Enhancement of Private Sector Capacities
On Disaster Risk Reduction and Management

BUSINESS CONTINUITY MANAGEMENT (BCM) SYSTEM
ISO 22301:2019

Handbook for Training of Trainers

DMC SRI LANKA

WFP World Food Programme

The Ceylon Chamber of Commerce

Enhancement of Private Sector Capacities
On Disaster Risk Reduction and Management

BUSINESS CONTINUITY MANAGEMENT (BCM) SYSTEM
ISO 22301:2019

Handbook for Training of Trainers

BUSINESS CONTINUITY MANAGEMENT (BCM) SYSTEM
ISO 22301:2019

Handbook for Training of Trainers

MESSAGE FROM THE SECRETARY MINISTRY OF INDUSTRY AND ENTREPRENEURSHIP DEVELOPMENT

I am pleased to extend my endorsement for the development of the Business Continuity Management System (BCMS) Handbook and Curriculum, funded by the World Food Programme (WFP) and technically supported by the Disaster Management Centre and the Ceylon Chamber of Commerce.

This initiative is a significant step toward strengthening the resilience of Sri Lankan small and medium enterprises (SMEs), enabling them to continue business operations during disaster situations.

SMEs are vital to our nation's economy but remain highly susceptible to disruptions caused by natural disasters, economic shocks, and other unforeseen challenges. The creation of a practical handbook and curriculum under the BCMS framework will equip businesses with the necessary strategies, tools, and preparedness measures to mitigate risks, safeguard livelihoods, and ensure business continuity.

The Ministry of Industries commends the collaborative efforts of World Food Prgramme, Disaster Management Centre and the Ceylon Chamber of Commerce in driving this crucial capacity-building initiative. We are confident that the BCMS handbook and curriculum will serve as an invaluable resource for SMEs, helping them to build resilience and contribute to a more stable and sustainable economic environment.

J M Thilaka Jayasundara
Secretary
Ministry of Industry and Entrepreneurship Development

MESSAGE FROM THE DIRECTOR GENERAL, DISASTER MANAGEMENT CENTRE

It is with great appreciation that I extend my support to the development of the Business Continuity Management System (BCMS) Curriculum and Handbook, an initiative funded by the World Food Programme (WFP) and technically supported by the Ceylon Chamber of Commerce.

Disasters whether natural or man-made pose significant threats to economic activities and the livelihoods they sustain. Small and medium enterprises (SMEs), in particular, are often the most vulnerable to disruptions. Establishing a structured BCMS is critical for ensuring that businesses are prepared to respond effectively and recover quickly from such events.

The Disaster Management Centre recognizes the importance of this initiative in building a culture of preparedness and resilience within the private sector. By equipping businesses with practical tools, knowledge, and strategies for continuity, the BCP Curriculum and Handbook will not only protect individual enterprises but also strengthen the overall socio-economic fabric of our nation.

We commend the collaborative efforts of all partners involved and reaffirm our commitment to supporting programs that enhance disaster risk reduction and resilience across all sectors.

Maj Gen Sampath Kotuwegoda (Retd.) ndc IG
Director General
Disaster Management Centre

MESSAGE FROM THE COUNTRY DIRECTOR A.I THE UNITED NATIONS WORLD FOOD PROGRAMME

It is with profound pride that I present the Business Continuity Management System (BCMS) Handbook and Curriculum a collaborative milestone of the Disaster Management Centre, United Nations World Food Programme (UN WFP), and the Ceylon Chamber of Commerce.

As an organisation with a mandate of saving and changing lives, we recognise the pivotal role of the private sector in sustaining the basic needs of communities in times of crisis. Whether confronting natural disasters, public health emergencies, or operational disruptions, the ability and resilience of businesses to continue functioning are vital to safeguarding the most vulnerable populations.

This handbook and curriculum provide a practical yet strategic framework to guide private sector entities in preparing for, responding to, and recovering from unforeseen events and challenges, while ensuring the continuity of essential services when needed most.

