Business Continuity Management by SIX

At a Glance

BCM Lived by SIX

This brochure provides an overview of the structure of the BCM program at SIX.

SIX operates the infrastructure for the financial centers in Switzerland and Spain, thus ensuring the flow of information and money between financial market players. SIX offers exchange services, securities services, financial information and banking services with the aim of increasing efficiency, quality and innovative capacity along the entire value chain. These services are critical not only in the corporate context, but also for the national economies in Switzerland and Spain.

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, in order to ensure the provision of the above mentioned services even in case of disruptive events.

The **BCM system** ensures that time-critical business processes can be continued at a predefined emergency level if events have occurred leading to one of the following generic loss of resource scenarios:

- Loss of building
- Loss of staff
- Loss of system/IT
- Loss of service providers/suppliers

In addition, SIX makes specific preparations for severe, but plausible scenarios, where several classes of resources may be unavailable for a longer period.

The **ITSCM system** ensures that the platforms and applications required for the emergency operation of time-critical business processes can be put into operation again in accordance with the requirements of BCM when the following scenarios occur:

- Physical destruction of a data center
- Logical destruction of data centers by cyber-attacks
- Inaccessibility of a data center
- Failure of wide area network connectivity

Plans are nothing; planning is everything.

Dwight D. Eisenhower

Policy and Program Management

SIX maintains dedicated **BCM and ITSCM policies,** closely aligned to the risk and security policies. SIX reviews and adapts its BCM and ITSCM policies and the related programs on a yearly basis. The underlying changes are evolutionary in nature rather than revolutionary, and are typically driven by new regulations, new technologies, new market opportunities, and new customer demands.

The BCM and ITSCM programs at SIX are integrated into a three lines of defense model, which has become standard practice in the financial sector. On the first line of defense the **Executive Board** is responsible for the adequate design and implementation of the BCM system at SIX. In each Business Unit and Corporate Function, a **BC Manager** supported by technical staff is responsible for implementing BCM according to the company-wide standards. Within the Corporate Function IT, an ITSC Manager is responsible for implementing the ITSCM likewise.

On the second line of defense, located in the Corporate Function Risk, Security and Compliance, a **Corporate BC Manager** reporting to the Chief Security Officer oversees the BCM program. Furthermore, the Corporate BC Manager provides a company-wide BCM methodology, which is geared toward international practices (e.g., BCI Good Practice Guidelines, standards (e.g., ISO22301) and regulations (e.g. FINMA Circular 2023/1). The Corporate BC Manager supports the Business Units and Corporate Functions in applying this methodology.

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 BCM and ITSCM organization and programs.

BCM Lifecycle

The yearly BCM Lifecycle consists of four phases:

1. Analysis

SIX conducts **Business Impact Analyses (BIA)** on different levels in order to identify Critical Functions and time-critical business processes. On the **strategic level** the SIX Board of Directors approves the Critical Functions (critical services to clients) and their Tolerances for Disruption with regard to Severe but Plausible Scenarios.

On the **tactical and operational level** all Business Units and Corporate Functions conduct Business Impact Analyses (BIA) in order to identify their time-critical business processes and continuity requirements regarding resources and dependencies. To allow a comparison across the company, the BIA process is conducted in a dedicated tool with a common methodology. BC Managers of the Business Units and Corporate Functions maintain and update their BIA annually and let them approve by their Business Unit Head or Corporate Function Head.

The core of the BIA is the **impact assessment,** in which the impacts of a total failure of processes are analyzed for multiple points in time after the outage. Thereby, the following impact categories are considered: external, regulatory, reputational, internal and financial.

Based on the impact assessment the **Recovery Time Objective (RTO)** is determined. For all business processes identified as time-critical, process dependencies and resource requirements for maintaining an emergency operation are identified.

The BIA results of all Business Units and Corporate Functions are consolidated and a **SIX-wide Business Process Prioritization** is conducted in order to be able to recover operations in an ordered manner in case of a crisis. The SIX Business Process Prioritization is assessed and approved by the Executive Board on a yearly basis.

