General Information on Business Continuity Management@Swisscom

Contents

Version	2.0
Issue date	28.08.2023
Status	Released
Valid until	28.08.2025
Document ID	SECDOC-128

1 Business Continuity Management at Swisscom

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

1.1 Goal of Swisscom's Business Continuity Management System (BCMS)

BCM is a management discipline that aims to ensure that Swisscom's critical activities (products, processes and services) can continue to operate at a predefined level in the event of an incident, or to be recovered as quickly as possible following a failure. Swisscom's BCMS thus aims to protect Swisscom's people, its products and services and to minimise financial, operational, legal and reputational impacts of disruptions.

At Swisscom BCM is implemented in the context of a Business Continuity Management System (BCMS) in order to meet Swisscom's strategic objectives: ensuring the best customer experience, building operational excellence and creating opportunities for new growth.

The BCMS accomplishes these strategic objectives by striving to meet four general goals:

1. Capability and reliability: The BCMS is a coherent, company-wide management activity that increases the company's business continuity capabilities and the reliability and stability of its services.
2. Continuous improvement: The BCMS is a dynamic and adaptable management system that is designed to act on and react to changes, trends and challenges Swisscom faces as a leading provider of ICT services.
3. Awareness: The BCMS builds an awareness of the activities associated with business continuity into Swisscom's daily business.
4. Resilience: The BCMS is a future-oriented, adaptive and comprehensive programme that links Swisscom's business units and management disciplines (risk management, service continuity management, information security, incident and emergency management, and crisis management) to improve overall resilience (organisational and operational).

1.2 Minimising Impacts on Critical Resources

Business Continuity Management at Swisscom is focused on minimizing disruption to the critical resources – the people, buildings, IT and suppliers – that support Swisscom's critical activities. Four generic disruption scenarios are defined.

These scenarios include:

- Loss of staff. Personnel with the necessary skills to ensure the continuity of Swisscom's identified critical activities are unavailable, affecting Swisscom's ability to operate.
- Loss of a building. A site, facility or building used for the production, support or delivery of one of Swisscom's identified critical activities is unavailable or fails, affecting Swisscom's ability to operate.
- Loss of ICT systems.[1] One or more ICT systems that support the delivery of Swisscom's identified critical activities are partially or completely unavailable, affecting Swisscom's ability to operate.
- Loss of a supplier. A supplier or related services used to support the delivery of a Swisscom critical activity is not available, affecting Swisscom's ability to operate.

[1] Swisscom's IT Service Management System is dedicated to the Service Continuity Management of Swisscom's critical IT services, platforms and resources. See section 2.2.

1.3 A Standardised Approach to BCM to meet Customer Expectations

Swisscom's BCMS has been established following the International Organisation for Standardisation's (ISO) Norm 22301:2019 Security and resilience — Business continuity management systems. Swisscom conducts internal and external assessments of its BCMS using this standard as a basis.

As an operator of critical infrastructure, Swisscom bears a high level of responsibility towards the Swiss society and Switzerland as a business location. As such, Swisscom is following the recommendations of several federal offices with resepct to its BCMS. Aditionally, Swisscom recognises that in some industries, particularly in the financial sector where Swisscom plays an important role as a partner and supplier, the company-wide establishment of BCM is a regulatory requirement.

Swisscom has established a close collaboration 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 follows the recommendations of the following federal offices in the implementation of its BCMS:

- Federal Office for National Economic Supply (FONES): With the so-called ICT Mimimum Standard, the Federal Office for National Economic Supply (FONES) provides operators of critical infrastructures with assistance and specific courses of action for improving their ICT resilience.
- Federal Office for Civil Protection (FOCP): Business Continuity Management is a key topic in the context of the Federal Council's National Strategy for Critical Infrastructure Protection.[2]
- Federal Office of Communications (OFCOM): sets guidelines for telecommunications service providers (TSPs) in its directive on the security and availability of telecommunication infrastructures and services [3] in order to ensure 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 the implementation of measures in the area of resilience management among operators of critical infrastructures.

[2] Currently available only in German or French.

[3] Currently available only in German or French.

2 The Swisscom Business Continuity Management System

The Swisscom BCMS has been developed to fit Swisscom's organisational context. Its operation follows best practices and aligns 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 Good Practice Guideline (2018).

