Anhang 5
Datensicherheit und Basis der ISAE 3000 Berichtserstattung von SIX

zum Teilnahmevertrag bLink Plattform

Dieser Anhang beschreibt die Datensicherheit der Plattform und der von SIX gegenüber den Teilnehmern erbrachten Dienstleistungen. Die aufgeführten Prüfziele basieren auf dem international anerkannten Standard «Information Security Forum (ISF) – The Standard of Good Practice for Information Security 2018» und sind in verschiedene Prüfgebiete unterteilt. Die untenstehenden Kontrollziele bilden die Basis für die Auswahl der Kontrollen der jährlichen ISAE 3000 Type II Berichtserstattung.

Nr.	Statement	Description	Ref (ISF)
1	Security Governance		
1.1	Security Governance Framework	SIX has a framework for information security governance, where commitment is demonstrated by the organisation's governing body.	SG.01.01.01
1.2	Security Direction	SIX has a full-time Chief Security Officer at executive management level with overall responsibility for the organisation's information security programme.	SG.01.02.01
2	Information Risk Assessment		
2.1	Information Risk Assessment Framework/ Methodology	SIX has a documented procedure for managing information risk assessments. Risk assessments are based on a structured and systematic information risk assessment methodology.	IR.01.01.01 IR.01.02.01
3	Security Management		
3.1	Information Security Policy	SIX has a documented information security policy which applies across the organisation and is communicated to all individuals with access to the organisation's information and systems.	SM.01.01.01
3.2	Acceptable Use Policies	SIX has a regulation which defines the way individuals are expected to use information and systems within the organisation.	SM.01.02.01
3.3	Information Security Function	SIX has dedicated Information Security Partners for business units, led by the Chief Security Officer, which have responsibility for promoting good practice in information security throughout the organisation.	SM.02.01.01
4	People Management		
4.1	Employment Lifecycle	SIX screens applicants for employment prior to commencing work (e.g. by taking up references, checking career history/qualifications and confirming identity, such as by inspecting a passport). In the case of functions that are particularly critical in terms of security, employees are regularly checked with respect to risk factors and in case of access to customer identifying data an extract of the criminal record and of the debt collection register must be obtained.	PM.01.01.01
4.2	Ownership and responsibilities	Within SIX ownership of critical business environments, processes, and applications (including supporting technical infrastructure) is assigned to individuals (e.g. business managers), acknowledged and documented.	PM.01.02.01
4.3	Security Awareness Programme	SIX has a security awareness programme to promote and embed expected security behaviour throughout the organisation and establish a security-positive culture. SIX employees are regularly trained regarding different security topics.	PM.02.01.01
5	Information Management		
5.1	Information Classification and Handling	SIX has an information classification scheme (supported by information handling guidelines) that applies throughout the organisation, based on the confidentiality of information.	IM.01.01.01 IM.02.02.01
5.2	Information Privacy	SIX has a Data Protection Officer who is responsible for managing information privacy and information security controls applied for handling personally identifiable information (i.e. information that can be used to identify an individual person).	IM.01.02.01
6	Physical Asset Management		
6.1	Hardware lifecycle Management	SIX has documented standards/procedures for managing the lifecycle of hardware.	PA.01.01.01

7	Mobile Computing		
7.1	Mobile Device Protection	SIX mobile devices (including laptops, tablets and smartphones) are built using standard technical configurations and subject to security management practices to protect information against loss, theft and unauthorised disclosure. They are also provided with secure means of connecting to other devices and to networks.	PA.02.01.01 PA.02.03.01
7.2	Portable Storage Devices	SIX has documented standards/procedures covering the use of portable storage devices.	PA.02.05.01
8	System Development		
8.1	System Development Methodology	Development activities of SIX are conducted in accordance with a documented system development methodology.	SD.01.01.01
8.2	System Development Environments	System development activities of SIX are performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.	SD.01.02.01
8.3	Specifications of requirements	System requirements (including those for information security) of SIX are documented in the business requirements and agreed before detailed design commences. Information security requirements for systems under development should be considered when designing systems.	SD.02.01.01
8.4	System Design	Information security requirements for systems under development is considered when designing systems.	SD.02.02.01
8.5	Software Acquisition	SIX has documented standards/procedures for acquiring software.	SD.02.03.01
8.6	System Testing	Systems under development (including application software packages, system software, hardware, communications and services) are tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.	SD.02.05.01
8.7	Security Testing	Systems under development are subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).	SD.02.06.01
8.8	System Promotion Criteria	Rigorous criteria (including security requirements) are met before new systems are promoted into the live environment. New systems are installed in the live environment in accordance with a documented installation process.	SD.02.07.01
8.9	System Decommission	Systems that are no longer required should be evaluated and subject to a decommissioning process (where required), taking account of relevant information, software, services, equipment and devices.	SD.02.10.01
9	Business Application Management		
9.1	Business Application Register	Business applications of SIX are recorded in an accurate and up-to-date business application register.	BA.01.01.01
9.2	Business Application Protection	Business applications of SIX are protected by using sound security architecture principles.	BA.01.02.01 BA.01.04.01
10	System Access		
10.1	Access Control	SIX has an access management process in place which regulates access (including periodic review) to business applications, systems, networks and computing devices by all types of user.	SA.01.01.01
10.2	Customer Access Arrangements	SIX has documented standards/procedures for the provision of access to the organisation's business applications by customers.	SA.02.01.01
10.3	Customer Connections	SIX has documented standards/procedures for establishing the technical security arrangements for customer connections.	SA.02.03.01
11	System Management		
11.1	Computer and Network Installations	Computer system, network and telecommunication installations (e.g. data centres) are designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.	SY.01.01.01
11.2	Server Configuration	Servers are configured in accordance with documented standards/procedures.	SY.01.02.01