We trust this handbook will catalyse building resilient and robust business continuity management systems, empowering organisations to thrive even in the face of adversity.

Robert Oliver
Country Director a.i
World Food Programme, Sri Lanka

MESSAGE FROM THE SECRETARY GENERAL AND CEO OF THE CEYLON CHAMBER OF COMMERCE

The Ceylon Chamber of Commerce is proud to facilitate the development of the Business Continuity Management System (BCMS) Handbook and Curriculum, initiated by the World Food Program with the guidance of Disaster Management Centre (DMC) to strengthen the resilience of small and medium enterprises (SMEs) in Sri Lanka.

SMEs are the backbone of our economy, yet they are often the most vulnerable during disasters and disruptions. The development of this handbook and curriculum is a critical step toward equipping businesses with the tools, knowledge, and frameworks needed to anticipate risks, maintain operations, and recover swiftly from adverse events.

Through this initiative, the Chamber reaffirms its commitment to empowering the private sector with best practices in risk management and disaster preparedness. We believe that a well-prepared business community contributes not only to economic stability but also to the overall resilience and sustainability of our nation.

We extend our sincere appreciation to the World Food Progarmme and all stakeholders for their collaboration in making this initiative a reality.

Buwanekabahu Perera
Secretary General and CEO
Ceylon Chamber of Commerce

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Sri Lanka faces significant natural disaster risks, worsened by socio-economic vulnerabilities, highlighting the need for enhanced resilience. Recognizing the private sector's critical role in Disaster Management, Risk Reduction, and Climate Services, the World Food Program (WFP), in partnership with the Ceylon Chamber of Commerce (CCC) and the Disaster Management Centre (DMC), is implementing a program to strengthen business resilience. This initiative supports enterprises in vulnerable sectors by developing Business Continuity Management Systems (BCMS) to mitigate disaster impacts and ensure continuity. To foster a BCMS ecosystem, the program includes a structured trainer training curriculum to build expertise in business continuity.

The Business Continuity Management System (BCMS) Participant's Handbook is the key resource for participants of the BCMS Trainer Training Program, a strategic initiative designed to strengthen organizational resilience through a network of certified BCMS trainers. The training program addresses critical gaps in disaster preparedness and business continuity planning, particularly within Small and Medium Enterprises (SMEs), which often lack structured business continuity measures due to low awareness, inadequate access to technical support, and financial constraints.

This training equips participants with a comprehensive understanding of the ISO 22301:2019 framework, offering sector-specific strategies to manage risks and enhance resilience in key industrial sectors such as agriculture, plantation, tourism, apparel, and fisheries.

Designed as an interactive learning resource, the handbook provides theoretical insights, practical exercises, and scenario-based training, covering BCMS principles, risk assessment, business impact analysis, and continuity planning. It serves as a structured learning guide, complemented with PowerPoint presentations, which include case exercises, studies, and tabletop exercise scenarios to enhance training delivery.

Beyond the training, the handbook continues to support the participants in establishing and implementing BCMSs within organizations. The BCMS Trainer Training Program is a forward-thinking initiative that not only enhances individual capacity but also contributes to Sri Lanka's broader disaster resilience goals by embedding sustainable business continuity principles within the SME ecosystem. By creating a network of skilled trainers, the program strengthens national resilience-building initiatives, promotes BCMS best practices, and fosters BCMS-compliant supply chains, ultimately enhancing economic stability and community resilience.

HOW TO USE THIS BCMS HANDBOOK

This handbook has been developed to serve both as a self-study guide for preparing a Business Continuity Management System (BCMS) within their organizations and as a reference manual for trainers and consultants delivering BCMS training and advisory services. It has been designed in alignment with ISO 22301:2019, the international standard for BCMS, and is intended for practical use by small and medium-sized enterprises (SMEs), institutions, and facilitators. Each chapter of this handbook presents essential concepts and a step-by-step approach to building key components such as continuity policies, risk assessments, business impact analyses, recovery/continuity strategies, testing, and improvement mechanisms.

