Group Business Continuity Management Policy

Message from the CEO

“Temenos has an ethical and social responsibility to protect its people, its clients and all its stakeholders. This realization is at the core of its business continuity activities. Therefore, all employees need to be part of business continuity, to understand its value and to make sure that they have adequate plans in place to respond to situations that threaten our goals. “

Max Chuard, CEO

Table of Contents

Document History

Author	Version	Date
David Kelly	2.1	04/02/20
Dimitrios Spentzas	2.1	21-June-2019
Approved by the Audit Committee		17-July-2018
Dimitrios Spentzas	2.0	04-June-2018
Natarajan Swaminathan	1.2	18-Oct-2016
Natarajan Swaminathan	1.1	14-Jul-2015
Will Munro	1.0	23-Apr-2013

Comments/Change log:

Reviewed
Revised Policy for 2019 with a new message by the CEO and updated requirements in monitoring supplier in terms of continuity and resilience
Segregated objectives section to depict requirements for strategic and operational objectives
Added a commitment for continual improvement of the BCMS
Added an additional section and appendix that references to the ISO22301 requirement for highlighting the interested partied of the BCMS

1. Introduction

Background

Temenos is committed to ensure the continuity of its operations in the event of an incident that causes major disruption. To achieve this, Temenos has established Business Continuity Management (BCM) as an integral part of the company's normal business operations.
The purpose of Business Continuity Management (BCM) is to establish and maintain a framework of procedures and contingency plans, which in the event of a disruption, enable the efficient and cost effective resumption of business.
The BCM Policy provides a framework and governance structure to ensure Business Continuity Plans (BCP) are aligned to business operating requirements; are periodically tested and reviewed to ensure they remain current and effective.

1.1 Definitions

Term	Definition	Source
Business Continuity (BC)	The capability of the organization to continue delivery of products or services at acceptable pre-defined levels following disruptive incident.	ISO 22300:2012
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.	ISO 22301:2012
Business continuity plan (BCP)	Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.	ISO 22301:2012
Business impact analysis (BIA)	The process of analysing activities and the effect that a business disruption might have upon them.	ISO 22300:2012
Crisis Management	The overall coordination of an organization’s response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization’s profitability, reputation, and ability to operate.	DRI/DRJ
Incident Response Plan (IRP)	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization’s IT systems(s)	CNSSI-4009
Invocation	The act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services.	ISO 22301:2012
IT Service Continuity (ITSC) / Disaster Recovery (DR)	The technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of those operations at a more permanent site.	DRI/DRJ

Maximum acceptable outage (MAO)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. See also MTPD.	ISO 22301:2012
Maximum tolerable period of disruption (MTPD)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. See also MAO.	ISO 22301:2012
Minimum Business Continuity Objective (MBCO)	The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.	ISO 22301:2012
Organizational resilience	The ability of an organization to absorb and adapt in a changing environment.	ISO 22316:2017
Organizational resilience business function	An all-encompassing business function that includes business continuity, crisis management, security, health and safety, risk management, supply chain, corporate responsibility etc.	Policy Author
Recovery point objective (RPO)	The point to which information used by an activity must be restored to enable the activity to operate on resumption.	ISO 22301:2012
Recovery time objective (RTO)	The period of time following an incident within which a product or service must be resumed, or activity must be resumed, or resources must be recovered.	ISO 22301:2012
Resources	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective.	ISO 22301:2012
Threat Assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	CNSSI-4009

1.2 Applicability

This policy applies to:

- All Business Units and Functions within the Temenos Group
- All subsidiaries and other consolidated entities
- All Temenos Group employees and workers, as well as consultants and contractors, irrespective of their location, function, grade or standing ('staff')

The above are collectively referred to in this document as 'Business Functions' or Business Units' and/or 'Staff'.

The policy does not apply to employees of Third Parties. However, by agreement between the Temenos and the Third Party, specific control requirements may be applied to a Third Party. In such cases, obtaining the agreement of the Third Party to the control requirement(s) and the monitoring/oversight of the effective operation of the related controls will be the joint responsibility of the Group BCM Manager and the Global Sourcing Manager as per the guidelines of the Global Procurement Policy.

Compliance with the Business Continuity Management policy is mandatory.

A transition period may be appropriate for acquisitions or new entities in the Temenos Group. The transition approach must be approved through the Executive Committee.

Local regulatory obligations take priority over the requirements laid out in the policy.

