Business Continuity Policy 2025v1

Table of Contents

1. Introduction.

Teleperformance MAR Business Continuity Policy outlines the principles and procedures for preparing for, responding to, and recovering from incidents. By following ISO 22301, the organization commits to protecting our employees, customers, and stakeholders, ensuring operational stability, and achieving our strategic objectives.

2. Objectives of the Policy.

- To establish a framework for Teleperformance MAR to ensure the continuity of its critical business functions and to minimize the impact of disruptions.
- To support the implementation, maintenance, and continual improvement of the Business Continuity Management System (BCMS) in alignment with ISO 22301:2019.

3. Scope.

- The guidelines of this policy are mandatory for all Teleperformance MAR employees, including direct and indirect employees, contractors, subcontractors, and suppliers, who provide support to the organization both from the physical facilities and from teleworking.

4. Responsibility.

- Senior Management is responsible for ensuring the resources and support necessary for compliance with this policy.
- The BCM Team is responsible for conducting annual reviews of the Business Continuity Management (BCM) including all documented information and related activities.
- Service providers, such as vendors, suppliers, and contractors, must be aware of and comply with the organization's policies.
- The communication and PR team will ensure communication and outreach in physical or digital form within the organization and accessibility to relevant internal and external stakeholders.
- Operating unit leaders are responsible for taking this policy into account in all aspects of their critical business functions and services.

5. Authority.

- Approval: Senior Management
- Review and update: Business Continuity Management System (BCMS) Leader

6. Normative References.

- ISO 22301:2019 international standard for Business Continuity Management Systems.
- ISO 31000:2018 international standard for Risk management

- GISP 14 - Information Security Aspects of Business Continuity Management Policy
- ISS.014.001 Business Continuity Management Standard

7. Pillars of the Policy.

- Ensuring the continuity of critical business activities during and after disruptive incidents.
- Meeting legal, regulatory, and contractual obligations.
- Protecting the interests of our customers, employees, shareholders, suppliers, and other stakeholders.
- Implementing a structured and effective Business Continuity Management System (BCMS) in accordance with ISO 22301:2019 international standard for Business Continuity Management Systems.
- Manage risks through the identification, assessment, and mitigation of threats, as well as the detection of opportunities that strengthen organizational resilience.
- Conducting annual business impact analyses and risk assessments to understand threats and vulnerabilities.
- Developing, maintaining, and testing business continuity strategies, plans, and procedures.
- Ensuring staff are trained and aware of their roles and responsibilities in the event of a disruption.
- Continually improving our BCMS through audits, reviews, exercises, and corrective actions.

8. Objectives of Business Continuity Management System (BCMS).

- Identify critical activities and their dependencies.
- Assess risks and impacts associated with disruptions.
- Establish effective response, recovery, and restoration strategies.
- Perform quarterly testing to demonstrate the extent to which strategies and plans are complete, current, and accurate.
- Minimize downtime and maintain an acceptable level of service.
- Ensure effective internal and external communication during incidents.
- Meet applicable compliance obligations.

9. Terms and definitions.

- **Business Continuity Management Systems (BCMS):** A comprehensive structure that guides organizations in identifying potential threats, assessing their impact on critical business functions, and formulating strategies to minimize disruption and facilitate a swift recovery.
- **Activity**: A set of one or more tasks with a defined output.
- **Audit**: Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
- **Business Continuity**: Capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.
- **Business Continuity Plan**: Documented information that guides an organization to respond to disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.

- **Business Impact Analysis**: Process of analyzing the impact over time of a disruption on the organization.
- **Competence**: ability to apply knowledge and skills to achieve intended results.
- **Continuous Improvement**: Recurring activity to enhance performance.
- **Disruption**: Any incident whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives.
- **Impact**: Outcome of a disruption affecting objectives.
- **Incident**: Event that can be, or could lead to, a disruption, loss, emergency, or crisis.
- **Prioritized Activity**: Activity to which urgency is given to avoid unacceptable impacts on the business during a disruption.
- **Risk**: Is any potential event that could interrupt an organization's critical operations, affecting its ability to deliver essential products or services.
- **Process**: Set of interrelated or interacting activities which transform inputs into outputs.
- Product And Service Output or Outcome: provided by an organization to interested parties.
- **Requirement**: Need or expectation that is stated, generally implied or obligatory.
- **Resource**: All assets (including plant and equipment), people, skills, technology, premises, and supplies and information (whether electronic or not) that an organization must have available to use, when needed, to operate and meet its objective.
- **Top Management**: Person or group of people who directs and controls an organization at the highest level.

