# General information on Business Continuity Management @ Swisscom

## Contents

# 1 Business Continuity Management @ Swisscom

Business continuity is a key concern for Swisscom. Swisscom provides its customers with a trustworthy and reliable ICT infrastructure. Business Continuity Management (BCM) helps to ensure the continuity of products, services and processes, thereby strengthening the trust of Swisscom's customers, partners and employees. For these reasons, Swisscom's Business Continuity Management System (BCMS) is structured in such a way that Swisscom is able to continue products, processes and services at an acceptable and predefined level in the event of disruptions.

## 1.1 Objective of the Business Continuity Management System at Swisscom

BCM is a management discipline that aims to ensure that Swisscom's critical activities (products, processes and services) continue to operate at a predefined level in the event of an incident or are restored as quickly as possible following an outage. Swisscom's BCMS therefore aims to protect Swisscom's employees, products, services and processes and to minimise the financial, operational, legal and reputational impact of disruptions.

BCM at Swisscom is implemented as part of a BCMS to fulfil Swisscom's strategic objectives, support the best customer experience, ensure operational excellence and create opportunities for new growth.

The BCMS does this by striving to fulfil four general objectives:

1. Capability and reliability: The BCMS is a coherent, company-wide management process that enhances the company's business continuity capability and the reliability and stability of its services.
2. Continuous improvement: The BCMS is a dynamic and adaptable management system designed to act and react to changes, trends and challenges that Swisscom faces as a leading provider of ICT services.
3. Awareness: The BCMS integrates awareness of activities related to business continuity into Swisscom's day-to-day operations.
4. Resilience: The BCMS is a forward-looking, adaptable and comprehensive programme that combines Swisscom's business areas and management disciplines (risk management, service continuity management, information security, emergency and crisis management) to improve overall resilience (organisational and operational).

## 1.2 Minimising the impact on critical resources

Business Continuity Management at Swisscom focuses on minimising disruption to the critical resources - staff, buildings, IT and suppliers - needed to support Swisscom's critical activities. Four generic interruption scenarios have been defined.

These scenarios include:

- Loss of personnel. Personnel with the necessary skills to ensure the continuity of Swisscom's identified critical activities are unavailable, affecting Swisscom's ability to operate.
- Failure of a building. A building used for the production, support or provision of any of Swisscom's identified critical activities is unavailable or fails, affecting Swisscom's ability to operate.
- Failure of ICT systems.[1] One or more ICT systems supporting the delivery of Swisscom's identified critical activities are partially or completely unavailable, affecting Swisscom's ability to operate.
- Failure of one or more suppliers. A supplier or an associated service required for the performance of a

[1] For further information on IT service management, see the chapter 3

critical Swisscom activity is unavailable, affecting Swisscom's ability to operate.

## 1.3 A standardised BCM approach to meet customer expectations

Swisscom's BCMS is structured and certified in accordance with ISO 22301:2019, the International Organisation for Standardisation (ISO) Security and Resilience - Business Continuity Management Systems.

As an operator of critical infrastructures, Swisscom bears a high level of responsibility towards Swiss society and Switzerland as a business location. Swisscom therefore follows the recommendations of several federal offices with its BCMS. Swisscom is also aware that in some sectors, particularly the financial sector, in which Swisscom plays an important role as a partner and supplier, a company-wide BCM is required by regulation. Swisscom has established close cooperation with the relevant Swiss Federal Offices, through which Swisscom ensures that the applicable legal, regulatory and other requirements identified by these offices are taken into account in the implementation and maintenance of Swisscom's BCMS. Swisscom is guided by the recommendations of the following federal offices when implementing its BCMS:

- Federal Office for Civil Protection (FOCP): Business Continuity Management is a central topic within the framework of the National Strategy for Critical Infrastructure Protection.
- Federal Office of Communications (OFCOM): Defines directives on the security and availability of telecommunication infrastructures and services in order to guarantee the reliability and availability of the entire national telecommunications system.
- National Cyber Security Centre (NCSC): The National Cyber Strategy (NCS) of the National Cyber Security Centre recommends that operators of critical infrastructures implement measures in the area of resilience management. The BACS is also responsible for the so-called ICT minimum standards. They offer operators of critical infrastructures assistance and concrete approaches for improving their ICT resilience.

# 2 The Swisscom Business Continuity Management System

Swisscom's BCMS was developed in such a way that it fits into the organisational context of Swisscom. Its functionality follows best practices and complies with the Plan-Do-Check-Act model of the International Standard for Security and Resilience - Business Continuity Management Systems (ISO 22301:2019) and the Business Continuity Institute's Best Practice Guide.

