CONVERGE
ICT SOLUTIONS INC.

Business Continuity Management

POLICY

Table of Contents

1. Introduction

Converge ICT Solutions Inc. ("Converge") and its affiliates operate in a fast paced and challenging environment that is susceptible to both manmade and natural catastrophic events. The company agrees that impacts of climate change and its tightened and widened restrictions to laws and regulations, and demands for resilient, economic, sustainable and ethical programs, among many others may disrupt normal company operations and thus considers these as part of the company's top risk profile. As a risk treatment plan and in commitment to the company's mission to delight its customers by taking care of its own, and become a world class ICT organization despite such threats, the Business Continuity Management Program was established to help prevent or mitigate service disruptions and rapidly respond to any loss of essential business processes.

Under its Business Continuity Management Program, Converge expects potential events that have high risk and impact to company operations and prepares the company before, during and after it happens. The overall program of the company for Business Continuity Management System (BCMS) includes management disciplines and support, processes and equipment required to ensure that essential business processes can continue to provide service and still generate revenue in the event of a significant business disruption, which is part of our commitment with customers, regulators, investors and stakeholders.

This Business Continuity Management Program is flexible to changes in the internal and external operating environment and delivers measurable value to the organization.

2. Purpose and Scope

The purpose of this policy is to provide reasonable, but not absolute, assurance that Converge ICT Inc. will continue business operations as soon as possible after any emergency, incident or crisis event that may disrupt some if not all of the company's essential business operations. This policy serves only as a guide and shall not be the sole reference to continue business operations.

The Policy defines the ongoing management process that each business unit completes to:

- Identify potential threats which could cause a disruption in operations;
- Implement cost-appropriate actions to mitigate the likelihood and/or severity of a threat;
- Design an effective plan and strategies that recovers lost business functions with minimal downtime and safeguards the reputation of the company and its stakeholders; and
- Confirm the capability of the business units to implement the plan.

This policy applies to Converge ICT Solutions Inc. Its subsidiaries can adopt this policy when mandated by its Board of Directors.

3. Definitions

The following terms are among the business continuity management concepts mentioned in this policy:

Term	Definitions
Business Continuity	The capability 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)	The process of implementing and maintaining business continuity in order to prevent loss and prepare for, mitigate and manage disruptions.
Business Continuity Management System (BCMS)	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
Business Continuity Plan (BCP)	The documented collection of procedures and information that guides Converge ICT and its affiliates to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Business Continuity Program	The ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
Business Continuity Strategy	The strategic approach by an organization to ensure its recovery and continuity in the face of a disaster or other major incidents or business disruptions.
Business Impact Analysis (BIA)	The process of identifying the product/service delivery requirements and the prioritized timeframes for activity and resource recovery. It also identifies interdependencies between activities and dependencies on supply chains, partners and other interested parties.
Crisis	A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.
Disaster	A sudden, unplanned catastrophic event causing unacceptable damage or loss.
Disruption	An 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

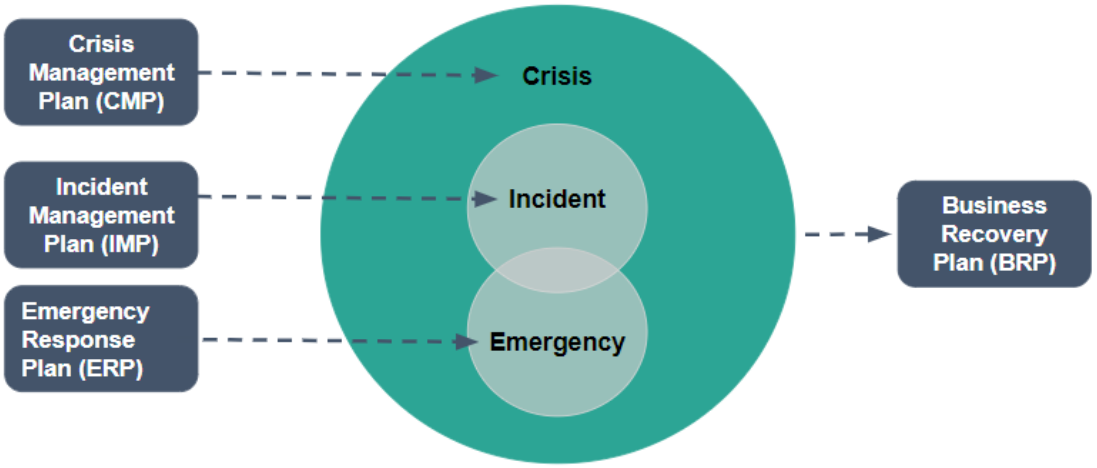
Term	Definitions
Emergency	Sudden, urgent, usually unexpected occurrence or event requiring immediate action.
Emergency Preparedness	The capability that enables an organization or community to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage.
Incident	An event that can be, or could lead to, a disruption, loss, emergency or crisis.
Maximum Tolerable Period of Disruption (MTPOD)	The amount of 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
Minimum Business Continuity Objective (MBCO)	The minimum level of service and/or products that is acceptable to the organization to achieve its business objectives during a disruption.
Recovery Point Objective (RPO)	The point to which information used by an activity must be restored to enable the activity to operate on resumption; can also refer to maximum data loss
Recovery Time Objective (RTO)	The amount of time following an incident within which: -product or service must be resumed, or -activity must be resumed, or -resources must be recovered The RTO must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