1.3 Strategic Objectives

The strategic objectives of Temenos Business Continuity Management are to:

- Protect the business, including its staff, customers and shareholders, by minimizing the impact of major disruptions.
- Understand and communicate the recovery needs of the business and ensure appropriate recovery capability is provided to meet those needs;
- Recover the business in a planned and controlled manner to meet the requirements of the business and comply with applicable laws, contracts, regulations or other factors in all regions.
- Ensure that Business Continuity is an essential part of business planning and development.

1.4 Operational Objectives

In order to ensure continual suitability, adequacy and effectiveness of the Business Continuity Management System and its associated procedures, a monitoring and reporting framework shall be established and presented to Management at the beginning of each calendar year that will determine:

- Operational metrics such as measureable KPIs to check compliance with current policy requirements together with ownership and frequency of reporting as well as targets for the year
- Strategic progress indicators on BCM Strategy Group implementation
- Tactical targets for Business Continuity maturity capability increase
- Specific BCM targets relevant to Temenos structure and operating model

2. Governance framework

2.1 Roles and responsibilities

Temenos Board

- Oversee overall BCM governance and control across Temenos
- Approve BCM policy

Executive Committee

- Approve Temenos aggregate BCM risk appetite through confirming the residual risk that stems from business requirements versus IT service continuity capabilities (DR)
- Monitor aggregate BCM risk and dictate appropriate remedial action
- Approve dispensation requests i.e. requests to deviate from the BCM policy for an amount of time, in order to perform actions to close the gap between policy requirements and current status
- Allocating knowledgeable personnel and sufficient financial resources to properly implement Business Continuity
- Ensure employees are trained and aware of their roles in BCM
- Ensure Business Continuity plans are regularly reviewed, updated and tested

Group Business Continuity and Risk Manager

- Develop and maintain the Temenos BCM policy
- Coordinate and oversee all BCM documentation, planning and testing
- Report core/support function compliance with the BCM policy to the Temenos senior management
- Undertake periodic conformance reviews to monitor compliance with the Temenos BCM policy

- Provide guidance, review and oversight of any response to a customer or prospective customer (RFP/RFI responses) on Temenos BCM approach and details of BCM capability
- Provide training and awareness to all staff involved in Business Continuity activities and especially those with an active recovery role

Crisis Management Team

- Be contactable 24/7 to respond to reports of crisis events.
- Escalate issues to relevant stakeholders including external parties
- Protect Temenos public image and reputation during crisis event

Accountable Business Executive and/or Local Management Team

- Sign-off all Business Continuity Documentation confirming that these are up to date and reflect current business activities
- Ensure the BCP testing schedule is maintained and performed
- Declaring an incident and executing an Incident Response/Business Resumption Plan

Business Continuity Coordinator (BCC)

- Prepare Business Continuity Documentation for the respective business function
- Educate team members on Business Continuity recovery roles and responsibilities
- Lead yearly testing including preparation of relevant documentation
- Ensure a copy of the BCP is available at all times to all responsibility holders defined within the BCP
- Act as a single point of contact for invocation events

All Staff

- All staff should know the basic requirements for emergency procedures at their site location.
- All staff must be aware of how to report an incident or potential incident
- Communication of Temenos' BCM capability to prospects, customers and other 3rd parties must be consulted with the Group Business Continuity and Risk Manager

2.2 Interested Parties

A list of all relevant interested parties for the Business Continuity Management System according to ISO22301 guidelines are presented in Appendix 5 of this policy.

2.3 Policy Structure

Business Continuity Management is a discipline that interconnects to other core disciplines such as Risk Management, Communications, Information Security etc. The different parts of the BCM Lifecycle can be seen in the picture below. These form the general structure of the current policy.

Source: Business Continuity Institute - Good Practice Guidelines (2018)

3. Policy

- Policy and Programme Management
  - BCM Governance must be established within the business in order to provide effective authority and control. Membership must be at a level senior enough to be able to make risk and investment decisions
  - The BCM Programme must comply with the BCM Policy and any related regulatory, legal and contractual requirements
  - Business functions must report on their recovery capability and compliance with the Temenos BCM policy on a periodic basis to ensure the requirements are being met
  - BCM capability must be reported to the Executive Committee

- Analysis
  - Business Units must articulate the breakdown and relative criticality of their business activities by estimating the impact a disruption would have in terms of:
    - Damage to financial value or viability (short or long-term)
    - Damage to reputation or interested party confidence
    - Breach of legal and regulatory obligations
    - Failure to meet the strategic objectives of Temenos
  - A BIA must be completed, using the relevant templates (Appendix 2) by the business continuity coordinator and approved by the owner/accountable business executive of each core business and support function, based on risk