## 2.1 Activities in Swisscom's Business Continuity Management System

Swisscom's BCMS is conducted in a four-stage life cycle that identifies Swisscom's critical activities (products, processes and services) and their resources and compares them with the known risks and threats in close cooperation with Risk Management (analysis). Continuity measures are derived from this analysis (design), on the basis of which business continuity plans are developed (implementation). The business continuity plans are tested and the system is reviewed and continuously improved (validation).


Figure 1 The BCM Lifecycle @ Swisscom

The four steps within the BCMS are documented with a series of delivery objects. At the end of the life cycle, every critical activity at Swisscom has one:

- Business Impact Analysis (analysis phase) with specification of the requirements for the continuity of the critical activity (RTO - target for the recovery time; and the MTPD - maximum tolerable interruption duration).
- Risk Impact Assessment (analysis phase), which presents the potential impact of known risks on the critical resources of a critical activity.
- Business Continuity Strategies (design phase), which fulfils the continuity requirements and covers the known risks for a critical activity.
- Business continuity plans (implementation phase), which details the recovery activities for a critical activity.
- Test concept, test script and test report (validation phase) detailing the test results of a business continuity plan.
- Review[2] (validation phase).

### 2.1.1 Analysis

In the analysis phase, Swisscom's operating environment is analysed in two parts. Firstly, business impact analyses (BIA) are carried out to identify critical activities (products, services and processes) and determine the scope of BCM at Swisscom. Criticality is determined by assessing the potential financial, reputational, regulatory and operational impact of the failure or disruption of any of these activities over a given period of time. Secondly, the critical activities are analysed in terms of the resources required for operations and the potential impact of known business, business and operational disruptive risks and threats in order to

[2] Checks are carried out internally by the central BCM team.

determine the continuity needs of Swisscom's critical activities in relation to the risk landscape in which the company operates.

### 2.1.2 Design

Based on the results of the analysis phase, the design phase identifies and develops continuity strategies that meet the identified continuity requirements of Swisscom's critical activities. The strategies reflect the speed of response required to ensure continuity. They may be new or based on existing resources or agreements and focus specifically on the mix of resources (personnel, buildings, IT and suppliers) required to deliver a critical activity. Swisscom implements business continuity strategies based on a cost-benefit analysis to ensure that unacceptable risks and single points of failure are addressed.

### 2.1.3 Implementation

In the implementation phase, the continuity strategies and recovery measures are further detailed and incorporated as such into business continuity plans (BCP). These plans are integrated into Swisscom's existing response structures (Swisscom Incident Management Process and Crisis Management). This ensures that these plans can be implemented quickly to guarantee the continuity of critical activities in the event of a disruption or crisis at Swisscom.

### 2.1.4 Validation

This step ensures that Swisscom's BCMS is continuously improved. Through various activities (such as exercises, reviews, internal and external audits, management reviews, etc.), Swisscom monitors and evaluates the activities as well as the BCMS and makes adjustments where necessary. The validation step ensures that the BCMS fulfils the objectives set by Swisscom.

### 2.1.5 BCM programme management and integration of BCM

At Swisscom, BCM is organised and implemented according to the "Three Lines of Defence" model. Programme management and activities to embed BCM in Swisscom's culture are coordinated by the second line, a special BCM team at Group level (Group Security and Assurance). The central team draws up the governance documents (BCM directive, policy and instructions), the BCM training documents and supports the business units (representing the first line) in implementing the BCMS. BCM at Swisscom is supported by the Executive Board and developments, changes or adjustments are reported to the Executive Board on a regular basis.

## 2.2 The pillars of Swisscom's Business Continuity Management

Swisscom's BCMS focuses on four central pillars or resources: personnel, buildings, IT and suppliers. Swisscom's Service Continuity Management is closely integrated into the BCMS and ensures the continuous provision of critical IT and infrastructure services. Service continuity management is the responsibility of the IT, Network and Infrastructure (INI) business unit and is carried out as part of Swisscom's service management system (Chapter 3 ).