4. Policy Statement

Converge ICT Solutions Inc. Business Continuity Management Program, supported by top management leadership, sponsorship and business unit ownership, aims to build a resilient organization by mitigating the effects of disruptive events through cost effective projects and sustainable programs including mitigation/prevention, planning, preparedness, education, training, exercises and communications.

Converge is committed to implementing BCM based on BCI Good Practice Guidelines and international standard ISO 22301:2019.

5. BCM Framework

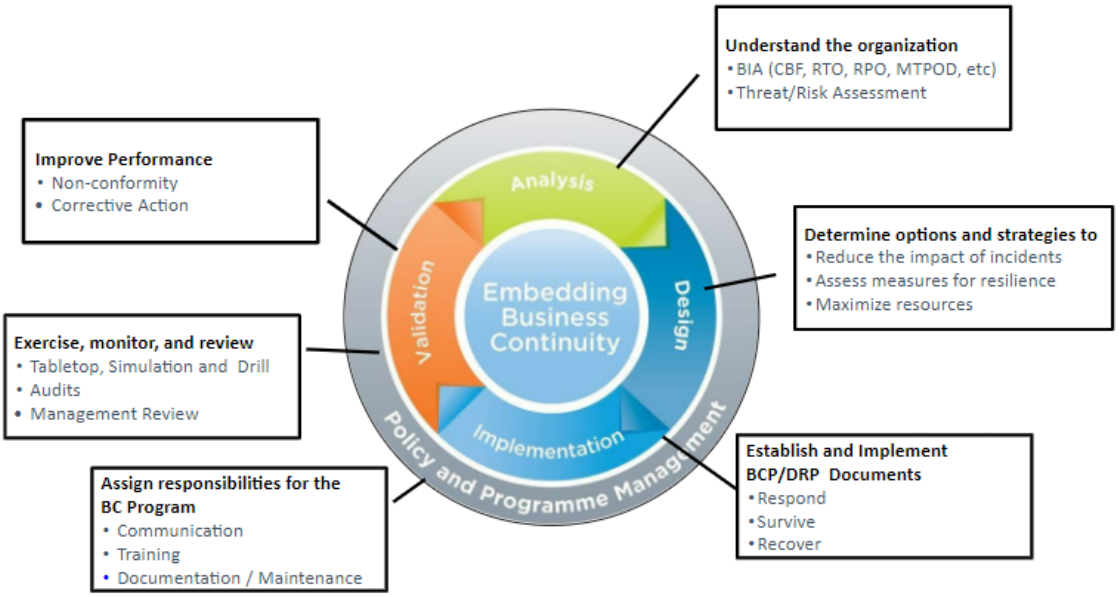


Documented procedures that guide organizations to **Respond**, **Recover**, **Resume** and **Restore** operations

The BCM Framework is designed to handle incidents depending on the needs of the business. It covers the following:

- Emergency Preparedness and Response Plan (EPRP) - to safeguard the stakeholders from harm caused by disruptive events such as the case during typhoons, flooding, earthquake, volcanic eruption, and more. This plan contains the steps to direct people and resources away from danger, holding emergency drills and training sessions, evacuating facilities and working with first responders to ensure all stakeholders are safe and sound throughout any disruptive event.
- Incident Management Plan (IMP) - to handle disruptive events immediately after it happens. It serves as the initial response to detect, manage, and contain the incident to minimize damage to company assets.
- Crisis Management Plan (CMP) - to outline how the company will respond if a crisis occurs. It contains the communication and decision-making components of the company for impact assessment and actions to contain it.
- Business Recovery Plan (BRP) - to guide the steps to take to maintain or restore the company's operations. This plan guides the company how to protect the interests of its key stakeholders, reputation, brand, and value-creating activities. Moreover, it ensures employees are able to return to work tasks following an emergency.

6. BCM Process



Converge ICT and affiliates shall adopt the process defined in ISO 22301:2019 in ensuring business continuity. Each stage of the process is detailed below as a guide from understanding the organization up to improving its performance against disruptive events.