2. Design

SIX has a set of **Business Continuity Options** in place to cope with the BCM scenarios mentioned above. Each Business Unit and Corporate Function documents the selected options for their time-critical processes and assesses their effectiveness in maintaining emergency operations in a BC Strategy.

For the **loss of building** scenario the main option is to work from home. For time-critical business processes requiring on-site presence for their operation, emergency workplaces are available in a separate location. Wherever possible, a permanent split operation is implemented for the most time-critical business processes even during normal operation (resilient operation). This allows a smooth transition to emergency operation in case of a loss of building scenario and significantly reduces the risk of a **loss of staff** scenario. If possible, the loss of staff scenario is covered with additional options (e.g., delegation of tasks to another team or multi-skill-training).

While the **loss of system/IT** scenario is generally covered by IT Service Continuity Management (see next chapter), the Business Units and Corporate Functions have prepared communication measures for their customers and workarounds, in cases where it is possible.

As for the **loss of service provider/supplier** scenario, contractual BCM agreements are in place, which require critical service providers suppliers of SIX to maintain their own BCM. If reasonable, SIX pursues a dual- or multi-vendor strategy for addressing the loss of service provider/supplier scenario (e.g., for power supply, procurement of IT hardware).

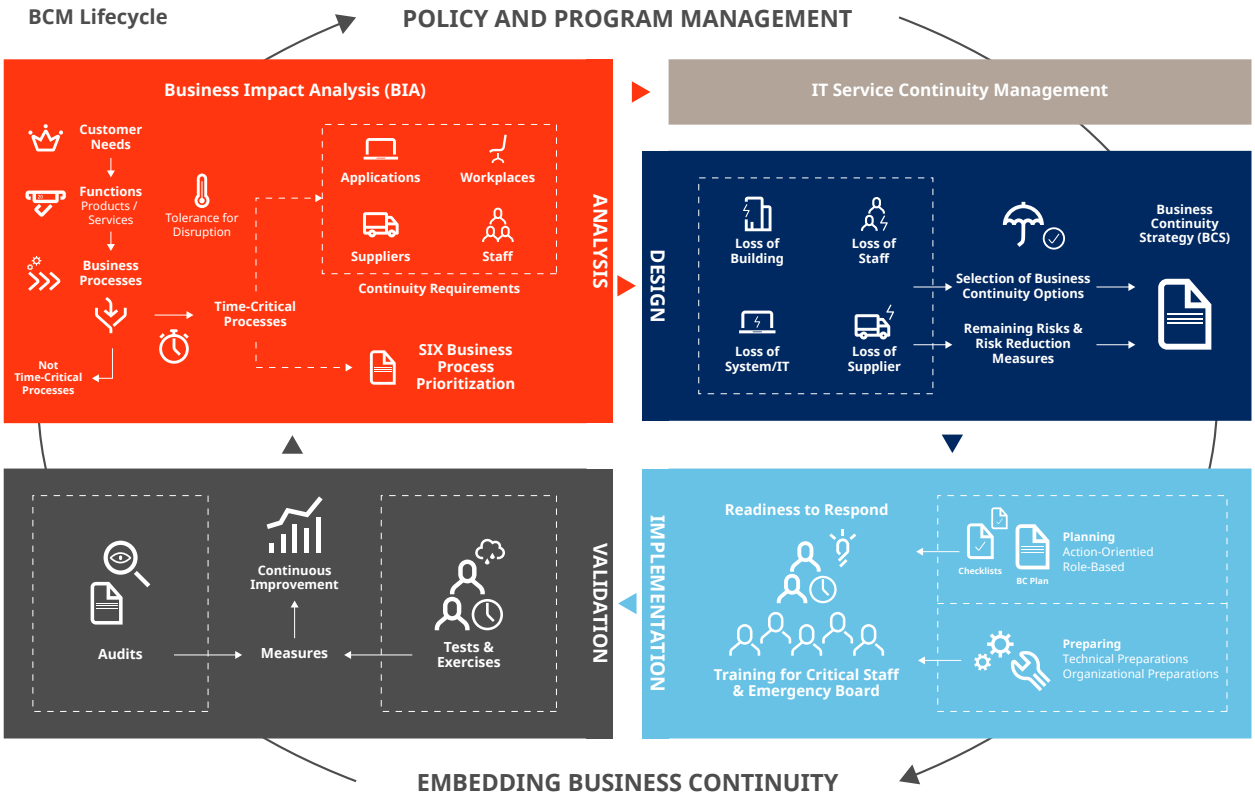
3. Implementation

To be able to respond quickly and consistently in case of a crisis, SIX maintains **BC plans** (including role-based checklists) and implements necessary **preparatory measures** (e.g., establishment of emergency workplaces). The staff of time-critical business processes are trained to implement the emergency operation according to BC plans in case of a crisis.

4. Validation

SIX conducts **tests and exercises** to validate the functionality of preparatory measures, such as emergency workplaces, and its BC plans. Exercises are scenario-based and include affected staff of time-critical business processes.