10.Leadership.

10.1 Leadership and commitment.

10.1.1 Top management shall demonstrate leadership and commitment with respect to the BCMS by:

a) ensuring the BCMS is effectively established and aligned with the organization's context.
b) facilitating the integration of BCMS requirements into the organization's existing processes.
c) guaranteeing the availability of necessary resources to support the BCMS.
d) promoting awareness of the BCMS and communicating its significance and requirements.
e) ensuring the BCMS delivers its intended results.
f) leading and encouraging all relevant stakeholders to actively contribute to BCMS's effectiveness.
g) fostering a culture of continual improvement within the BCMS framework.

10.2 Policy.

10.2.1 The business continuity policy shall:

a) be appropriate for the purpose of the organization.
b) provide a solid framework for setting business continuity objectives.
c) include a clear commitment to meeting applicable requirements.
d) consider the continuous improvement of the BCMS.

10.2.2 The Policy shall be communicated and readily available as documented information to interested parties, as appropriate.

10.3 Roles, responsibilities, and authorities.

10.3.1 Senior management shall ensure that responsibilities and authorities for relevant functions are assigned and communicated to interested parties, as appropriate.
10.3.2 Senior management shall ensure that the BCMS complies with the requirements of this policy.
10.3.1. The BCMS leader shall report on the performance of the BCMS to senior management.

11.Planning.

11.1 Actions to address risks and opportunities.

11.1.1 Determining risks and opportunities.

11.1.1.1 The organization shall consider the requirements and determine the risks and opportunities that need to be addressed.
11.1.1.2 The organization shall give assurance that the BCMS delivers its intended results.
11.1.1.3 The organization shall prevent, or reduce, undesired effects.
11.1.1.4 The organization shall achieve continual improvement within the BCMS framework.

11.1.2 Addressing risks and opportunities.

11.1.2.1 The organization shall plan actions to address these risks and opportunities.
11.1.2.2 The organization shall integrate and implement these actions into its BCMS processes and evaluate their effectiveness.

11.2 Business continuity objectives and planning to achieve them.

11.2.1 Establishing business continuity objectives.

11.2.1.1 The organization shall establish business continuity objectives.
11.2.1.2 The organization shall be consistent with the business continuity policy.
11.2.1.3 The organization shall measure the performance of the BCMS.
11.2.1.4 The organization shall consider applicable requirements.
11.2.1.5 The organization shall communicate the policy.
11.2.1.6 The organization shall annually update or review the policy.
11.2.1.7 The organization shall retain documented information on the BCMS.

11.2.2 Determining business continuity objectives.

11.2.2.1 The organization shall plan the BCMS activities.
11.2.2.2 The organization shall allocate the necessary resources.
11.2.2.3 The organization shall define who will be responsible.
11.2.2.4 The organization shall review and evaluate the results.

11.3 Planning changes to the business continuity management system.

11.3.1 When the organization determines the need for changes to the BCMS, these shall be carried out in a planned manner and considering:

a) The purpose of the changes and their potential consequences.
b) The integrity of the BCMS and services.
c) The availability of resources in the organization.

12.Support.

12.1 Resources.

12.1.1 The organization shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the BCMS.

12.2 Competence.

12.2.1 Employees must be competent in their intended roles. To achieve this, the organization shall:

a) determine the necessary competence of employees assigned to the BCMS.
b) retain appropriate documented information as evidence of competence.
c) promote regular training in Business Continuity.

12.3 Awareness.

12.3.1 Employees doing work under the organization's control shall be aware of: a) the business continuity policy.
b) their contribution to the effectiveness of the BCMS.
c) support the continuous improvement of the BCMS.
d) the implications of not conforming with the BCMS requirements.
e) their own role and responsibilities before, during and after disruptions.

12.4 Communication.

12.4.1 The organization shall determine the internal and external communications relevant to the BCMS, including:
a) on what it will communicate.
b) when to communicate.
c) with whom to communicate.
d) how to communicate.
e) who will communicate.

12.5 Documented information.

12.5.1 The organization shall develop and maintain the documented information required for the BCMS.
12.5.2 When creating and updating documented information the organization shall follow the internal procedure: IGPC-01.
12.5.3 The documented information required by the BCMS and by this document shall be controlled to ensure compliance with the internal procedure: IG-PC-01.