6.1 Conducting Risk Assessment

Risk Assessment's objective is to determine the risks and analyze its impact to the company, enabling Converge ICT to evaluate and determine the most effective use of resources to reduce the impacts. It is essential to identify all risks that could disrupt the company's objectives, strategies, and operations by profiling all potential threats, analyze and evaluate each risk based on consequences or impact, likelihood of occurrence, and determining which risks require treatment.

6.2 Establishing Business Impact Analysis (BIA)

Once risk assessment is complete, it is now time to identify and prioritize which company functions and processes will have the greatest impact based on qualitative and quantitative criteria should they not be available. This criteria covers the customer impact, financial impact, regulatory impact, operational impact, reputational impact, and human impact.

During this phase, the company shall also collect information on recovery assumptions, including Recovery Point Objectives (RPO), Recovery Time Objectives (RTO), Maximum Tolerable Period of Disruption (MTPOD), internal and external interdependencies, and other special circumstances.

6.3 Developing Business Continuity Strategies

The development of business continuity strategies shall bear in mind cost-effective options in reducing deficiencies as identified during the risk assessment and business impact analysis. During its development, different perspectives must be considered (e.g., customer, supply chain, employees from all affected departments). It is also during this phase that we will validate the recovery times defined in the BIA.

6.4 Developing, Establishing, and Implementing the Business Continuity Plan

The business continuity plan aims to enable the company to continue its critical functions. This involves synthesizing the risk assessment and BIA findings, the operational, incident response, recovery, restoration, and return-to-normal operations strategies in both short or long term for either local, regional or national level into the plan.

It must also establish the roles and responsibilities, timeline, policies and procedures including any assumptions, escalation, reporting process, and recovery and restoration procedures.

The implementation of the plan shall be planned, constantly monitored, and regularly reviewed. The results shall be documented and reported as appropriate.

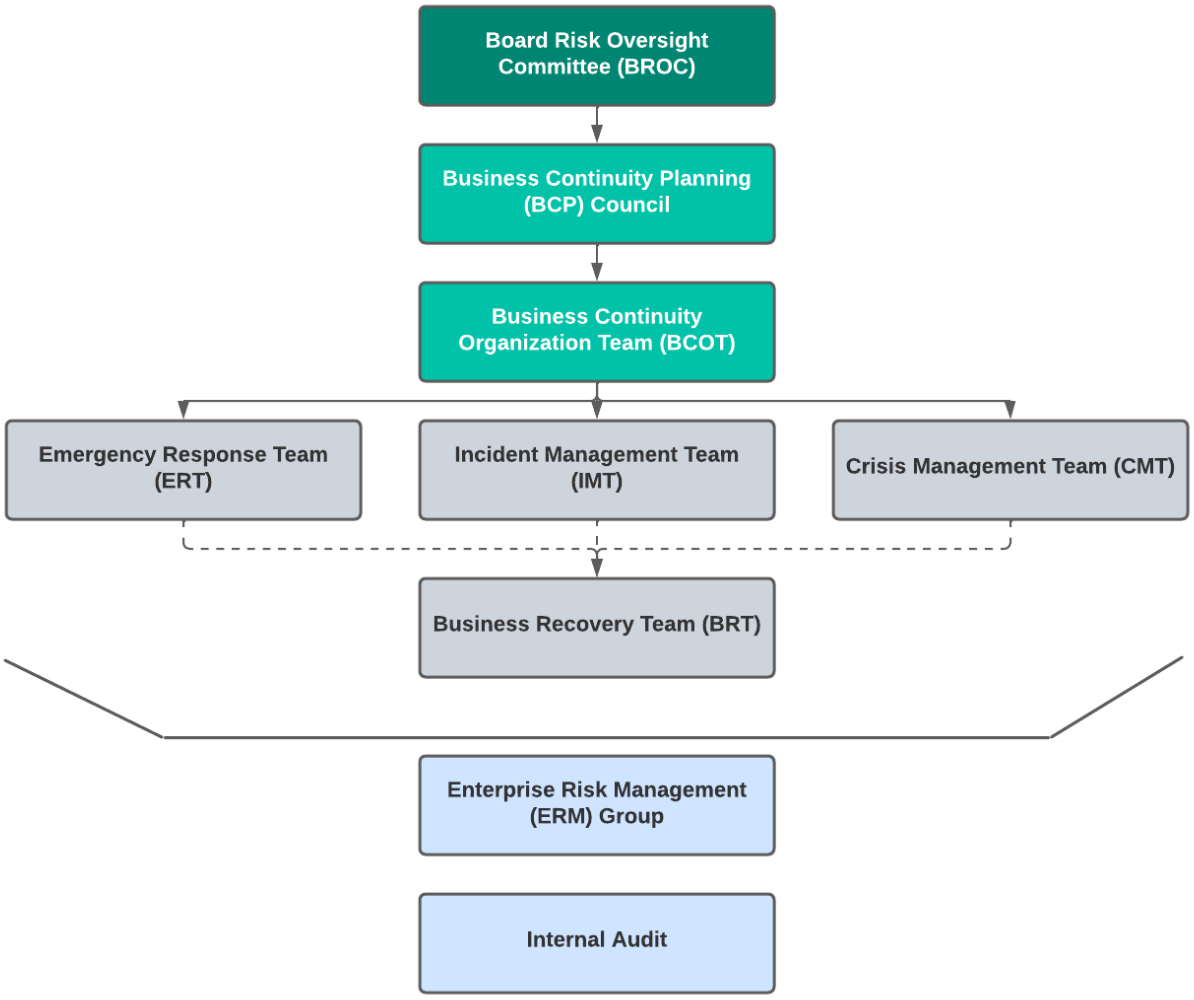
6.5 Conducting Awareness and Training Programs, BCP Exercise, Assessment, and Maintenance and Improvement of the BCP

