SUPPLIER SHIELD

Business Continuity Management Program

Rue de la gare 39 | 1110 Morges | Switzerland | T +41 21 802 35 54 | request@suppliershield.com
https://www.suppliershield.com/

Table of Contents

1. Purpose

This document outlines Supplier Shield™ Business Continuity Management (BCM) Program. It is intended for external audiences requiring visibility in our BCM Framework. While the structure, processes, and response teams are presented, Supplier Shield™ reserves the right to omit confidential information that may compromise the employees, stakeholders or company's security and privacy.

Supplier Shield™ has developed and launched a comprehensive Business Continuity Management Program. This initiative provides a clear strategy and framework for managing business, impacting disruptive events. The program includes a structured set of requirements for establishing recovery teams and implements clear processes for execution, coordination, and recovery. Risk is inherently uncertain and subjective, shaped by the evaluator's experience, assumptions, and knowledge. A known risk may not materialize; an unknown risk may emerge unexpectedly. No process or system is entirely risk-free or immune to failure.

Supplier Shield™ does not guarantee that every risk identified will be addressed or that its business continuity plans will always function as intended. Rather, the BCM program provides a structured and strategic guide to help the organization transition in and out of a contingency operation effectively.

2. Scope

The Business Continuity Management (BCM) Program applies to all business disrupting events that may affect Supplier Shield's operations, customers, or personnel. These events include, but are not limited to, cybersecurity incidents, technological failures, natural disasters, human error, pandemics, and civil unrest, or any other regionally significant occurrences that could impact business continuity. The program includes:

- Supporting systems such as applications and cloud databases,
- Personnel, including employees, contractors, and critical third-party partners.
- Processes, procedures and other relevant documented information.

In any emergency or crisis scenario, early activation of the business continuity plan (BCP) and a clear communication strategy are part of critical actions activated allowing to return to a "business as usual" state.

To support this, Supplier Shield™ has established a dedicated Crisis Communication Team responsible for managing real-time internal and external communication during events impacting the business. While some events may not directly disrupt services or endanger personnel, those that do will prompt coordinated action between the designated teams. This integrated model ensures that a holistic and resilient response framework is aligned with the organization's continuity objectives.

3. Definitions

Term / Abbreviation	Definition
Availability	Characteristic of the information by which authorized persons can access when it is needed.
Business Continuity	The capacity of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.
Business Continuity Management (BCM)	Business Continuity Management - the overall program.
Business Continuity Plan (BCP)	Documented information that guides an organization to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives.
Business Impact Analysis (BIA)	Process of analyzing the impact over time of a disruption on the organization. The outcome is a statement and justification of business continuity.
Confidentiality	Characteristic of the information by which it is available only to authorized persons or systems.
Disruption	An incident, whether anticipated or unanticipated, which disrupts the normal course of operations at an organization's location.
Integrity	Characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
Steering Committee (SteerCo)	The Information Security Steering Committee responsible for overseeing the effective implementation of the Information Security Program (ISP), and ensuring that the confidentiality, integrity, and availability of Supplier Shield™ systems and data are maintained.
Recovery Point Objective (RPO)	Point in time to which data must be recovered after a disruption has occurred.
Recovery Time Objective (RTO)	The period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred.

4. Roles & Responsibilities

Steering Committee (SteerCo):

- Provides governance and oversight of the BCM, aligning it with security and enterprise risk management requirements.

ISMS Operation Team:

- Leads response operations for any crisis event, including activating recovery procedures.
- Coordinates all internal and external communication during crisis events, ensuring accurate and timely updates.

5. Business Continuity Management

a. Business Continuity Objectives

A Business Impact Analysis (BIA) is conducted to define the business continuity objectives for Supplier Shield™. The BIA enables the identification and assessment of all critical elements required to maintain or restore operations within acceptable timeframes. Specifically, the BIA aims to:

- Identify and classify all critical primary and supporting assets, including systems, data, facilities, and human resources.
- Determine the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for these assets.
- Define the information security and resilience controls necessary to protect these assets and ensure their recovery within the defined objectives.

The BIA is performed at least annually, or whenever a significant organizational, technological, or operational change occurs that may affect business continuity requirements.
Below are the categories of critical assets, along with the corresponding types of controls implemented to ensure their protection and recoverability.

b. Continuity of business components

Bellow are the categories of our critical assets along with type of controls implemented:

Business Components	Strategy & Controls
Suppliers	• Maintain and periodically evaluate critical suppliers to ensure continuity of services. • Perform supplier risk assessments on a regular basis. • Establish alternate or backup suppliers where feasible to mitigate dependency risks.
People Management: Loss of staff due to pandemic, regional outage, etc.	• Train and maintain qualified backup personnel to ensure competence in continuity-related activities. • Implement and support secure remote working capabilities to sustain operations during disruptions. • Maintain up-to-date, documented internal procedures for all critical activities. • Evaluate regularly continuity plans and backups through exercises and tests. • Strengthen workforce resilience through vendor-based staff augmentation when needed. • Accelerate recruitment, onboarding, and provisioning of IT equipment to minimize operational downtime. • Utilize threat intelligence and industry benchmarking to stay aligned with evolving technologies and best practices.

Information and applications	• Classify information and define protection levels according to sensitivity and business impact.
	• Perform automated backups of critical assets, including:
	  ○ Daily incremental and weekly full backups of customer data using AWS Elastic File System (EFS) in a separate AWS region.
	  ○ Database-level backups through AWS Relational Database Service (RDS) snapshots as part of the disaster recovery strategy.
	• Enable user-managed data exports through the supported backup export process.
	• Maintain a centralized documentation repository to ensure accessibility of essential information.
	• Reduce attack surface exposure using AWS Lambda and other secure architectures.
	• Conduct regular vulnerability scans and implement timely remediation actions.
	• Use collaboration and communication solutions supporting real-time interaction with partners and internal teams.

Technology	• Maintain multi-site data redundancy hosted at AWS facilities with an uptime SLA of 99.99%. • Ensure logical segregation through private cloud environments within AWS data centers. • Leverage AWS-native services and security controls to protect the Supplier Shield™ infrastructure. • Preserve operational flexibility through cloud-based architectures allowing rapid platform migration (e.g., to Microsoft Azure) in case of a major outage

c. Continuity of business functions & services

Supplier Shield™ continuity solutions are defined across different business units to ensure uninterrupted client and supplier interactions. These include alternative service channels, such as email and telephone, redundant infrastructure, and regular backups.

Business Function	Continuity Solution
Product development, Evaluators, Infrastructure	• Clients can continue to register via email and telephone. • Provide remote assistance and response. • Use alternate tools such as Excel. • Perform regular backups.
IT Security Team	• Establish redundant team members for all critical functions. • Ensure support availability across time zones for incident response.
Facilities	• Client and supplier support continues without on-site dependency.

d. Training & Awareness

At the time of this publication, Supplier Shield™ is developing the BCM program. Supplier Shield™ has implemented a formal Training and Awareness program to promote knowledge and drive readiness throughout the organization.

6. Document Control

a. Approval

This version is validated as of 01.11.2025 and supersedes all previous versions. For further information, please contact us via email: request@suppliershield.ch.

Title	**Business Continuity Management Program**
Approved By	Alexis Hirschhorn
Date of Approval	01.10.2025
Version Number	1.1

b. Version History

Version	Date	Reason for Amendment
1.0	09.09.2023	Initial version
1.0	05.10.2024	Review (no change)
1.1	01.10.2025	Annual review and update purpose, scope, roles & responsibilities, BCMP