SIX aims to increase the complexity of its exercises over time in order to identify new measures. This helps to ensure the continuous improvement of the BC plans and the BCM system as a whole.



ITSCM Lifecycle

The yearly ITSCM Lifecycle consists of four phases aligned to the BCM Lifecycle:

1. Analysis

The ITSCM lifecycle starts with an **ITSC Gap Analysis** in which the IT recovery test results are compared with the requirements from the Business Impact Analysis (BIA) identified in the BCM lifecycle. The analysis is conducted in a dedicated ITSCM Status Monitoring Tool. This enables deviations to be identified promptly and mitigating measures to be implemented.

2. Design

SIX operates **redundant data centers** worldwide to guarantee high availability of services, for example, in case of a physical destruction of a data center. Most data centers are operated by external providers., whereas IT (with the exception of cloud services) is always operated by SIX. Secondary data centers that are used for failover in case of IT disaster recovery are located in different areas with generally different risk profiles. In this context, SIX operates **emergency workplaces** for critical IT staff in case of a loss of the respective building. Additionally, required data center staff is working in a **permanent split operation** to avoid a complete loss of staff.

Outsourced IT services must also comply with IT disaster recovery requirements. The relevant requirements are contractually agreed with external suppliers and must be confirmed.

SIX operates a **Security Operation Center (SOC),** which is managed by a global team at multiple international locations. Its practices are aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework. For cyber threats including malware or DDoS attacks, SIX has implemented detection and protection measures and is maintaining and developing solutions to respond and recover. Continuous improvements are implemented along the SIX Information Security Strategy.

Remote access enables the operation and switchover of the data center in case of inaccessibility of data centers. The scenario of a wide area network failure is covered by **redundant data connections** of the data centers from different providers.