To ensure all stakeholders are aware and prepared to act on the plan, awareness and training programs and exercises must take place. This will ensure that the policy is implemented successfully and if any discrepancies are discovered, shall be used for the improvement of the BC plan.

7. Authorities and Responsibilities

The authorities who participate in institutional Business Continuity program policy development, planning and governance, and implementation are executive management and critical processes, systems, services and applications owners. A formal Business Continuity Program governance structure shall be developed to ensure effective decision-making and compliance.

The BCM Structure of Converge is illustrated in the diagram below:



Group / Individual	Responsibilities
Board Risk Oversight Committee (BROC)	Provides an oversight role to business continuity management activities including the periodic review and approval of BCM framework and its implementation.
Business Continuity Planning (BCP) Council	Composed of Senior Leadership Team (SLT) which provides direction on the design and implementation of appropriate system, tools, and methodologies to support BCM processes and other business continuity management activities.
Business Continuity Organization Team (BCOT)	This is activated during an emergency, incident or crisis events to provide direction and control activities. The BCOT consist of the following sub-teams: a. Emergency Response Team (ERT) - this team is activated to manage and respond to any type of events which may affect the health, safety and life of individuals, especially our team members. b. Incident Management Team (IMT) - this team is activated to manage and respond to any type of incidents which affects operational, reputation, environmental, compliance and legal. c. Crisis Management Team (CMT) - this team is activated when an emergency and/or incident is unable to manage and there's a need for escalation. This team usually consists of the SLT. d. Business Recovery Team (BRT) - this team is activated to provide recovery activities. It is responsible for managing all tactical resources and overseeing recovery activities. **Note:** Specific individuals for each team are reflected in the Emergency Preparedness and Response Plan (EPRP), Incident Management Plan (IMP), Crisis Management Plan (CMP), and Business Recovery Plan (BRP) documents.
ERM Department (ERMD)	Facilitates, supports and integrates the BCM processes across Converge in coordination with the CRO and BCM Champions.
Internal Audit	Provides an independent assessment of the BCM framework on an enterprise-wide basis.

8. External Parties

Whenever applicable, each Business Unit (BU) shall also identify external interested parties that have business continuity requirements affecting the services/products of the BU. These shall include but not limited to the following:

Group / Individual	Role
Clients/Customers	A group or individual using Converge services.
Regulators	A group or an individual that checks whether Converge is working in accordance with government requirements, rules or laws. Regulators include but are not limited to the following: Securities and Exchange Commission (SEC), Philippine Stock Exchange (PSE), National Telecommunications Commission (NTC), Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE).
Service Providers/Suppliers	An entity or a person which provides and delivers services/supplies to Converge under an agreement.
Investors	A group or individuals who commits capital with expectation of receiving financial returns.

9. Policy Review

This Business Continuity Management Policy shall be reviewed by the Converge ICT Enterprise Risk Management Group at least annually to ensure its continuing adequacy and consistency with the company's goals and responsibilities.

10. Effectivity and Compliance

This policy will take effect immediately upon its approval. The Enterprise Risk Management Group is tasked to disseminate and enforce this policy enterprise-wide.

11. Related Document References

11.1 ISO 22301:2019 Societal Security-Business Continuity Management Systems-Requirements
11.2 BCI Good Practice Guidelines 2018 Lite Edition
11.3 DRI International Glossary for Resilience (Version 2 - July 2018)