2.1 Activities in Swisscom's Business Continuity Management System

The Swisscom BCMS is conducted continuously in a four-step 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).

The four active steps within the BCMS are documented with a range of deliverables. Following completion of the lifecycle, each Swisscom critical activity has a:

- Business Impact Analysis (Analysis phase) indicating the continuity requirements of the critical activity (RTO - Recovery Time Objective; and MTPD - Maximum Tolerable Period of Disruption).
- Risk Impact Assessment (Analysis phase) illustrating the potential impact of known risks on the critical resources of a critical activity.
- Business Continuity Strategy (Design phase) meeting the continuity requirements and addressing the known risks to a critical activity.
- Business Continuity Plan (Implementation phase) detailing the recovery activities for a critical activity.
- Test concept, test script and test report (Validation phase) detailing the testing results of a business continuity plan.
- Review[4] (Validation phase)

2.1.1 Analysis

The analysis phase examines Swisscom's operating environment in two parts. First, Business Impact Analyses (BIA) are conducted to identify critical activities (products, processes and services) to establish the scope of BCM at Swisscom. Criticality is determined by an assessment of the estimated financial, reputational, regulatory and operational impacts over time as a result of the loss or disruption of one of these activities. Secondly, the critical activities are examined in terms of resources required to operate and the potential impact of known enterprise, business and operational disruptive risks and threats in order to 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 and may be new or based on existing resources or arrangements, and focus specifically on the mix of resources (people, buildings, IT and suppliers) that are 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

[4] Reviews are conducted internally by the central BCM Team. Swisscom critical BCM activities are selected at random for a review.

In the Implementation phase, the continuity strategies are further detailed in recovery measures and as such built into Business Continuity Plans (BCP). These plans are integrated into Swisscom's existing response structures (Swisscom Incident Management Process and Crisis Management) to ensure that these plans can be activated quickly to ensure the continuity of Swisscom's critical activities in the event of a disruption or disaster.

2.1.4 Validation

This step ensures that Swisscom's BCMS is continuously improved. Through a variety of activities (such as exercises, reviews, internal and external audits, and management reviews *etc.*), Swisscom monitors and evaluates the activities within the BCMS, and the System itself, and makes adjustments as required. The validation step ensures that the BCMS meets the objectives set out in Swisscom's BCM Directive.

2.1.5 BCM Program Management and Embedding BCM

At Swisscom, BCM is organised and implemented using the "Three Lines of Defense" Model. The Program Management and activities to embed BCM into the culture of Swisscom are coordinated by the 2nd Line, a dedicated BCM Team positioned at the Group level (Group Security and Assurance). The central team prepares the governance documentation (BCM Directive, Policy and Instructions), the BCM training materials, and supports the business units (representing the 2nd Line) in the implementation of the BCMS. BCM at Swisscom is supported by the Executive Board, and developments, changes or adaptations are reported periodically to the Board.

2.2 Swisscom's Business Continuity Management Pillars

Swisscom's BCMS focuses on four central pillars or resources: staff, buildings, IT and suppliers. Service Continuity