11.3	Service Level Agreements	Computer and network services that support critical business applications and processes are defined in documented service agreements (e.g. contracts or service level agreements) that meet operational, safety and security requirements.	SY.02.01.01
11.4	Backup	Backups of essential information and software is performed frequently enough to meet business requirements.	SY.02.03.01
11.5	Change Management	Changes to business applications, information systems and network devices are tested, reviewed and applied using a change management process.	SY.02.04.01
12	Networks and Communications		
12.1	Network Management	SIX network devices are configured to function as required, and to prevent unauthorised or incorrect updates. Network devices are physically protected.	NC.01.01.01 NC.01.02.01
12.2	Wireless Access	SIX wireless access are subject to authorisation, authentication of users and computing devices, and encryption of wireless traffic.	NC.01.03.01
12.3	External Network Connections	All external network connections to systems and networks are individually identified, verified, recorded, and approved by the system or network owner.	NC.01.04.01
13	Electronic Communications		
13.1	Email/Collaboration	Email systems and collaboration platforms are protected by a combination of policy, awareness, procedural and technical security controls.	NC.02.01.01 NC.02.02.01
14	Supply Chain Management		
14.1	External Supplier Management Process	SIX has a documented process for managing the information risks associated with external suppliers (including organisations in the supply chain).	SC.01.01.01
15	Technical Security Management		
15.1	Malware Protection Activities	Activities are performed to make users aware of the risks from malware, and to specify the actions required to minimise those risks.	TS.01.02.01
15.2	Malware Protection Software	Systems throughout the organisation are safeguarded against all forms of malware by maintaining up-to-date malware protection software, which is supported by effective procedures for managing malware-related security incidents.	TS.01.03.01
15.3	Intrusion Detection	Intrusion detection mechanisms are employed for networks with critical business applications and systems to identify predetermined and new types of attack.	TS.01.05.01
16	Cryptography		
16.1	Cryptographic Solutions	Cryptographic solutions are subject to approval, documented and applied throughout the organisation.	TS.02.01.01
16.2	Cryptographic Key Management	SIX has documented standards/procedures for managing cryptographic keys.	TS.02.02.01
17	Threat and Incident Management		
17.1	Technical Vulnerability Management	SIX has a process for the identification and remediation of technical vulnerabilities in business applications, systems, equipment and devices.	TM.01.01.01
17.2	Security Event Logging	Important security-related events are recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis.	TM.01.02.01 TM.01.03.01
18	Security Incident Management		
18.1	Security Incident Management Framework	An information security incident management framework is established, including relevant individuals, information and tools required by the organisation's information security incident management process.	TM.02.01.01
18.2	Emergency Fixes	SIX has documented standards/procedures for applying emergency fixes to business information, business applications and technical infrastructure (including systems software and computer equipment)	TM.02.03.01

19	Physical and Environmental Security		
19.1	Physical Protection	All critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) are physically protected against accident or attack and unauthorised physical access.	LC.02.01.01
20	Business Continuity Management		
20.1	Business Continuity Program	A business continuity programme is established, which includes developing a resilient technical infrastructure, creating a crisis management capability, and coordinating and maintaining business continuity plans and arrangements across the organisation.	BC.01.02.01
20.2	Crisis Management	A crisis management process should be established, supported by a crisis management team, which details actions to be taken in the event of a major incident or serious attack.	BC.01.04.01
20.3	Business Continuity Planning	Business continuity plans are developed and documented to support critical business processes throughout the organisation.	BC.02.01.01
21	Security Monitoring and Improvement		
21.1	Security Audit Management	Independent security audits are performed regularly for target environments that are critical to the success of the organisation.	SI.01.01.01
22	Zulassungskriterien (SIX internes Reglement)		
22.1	Zulassungsprüfung	SIX hat einen dokumentierten Prozess, welcher das Vorgehen bei einer Erst- oder Wiederholungszulassungsprüfung für Plattformteilnehmer definiert und die Zulassungskriterien gemäss Teilnehmervertrag prüft.	N/A