13.Operation.

13.1 Operational planning and control.

13.1.1 The organization shall plan, implement, and control the processes needed to meet requirements, and to implement the actions determined by:
a) defining criteria for process execution.
b) applying controls to processes in alignment with the established criteria.
c) maintaining documented information as needed, to ensure confidence that processes are performed as intended.
d) managing planned changes and assessing the impact of unintended changes, taking corrective actions to minimize any negative effects when necessary.
e) ensuring that outsourced processes and the supply chain are effectively controlled.

13.2 Business impact analysis and risk assessment.

13.2.1 General.

13.2.1.1 The organization shall implement and maintain systematic processes for analyzing the business impact and assessing the risks of disruption.
13.2.1.2 The organization shall review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.

13.2.2 Business impact analysis.

13.2.2.1 The organization shall use the process for analyzing business impacts to determine business continuity priorities and requirements. The process shall:

a) define the types of impacts and the assessment criteria relevant to the organization's specific context.
b) identify the key activities that support the delivery of products and services.
c) apply the defined impact types and criteria to evaluate the effects of disruptions over time on these activities.
d) determine the time frame within which the organization would consider the impacts of not resuming activities to be unacceptable.
e) establish prioritized recovery time frames within the identified limits to resume disrupted activities at a minimum acceptable level.
f) use the results of this analysis to identify and prioritize critical activities.
g) identify the resources required to support these prioritized activities.
h) determine the dependencies and interdependencies of prioritized activities, including those involving partners and suppliers.

13.2.3 Risk assessment.

13.2.3.1 The organization shall implement and maintain a risk assessment process.

13.2.3.2 The organization shall identify the risks of disruption to the organization's prioritized activities and to their required resources.

13.2.3.3 The organization shall analyze and evaluate the identified risks.

13.2.3.4 The organization shall determine which risks require treatment.

13.3 Business continuity strategies and solutions.

13.3.1 General.

13.3.1.1 Based on the outputs from the business impact analysis and risk assessment, the organization shall identify and select business continuity strategies that consider options for before, during and after disruption. The business continuity strategies shall be comprised of one or more solutions.

13.3.2 Identification of strategies and solutions.

13.3.2.1 Identification shall be based on the extent to which strategies and solutions:

a) fulfill the requirements to sustain and restore prioritized activities within the defined time frames and agreed capacity levels.
b) safeguard the organization's critical activities.
c) minimize the likelihood of operational disruptions.

d) reduce the duration of any disruptions that occur.
e) mitigate the impact of disruptions on the organization's products and services.
f) ensure the availability of sufficient and appropriate resources.

13.3.3 Selection of strategies and solutions.

13.3.3.1 Selection shall be based on the extent to which strategies and solutions:
a) comply with the requirements to maintain and restore prioritized activities within the designated time frames and agreed capacity levels.
b) consider the level and nature of risk the organization is willing or unwilling to accept.
c) evaluate the related costs and benefits in decision-making.

13.3.4 Resource requirements.

13.3.4.1 The organization shall determine the resource requirements to implement the selected business continuity solutions. The types of resources considered shall include, but not be limited to:
a) Personnel.
b) information and data.
c) physical infrastructure such as buildings, workplaces, or other facilities.
d) critical utilities such as energy, water, network access.
e) equipment and consumables.

13.3.5 Implementation of solutions.

13.3.5.1 The organization shall implement and maintain selected business continuity solutions so they can be activated when needed.

13.4 Business continuity plans and procedures.

13.4.1 General.

13.4.1.1 The organization shall implement and maintain a response structure that will enable timely warning and communication to relevant interested parties.
13.4.1.2 The organization shall identify, and document business continuity plans and procedures based on the output of the selected strategies and solutions.
13.4.1.3 The procedures shall:
a) develop plans and procedures to guide the organization's response during a disruption.
b) activate business continuity solutions when necessary.
c) clearly outline the immediate actions to be taken in the event of disruption.
d) remain adaptable to evolving internal and external conditions during a disruption.

e) address the potential impacts of incidents that could lead to operational disruptions.
f) effectively reduce disruption impacts through the implementation of suitable solutions.
g) define roles and responsibilities for executing tasks within the plans.

