored cloud security controls cover a wide range of common security measures, including network security, access management, data protection, secure configuration, and security monitoring. This comprehensive approach is fundamental to maintaining robust security management for cloud services as it allows for the secure use of these services. Clear cloud security requirements are communicated to everyone involved in purchasing, developing, configuring, or using these services.

14 Technical Infrastructure

SIX ensures the security and reliability of its technical infrastructure by designing and building systems and network installations to handle current and future workloads securely. Systems are configured consistently to protect against cyber-attacks, unauthorized access, and data loss. The infrastructure incorporates security architecture principles, considers zero trust architecture, and supports secure virtual instances. Containers are deployed and managed securely, with protection for container host operating systems and orchestration tools. This robust infrastructure aims to safeguard critical systems, data, and services, reducing the risk and impact of cyber threats and system overloads.

15 System Resilience

The resilience of our systems assures the reliability and security of our technical infrastructure. Therefore, our resilience program includes using robust hardware and software, supported by alternative facilities, to maintain system performance and availability. We manage capacity requirements, apply rigorous change management processes, perform regular backups, and monitor performance to safeguard against malicious attacks and human error. Additionally, we validate and enhance our system resilience by conducting cyber security exercises. This approach ensures that our systems can be restored quickly and effectively in the event of a major security incident, without compromising the confidentiality or integrity of the information they handle.

16 Network Management and Connectivity

Our network management framework ensures the design of reliable networks, preventing unauthorized access and encrypting connections. We protect our networks with physical and logical controls, accurate documentation, and proper labeling. Network devices are configured to segregate networks and firewalls restrict network traffic. We have measures in place to detect potential intrusions and safeguard against Denial-of-Service (DoS) attacks. Additionally, we strictly control remote maintenance and external connections to safeguard critical and sensitive information.

17 Cryptography

We deploy approved cryptographic solutions across our organization to safeguard sensitive information. Our cryptographic key management process ensures keys are protected throughout their lifecycle, preventing unauthorized access or destruction. We implement secure public key infrastructures (PKI) with trusted certification and registration. These measures are designed to protect the confidentiality, integrity, and authenticity of critical information. The aim is to support strong authentication and non-repudiation, ensuring our operations remain secure and reliable.

18 Threat Protection

At SIX, we implement comprehensive threat protection solutions to safeguard our critical systems and infrastructure from malware and malicious attacks. Our approach includes regular vulnerability scans, continuous security event monitoring, and regular penetration tests. We aim to quickly identify and remediate technical vulnerabilities, reducing the risk of exploitation and security incidents. By maintaining robust malware protection and intrusion detection mechanisms, we ensure timely responses to potential threats. Our goal is to minimize the frequency and impact of cyber-attacks, ensur-ing the security and resilience of our operations.

19 Security Event and Incident Management

To safeguard our operations and customer interests, we have implemented a robust security event and incident management process. Detailed logs of security events are maintained, protected from unauthorized changes, and regularly analyzed. Our security specialists use both automated and manual methods to review these events, supported by a dedicated threat intelligence team. We have a comprehensive incident management framework to identify, respond to, and recover from security incidents efficiently. Additionally, we ensure prompt and secure application of emergency fixes and, if necessary, conduct forensic investigations to preserve evidence and identify perpetrators. SIX is connected to various national and international, as well as industry-specific, Information Sharing and Analysis Centers (ISACs) to enhance our security pos-ture through shared intelligence and collaboration.

20 Physical Protection

Physical security at SIX encompasses organizational, structural, and technical measures to ensure the safety of employees, guests, and clients. It aims to protect buildings, facilities, and assets through zoning, barriers, and surveillance. The goal is to maintain uninterrupted business operations and infrastructure availability. The approach includes risk prevention, minimization, and intervention. Compliance with ASA directive EKAS 6508 and ISO 45001 ensures adherence to and safety standards.

21 Business Continuity

The Business Continuity Management (BCM) Program at SIX is integrated into the three lines of defense model, a standard in the financial sector. Business Units and Corporate Functions form the first line of defense, each with a Business Continuity Manager responsible for BCM implementation. An IT Continuity Manager oversees IT Service Continuity Management (ITSCM). Both BCM and ITSCM life cycles are reviewed annually. The “Business Continuity Management by SIX” brochure provides an overview of the program’s structure: Corporate Security at SIX.