- The BIA should:
  - Include assessment and prioritisation of key business functions and processes, including their interdependencies
  - Identify legal, regulatory and contractual requirements
  - Identify all products, services, processes and activities prioritized by Maximum Tolerable Period of Disruption (MTPD), Recovery Time (RTO) and Recovery Point Objectives (RPO)
  - Include a risk assessment to identify, analyse and evaluate a range of risks relevant to the business unit/function
- The business functions must identify the underlying resources (people, IT systems, 3rd parties, suppliers, etc.) which support the business activities and the level at which they are required in recovery

- Design
  - BCM plans must be created for all Core/Support business and their associated IT systems to enable response to an incident and continue to provide the identified prioritised activities
  - The assumptions and scenarios for building plans are included in Appendix 1
  - BCM plans must be documented using the respective template in Appendix 2
  - Each BCM plan must have a single accountable business executive with sufficient oversight of the resources and functions provided for the respective business function. In case of absence the role can be substituted by the Business Continuity Coordinator who has first-hand knowledge of the information above
  - All plans must be kept under annual review and updated as necessary
  - Alternative working arrangements, if needed, must be defined and put in place for all staff with an active recovery role
  - Recovery provision must be deployed for all IT systems identified that support the business unit's/function's critical processes as identified in the Business Impact Analysis
  - Primary and alternate sites, if utilised, must physically be separate and operate independently

- Implementation
  - Incident Response/Business Resumption Plans (IRP/BRP) must be prepared as part of Business Continuity Management provisions. Plans must contain:
    - The nature and details of the recovery provisions (e.g. alternate sites, dependencies etc.)
    - Prioritised business activities to be supported post-incident, including timescales
    - Key contact details
    - Recovery and response tasks to be performed by the team post-incident
    - Recovery plans must be created for all people/teams and IT systems with an active recovery role
    - All plans must be kept under regular review and updated as necessary
  - IRPs/BRPs must be reviewed and signed-off by the plan owner regularly or when there is significant change to the business, its objectives or structure
  - A copy of the IRP/BRP must be available offsite even if the primary work area is lost

- Validation
  - Recovery provision must be tested annually to validate that recovery capability meets business requirements.
  - Business continuity tests and exercises must be conducted in a manner which does not put Temenos at undue risk
  - Business continuity tests and exercises must have a defined scope, success criteria and result assessment process. Appropriate documentation must be kept with timeline of events and final results

- Where deficiencies are identified in the recovery provision or associated plans, remediation activities must be put in place and tracked to completion

- ### Embedding BCM in the organizational culture

  - All staff must be made aware of the role of BCM within Temenos and their responsibilities in relation to it
  - All staff must be aware of the recovery strategy of their immediate team in the event of an incident
  - All staff with an active recovery role must be aware of their responsibilities and have the knowledge to perform the role
  - All staff with business continuity or crisis management responsibilities must complete an appropriate education and awareness programme

- ### Third Parties

  BCM is primarily concerned with third parties that supply products or services in support of critical business activities. For these third parties Temenos must:

  - Understand the ability of the third party to continue to supply or support Temenos in the event of an incident that affects either Temenos or the third party
  - Perform criticality assessment of all vendors and produce control requirements regarding BCM to the critical suppliers
  - Perform yearly assessment of the most critical suppliers to understand current level of risk in terms of continuity and resiliency
  - Create supplier contingency plans to cover cases of risk above tolerable levels

- ### Continuous Improvement

  Temenos is committed to the continual improvement of its Business Continuity Management System. Continual improvement projects are identified by making use of feedback for improvements through audit results, analysis of data and reports, corrective and preventive actions and the discussions held in management reviews and consultation with the business teams/functions in scope and employees. Adopting and implementing such initiatives for continual improvement:

  - Leads to a gradual and continual improvement of the BCMS
  - Ensures that Business Continuity scope remains continuously aligned to business requirements
  - Results in gradual improvements in cost effectiveness through a reduction in costs and/ or the capability to handle more work at the same cost
  - Identifies opportunities for improvements in all BCM stages, organizational structures, resourcing capabilities, partners, technology, staff skills and training, and communications

4. Annexes

1. Business Continuity Scenarios and Assumptions
2. BIA Template
3. BCP Template
4. Testing scripts template
5. BCMS Interested Parties