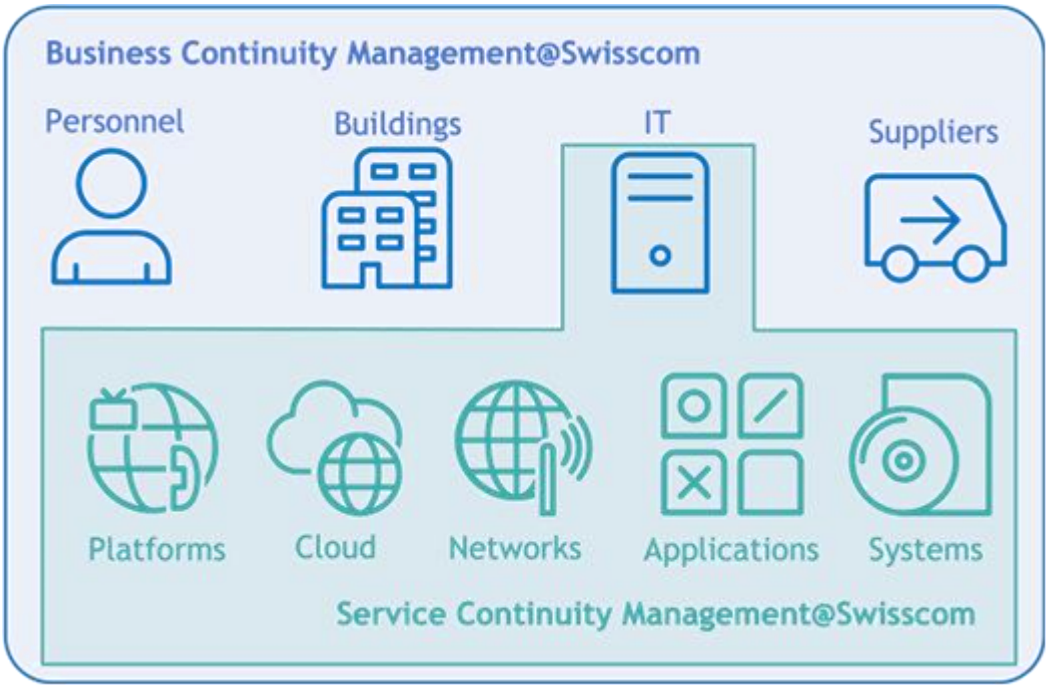


Figure 2: Business Continuity Management @ Swisscom. BCM focuses on the four "pillars" of BCM (personnel, buildings, IT and suppliers). Service Continuity Management (a key practice of Swisscom's Service Management System) ensures the continuous operation of IT.

# 3 Supplementary information: Service Continuity Management

Service Continuity Management is part of Swisscom's Operation Management System (OMS), which is based on the practices of the Information Technology Infrastructure Library (ITIL4). Service Continuity Management includes supplementary precautions such as additional hardware, software and geo-redundancy as well as procedural measures for a specific service. The aim of Service Continuity Management is to ensure the recovery of a service within agreed times (service level metrics RTO/RPO). For services that have an RTO/RPO (Recovery Time Objective/Recovery Point Objective) with defined target values, service continuity management includes regular tests on the continuity of the ICT service on the service platform. As shown in Figure 2, Service Continuity Management develops corresponding service continuity and disaster recovery plans for the services categorised as critical by Swisscom. It is therefore an important interface in the Swisscom BCM system.

## 4 Supplementary information: Risk Management

At Swisscom, risk management is geared towards achieving the company's strategic goals while protecting the company's assets and reputation. Risk management supports the company in making informed decisions based on a comprehensive knowledge of threats and their potential impact. Risk management at Swisscom takes place on three levels: at Group level, in the business units and in the context of security risks. The BCMS is closely interlinked with risk management at each of these levels to ensure that known risks are taken into account in the development of business continuity strategies (BCS) and business continuity plans (BCP) and that new risks are also identified and recorded.

## 5 Supplementary information: Incident Management

Swisscom relies on existing response structures coordinated by the Operational Control Centres (OCC) in Bern and Zurich to deal with incidents and emergencies. All incidents are managed by the Swisscom Incident Management Process. This process has proven its worth and has clearly documented sub-processes and procedures that show that Swisscom is able to respond effectively and efficiently to every incident, regardless of its cause. The process comprises operational, tactical and strategic (crisis management) elements, which are implemented using a well-established escalation model.

## 6 Supplementary information: Emergency and Crisis Management

Crises are sudden, exceptional situations that can have an impact on Swisscom's reputation, freedom of action or existence. These situations are dealt with at Group level on behalf of the CEO and with the involvement of the designated representatives of Swisscom's business units. Where necessary and appropriate, the business continuity plans developed as part of the BCMS can be used to support the emergency and crisis management process. All members of Swisscom's emergency and crisis management organisation receive annual training (including in the principles of business continuity management) in order to maintain their skills and fulfil their duties.

## 7 Supplementary information: Swisscom "ICT Business Continuity" service

In order to provide comprehensive support for our customers' business continuity needs, Swisscom offers the "ICT Business Continuity" product. This service guarantees the recovery of business-critical systems in the event of a disruption. As part of this service, Swisscom provides special IT resources to ensure the contractually agreed recovery times both in geo-redundant Tier 4 data centres and in other highly available facilities. Redundancy is a key aspect in guaranteeing the availability of systems. The functionality of the business continuity of the customer's processes and infrastructure provided by Swisscom is tested through regular failure tests

## Document information

| | |
|---|---|
| Doc ID | SECDOC-128 |
| Version | 3.0 |
| Classification | C2 General |
| Issue Date | August 2025 |
| Status | Released |
| Document subject | Information on Business Continuity Management |
| Contact us at | swisscom.bcm@swisscom.com |