13.4.2 Response structure.

13.4.2.1 The organization shall implement and maintain a structure, identifying one or more teams responsible for responding to disruptions.
13.4.2.2 The roles and responsibilities of each team and the relationships between the teams shall be clearly stated.
13.4.2.3 Collectively, the teams shall be competent to:
a) evaluate the nature, scope, and potential impact of disruption.
b) compare the impact against predefined thresholds to determine if a formal response is warranted.
c) initiate an appropriate business continuity response when necessary.
d) plan and coordinate the necessary response actions.
e) establish response priorities, with the health & safety of people as the highest priority.
f) continuously monitor both the disruption and the effectiveness of the organization's response.
g) deploy business continuity solutions as required.
h) communicate effectively with relevant stakeholders, authorities, and the media.
13.4.2.4 For each team there shall be:
a) personnel, along with designated alternates, must be identified and assigned with the appropriate responsibility, authority, and competence to fulfill their specific roles.
b) documented procedures must be in place to guide their actions, including protocols for activation, operation, coordination, and communication during the response.

13.4.3 Warning and communication.

13.4.3.1 The organization shall document and maintain procedures for:
a) communicate internally and externally with relevant stakeholders, specifying what information will be shared, when, with whom, and through which channels.
b) receive, document, and respond to communications from interested parties, including alerts from national or regional risk advisory systems or their equivalents.
c) ensure communication tools and channels remain operational during a disruption.
d) support structured and coordinated communication with emergency response teams.
e) outline the organization's media response following an incident, including a defined communication strategy.
f) maintain records of the disruption, including actions taken and decisions made.
13.4.3.2 Where applicable, the following additional measures should be considered and implemented:
a) notify stakeholders who may be affected by an actual or potential disruption.
b) ensure effective coordination and communication among multiple responding organizations.
c) conduct regular exercises of the warning and communication procedures as part of the organization's overall exercise program.

13.4.4 Business continuity plans.

13.4.4.1 The organization shall document and maintain business continuity plans and procedures. The business continuity plans shall provide guidance and information to assist teams to respond to a disruption and to assist the organization with response and recovery.

13.4.4.2 The business continuity plans shall clearly outline the actions that teams will undertake to:

a) maintain or restore prioritized activities within the established time frames.
b) monitor both the disruption's impact and the effectiveness of the organization's response.
c) Comply with predefined thresholds and the procedures for initiating the response.
d) Follow guidelines and procedures to ensure the delivery of products and services at the agreed capacity levels.
e) manage the immediate consequences of the disruption, with attention to individual well-being, prevention of further losses or interruptions to critical activities, and mitigation of environmental impacts.

13.4.4.3 Each plan shall include:

a) the purpose, scope, and objectives of the plan.
b) defined roles and responsibilities of the team responsible for executing the plan.
c) specific actions required to implement the planned solutions.
d) activation criteria, supporting information, operation, coordination, and communication of the team's activities.
e) identification of internal and external interdependencies.
f) required resources to support plan execution.
g) reporting protocols and requirements.
h) defined process for deactivating or standing down the plan.
i) the plans must be readily accessible and usable by all interested parties.

13.4.5 Recovery.

13.4.5.1 The organization shall have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption.

13.5 Exercise program.

13.5.1. The organization shall implement and maintain a program of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.

13.5.2. The organization shall conduct exercises and tests that:

a) align with the organization's business continuity objectives.
b) are based on well-designed scenarios with clearly defined goals and objectives.
c) enhance teamwork, build competence and confidence, and increase the knowledge of interested parties.
d) validate the effectiveness of business continuity strategies and solutions over time.
e) generate formal post-exercise reports that include outcomes, recommendations, and actions for improvement. f) are reviewed in the context of driving continual improvement.

g) are conducted at scheduled intervals and in response to significant organizational or contextual changes.

13.5.3. The organization must act on the findings from exercises and tests to implement necessary changes and improvements.

13.6 Evaluation of business continuity documentation and capabilities.

13.6.1 The organization shall:

a) assess the suitability, adequacy, and effectiveness of its business impact analysis, risk assessments, strategies, solutions, plans, and procedures.
b) perform reviews of the BCMS through, analyses, exercises, testing, and post-incident evaluations.
c) evaluate the business continuity capabilities of relevant partners and suppliers.
d) ensure compliance with applicable legal and regulatory requirements, industry best practices, and alignment with the organization's business continuity policy and objectives.
e) annually update documentation and procedures based on evaluation outcomes.
f) conduct annual evaluations, following incidents, BCP/DRP activations, or when significant changes occur.

14.Performance evaluation.