3. Implementation

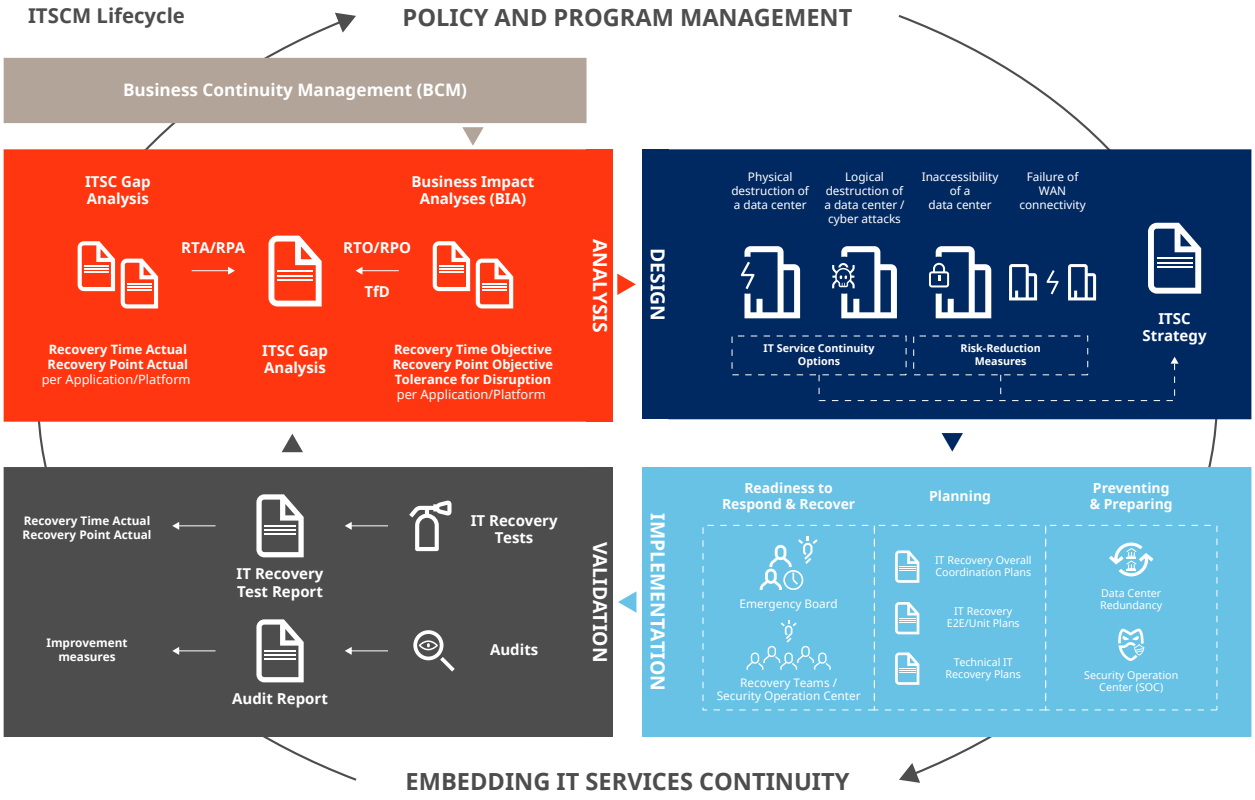
IT Recovery End-to-End plans for a complete area of SIX (e.g. for a Business Unit) describe the sequence and the procedure of how the platforms and applications of the most time critical processes are to be recovered in a coordinated manner.

IT Recovery Overall Coordination Plans based on the SIX Business Process Prioritization created in the BCM lifecycle describe the SIX-wide sequence of the platforms and applications to be put back into operation. They serve as a coordination tool for the IT Emergency Board.

4. Validation

The functionality of **IT recovery plans** is regularly validated in IT recovery tests. Unit tests confirm recovery procedures for single applications. End-to-End tests validate the recovery procedure for a complete area of SIX (e.g. for a Business Unit including dependencies to other units). The proactive planning, monitoring and tracing of the tests takes place in the ITSCM Status Monitoring Tool.

More than 300 IT recovery tests are conducted at SIX every year, either remotely or from the contingency site.



Embedding BCM and ITSCM

The SIX-wide embedding of BCM is achieved through **education and training** of the affected roles and by means of awareness measures. Employees holding a BCM role are familiar with the BCM specifications and take these into account in their daily work. SIX addresses the topics of BCM and ITSCM in a targeted and tailored manner to the different audiences within the company (staff/management) and beyond (external stakeholders).

Response Structure

Besides the staff of time-critical business processes, who implements the Business Continuity and IT Recovery Plans in case of an event, SIX operates an **Incident Management** as well as an **Emergency and Crisis Management.**

Small-scale incidents are handled by Incident Management. Incidents may then be escalated to the responsible Local Emergency Management Teams or Emergency Management Boards. Large scale incidents are then escalated to the topmost body, the Crisis Management Board of SIX. Alternatively, depending on the nature of the incident and depending on the impact expected or the time line anticipated, the Emergency or Crisis Management Boards of SIX can be activated immediately after an incident has been detected/identified.