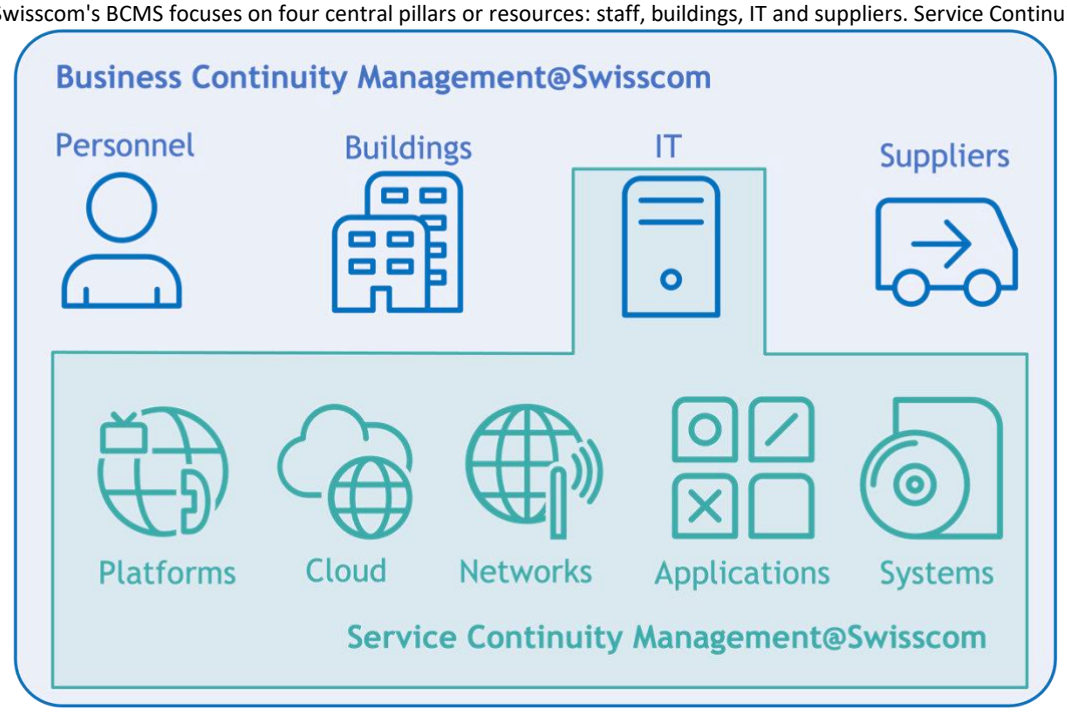

Figure 1: Business Continuity Management@Swisscom. BCM focusses on the four "pillars" of BCM (staff, buildings, IT and suppliers). Service Continuity Management (a key practice of Swisscom's Service Management System) ensures the continuous operation of IT.

Management at Swisscom is closely integrated into the BCMS, and ensures the continuous delivery of critical IT and infrastructure services. Service Continuity Management is the responsibility of the IT, Network and Infrastructure (INI) Business Unit, and is conducted within Swisscom's Service Management System (Section 3).

3 Supplementary Information: Service Management System

Swisscom's Service Management System (SMS) is aligned to the Information Technology Infrastructure Library (ITIL) 4 set of practices. An important element of the SMS are the Reliability Enhancing Procedures (REPs), which include Service Continuity Management (SCM) and are designed to continuously improve the resilience and reliability of Swisscom's ICT services and resources. As illustrated in Figure 1, Service Continuity Management develops Service Continuity Plans for Swisscom's BCM critical IT resources, and is therefor a key interface in the Swisscom BCM System.

4 Supplementary information: Risk Management

At Swisscom, risk management is designed to allow the company to meet its strategic goals while protecting the company's assets and reputation. Risk management supports business to make informed decisions based on a comprehensive knowledge of threats and their potential to cause impacts. Risk management is conducted at three levels within Swisscom: at the group level, within the business units, and in the context of security risks. The BCMS forms close interfaces with risk management at each of these levels to ensure that known risks are addressed in the development of Business Continuity Strategies (BCS) and documented in Business Continuity Plans (BCP). New risks can also be identified and documented through this process.

5 Supplementary information: Incident Management

Swisscom relies on existing response structures coordinated by the Operational Control Centres (OCC) in Berne and Zurich to manage incidents and emergencies. All incidents are managed through the Swisscom Incident Management Process. This process has proven its worth and has clearly documented sub-processes and procedures that demonstrate Swisscom's ability to respond effectively and efficiently to any incident, regardless of its cause. The process includes operational, tactical and strategic (crisis management) elements implemented through a well-established escalation model.

6 Supplementary information: Emergency & Crisis Management

Crises are sudden, extraordinary 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, with the involvement of designated representatives of Swisscom's business units. Where necessary and appropriate, Business Continuity Plans developed in the BCMS can be used to support the emergency and crisis management processes. All members of Swisscom's Emergency & Crisis Management organization receive annual training (including in the principles of business continuity management) in order to maintain skills and to perform their roles.

7 Supplementary information: Swisscom Service "ICT Business Continuity"

To support the business continuity activities and requirements of our clients, Swisscom offers the "ICT Business Continuity" product. The service guarantees the recovery of clients' business-critical systems in the event of a failure. Within this service, Swisscom provides dedicated IT resources to ensure contractually agreed recovery times in geo-redundant Tier 4 data centres. Periodic simulations of failures are used to check the business continuity functionality of the client's Swisscom provided processes and infrastructure.