14.1 Monitoring, measurement, analysis, and evaluation.

14.1.1 The organization shall:

a) identify what aspects of the Business Continuity Management System (BCMS) need to be monitored and measured.
b) define the methods for monitoring, measurement, analysis, and evaluation to ensure accurate and reliable results.
c) define the frequency of the monitoring activities and the personnel responsible for performing them.
d) maintain appropriate documented information as evidence of monitoring and outcomes.
e) annually assess the performance and effectiveness of the BCMS.

14.2 Internal audit.

14.2.1 General.

14.2.1.1 The organization shall conduct annual BCMS internal audits to validate compliance with:

a) the ISO 22301:2019 international standard for Business Continuity Management Systems.
b) the organization's global and local requirements for Business Continuity Management Systems.
c) the requirements of this policy.

14.2.2 Audit program.

14.2.2.1 The organization shall:

a) develop, implement, and maintain an audit program that outlines the frequency, methods, responsibilities, planning requirements, and reporting.
b) request formal approval from senior management to conduct the audit process.
c) define the audit criteria and scope for each audit process.
d) consider the significance of the processes involved and the outcomes of previous audits.
e) select qualified auditors and conduct audits in a manner that ensures objectivity and impartiality.
f) ensure audit findings are communicated to senior management.
g) maintain documented evidence of the audit program's implementation and the results of each audit process.
h) take corrective actions in a timely manner to address identified nonconformities and their root causes.
i) include follow-up activities to verify the effectiveness of corrective actions and document the results of these verifications.

14.3 Management review.

14.3.1 General.

14.3.1.1 Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness.

14.3.2 Management review input.

14.3.2.1 The management review shall include consideration of:

a) the status of actions identified during previous management reviews.
b) changes in internal and external factors relevant to the BCMS.
c) identified nonconformities and the effectiveness of corrective actions.
d) results from monitoring, measurement, and evaluations.
e) findings from internal and external audits.
f) feedback received from interested parties.
g) the need for updates to the BCMS, including its policy and objectives.
h) opportunities for improvement to the BCMS performance and effectiveness.
i) insights from business impact analyses and risk assessments.
j) outcomes from evaluations of business continuity documentation and capabilities.
k) risks or issues that were not sufficiently addressed in previous risk assessments.
l) lessons learned and actions taken in response to near-misses and actual disruptions.

14.3.3 Management review output.

14.3.3.1 The output of the annual management review shall include decisions related to continual improvement opportunities and any need for changes to the BCMS to improve its efficiency and effectiveness, including the following:

a) reviews to the scope of the BCMS.
b) reviews to business impact analysis, risk assessment, continuity strategies and solutions, and BCP/DRP.
c) review procedures and controls in response to internal or external factors that may affect the BCMS.
d) defined methods for measuring the effectiveness of implemented controls.
e) retention of documented evidence as part of the management reviews.
f) communication of the results of the management review to relevant interested parties.
g) appropriate actions taken based on the findings of the review.

15.Improvement.

15.1 Nonconformity and corrective action.

15.1.1 The organization shall determine opportunities for improvement and implement necessary actions to achieve the intended outcomes of its BCMS.

15.1.2 The organization shall address nonconformities through the following actions:

a) provide an adequate response to the nonconformity.
b) implement the necessary corrective actions.
c) evaluate the effectiveness of the corrective actions taken.
d) manage any resulting consequences.
e) assess the need for further actions to eliminate the root cause(s) of the nonconformity to prevent recurrence or occurrence.
f) determine whether similar nonconformities exist or could potentially arise.
g) make the necessary changes to the Business Continuity Management System (BCMS).

15.1.3 The organization shall retain documented information as evidence of:

a) the nature of the nonconformities and any subsequent actions taken.
b) the results of any corrective action.

15.2 Continual improvement.

15.2.1 The organization shall pursue continual improvement of the Business Continuity Management System (BCMS) to enhance its suitability, adequacy, and effectiveness, using both qualitative and quantitative performance indicators.

15.2.2 The organization shall consider the results of analyses, evaluations, and management reviews to identify and address any needs or opportunities for improvement related to the business or the BCMS.

16.Change Control and Approval Cycle:

Date	Version	Description	Approval Cycle
10/06/2025	1	Document creation.	**Created:** Liliana Villar - Senior Information Security Analyst. **Reviewed:** Luis Gonzalez - Information Security Manager. **Approved:** Claudio Esteves - Chief Information Office.