In case of an emergency or a crisis, a **Communication Board** may be activated. The board makes sure that communication to internal and external stakeholders as well as clients is aligned with the Emergency Boards and the Crisis Management Board. It also takes into account the management of information flows at national and international level.

SIX, in its capacity as the operator of the financial market infrastructure, is represented in the Interbank Alarm and Crisis Organization (IACO) headed by the Swiss National Bank (SNB). SIX is also a founding member of the **Swiss Financial Sector Cybersecurity Centre (Swiss FS-CSC)** association. As a member of these organizations, SIX supports all efforts to prevent and overcome any crisis impacting the Swiss Financial Centre.

Operational Resilience

Operational resilience is the ability to identify and protect against threats and potential failures, to respond and adapt to disruptive events, and to recover and learn from them to minimize their impact on the delivery of critical services to clients. For SIX the central aspects for increasing operational resilience are:

- focusing on the preparations for Severe but Plausible Scenarios
- fostering of an optimal interplay between the different security and risk management disciplines.

Regulatory Requirements

SIX is subject to the supervision of several regulatory bodies and aims to run its business services in full compliance with regulatory requirements. Internal and external audits document the basic effectiveness of the SIX BCM system both in Switzerland and Spain on a regular basis.

In Switzerland, the Swiss National Bank (SNB) is both a regulator (for the supervision of systemic important processes) and a client of SIX. Most importantly, SIX operates the systemically important SIC (Swiss Interbank Clearing) system on behalf of SNB.

In addition, the Swiss Financial Market Supervisory Authority (FINMA) oversees the activities of SIX and several of its subsidiary legal entities such as SIX Swiss Exchange Ltd, SIX Digital Exchange Ltd, SDX Trading Ltd, SIX SIS Ltd, SIX x-clear Ltd, SIX Repo Ltd and SIX Trade Repository Ltd which are licensed according to Swiss Financial Market Infrastructure Act (FMIA). With respect to BCM, SIX is subject to FINMA Circular 2023/1 (Operational Risk & Resilience – Banks). Furthermore, the annual Payment Card Industry Data Security Standard (PCI DSS) certification is required for all ATM acquiring services and debit card issuing services which SIX provides to the Swiss banks.

In Spain, BME (Bolsas y Mercados Españoles), a subsidiary of SIX, aims to run its business services in full compliance with regulatory requirements. The Spanish Markets Supervisory Authority (CNMV) oversees the activities of BME and several of its subsidiary legal entities such as the Exchanges, Sociedad de Bolsas, S.A., BME Regulatory Services S.A., BME Clearing S.A. and Iberclear. The Spanish Central Bank (Banco de España, BdE) also has supervisory oversight related to the Public Debt market and its registration. Furthermore, ESMA, the European supervisory body, oversees the Trade Repository, REGIS-TR.

In the UK, the basic effectiveness of FCA oversees the Trade Repository, REGIS-TR UK Ltd.

In different European locations SIX is subject to the supervision of **Digital Operational Resilience Act (DORA)** - Regulation (EU) 2022/2554, e.g., in Spain (BME), Germany (SECB) or Luxembourg (Regis-TR Luxemburg). This supervision is done through the corresponding National Competent Authority.

SIX is committed to continuous improvement. Self-driven optimization of existent processes and preparations and the devising of new ones in order to adapt in an ever-changing environment are a pre-requisite for success, not only in the field of BCM.

SIX Group Ltd
Hardturmstrasse 201
P.O. Box
CH-8021 Zurich

corporate-bcm@six-group.com
www.six-group.com

This brochure aims to introduce the topic of BCM (Business Continuity Management) as lived by SIX to current, potential, and future customers of SIX worldwide as well as to suppliers of SIX.