To support practical application, the handbook should be used together with the attached BCMS Exercise Workbook. Each chapter corresponds to a specific exercise designed to help users apply what they've learned and begin drafting the BCMS manual for an organization. For example, after reading Chapter 4, users should complete Exercise 4 in the workbook. Exercises start from chapter 4. These exercises are intended to turn learning into action and directly contribute to building a functional BCMS.

Alongside the handbook and workbook, a set of PowerPoint presentations is provided to support structured training and consultancy. These slides highlight key points from each chapter and help to explain concepts, lead discussions, and guide exercises. Trainers delivering formal sessions may use the slides to introduce each chapter, then allow participants to explore the content in detail using the handbook, followed by engaging them in completing the related exercise in the workbook. Consultants may also find these materials useful when guiding clients through BCMS implementation processes.

Case studies included in this handbook also serve to further illustrate how Business Continuity Management concepts are applied in real-world situations across different sectors and environments. They provide practical examples that show how organizations identify risks, respond to disruptions, and implement continuity strategies. The case studies can be used to spark discussions, compare approaches, or encourage participants to reflect on how similar practices can be adapted within their organizations.

This handbook should be viewed as a living document. Users are encouraged to adapt the content and examples to suit their local context, regulatory environment, and organizational priorities. The handbook and its accompanying materials may be revised over time to reflect new learning, feedback from implementation, and changes in international standards or best practices.

GLOSSARY

ADPC	Asian Disaster Preparedness Center
ANZ	Australian Standard
BCI	Business Continuity Institute
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BOD	Board of Directors
BS	British Standard
BSI	British Standards Institution
CBSL	Central Bank of Sri Lanka
CCC	Ceylon Chamber of Commerce
DM	Disaster Management
DMC	Disaster Management Center
DRI	Disaster Recovery Institute
DRM	Disaster Risk Management
DRR	Disaster Risk Reduction
EOC	Emergency Operation Center
FI	Financial Institutes
HNB	Hatton National Bank
IBSL	Insurance Board of Sri Lanka
ICT	Information Communication Technology
ILO	International Labour Organization
ISO	International Organization for Standardization
IT	Information Technology
MBCO	Minimum Business Continuity Objective
MSME	Micro, Small, and Medium Enterprises
MTPD	Maximum Tolerable Period of Disruption
NBRO	National Building Research Organization
NDMP	National Disaster Management Plan
NEOP	National Emergency Operation Plan
NIST	National Institute of Standards and Technology
PA	Prioritized Activity
PDCA	Plan-Do-Check-Act
RA	Risk Assessment
RTO	Recovery Time Objective
SLPP	Sri Lanka Preparedness Partnership
SME	Small and Medium Enterprises
SS	Singapore Standard
UK	United Kingdom
UN	United Nations
US	United States
WFP	World Food Program
Y2K	The Year 2000

BCMS VOCABULARY

Alternate Worksite

Work location, other than the primary location, to be used when the primary location is not accessible

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 Management

Process of implementing and maintaining business continuity

Business Continuity Management System

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity

The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes, and resources.

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

Maximum Tolerable Period Of Disruption MTPD

maximum acceptable outage MAO

Time it would take for adverse impacts, which can arise as a result of not providing a product/ service or performing an activity, to become unacceptable

Minimum Business Continuity Objective MBCO

Minimum capacity or level of services and/or products that is acceptable to an organization to achieve its business objectives during a disruption

Prioritized Activity

Activity to which urgency is given to avoid unacceptable impacts on the business during a disruption

Recovery Point Objective RPO

Point to which information used by an activity is restored to enable the activity to operate on resumption

Can also be referred to as “maximum data loss”.

Recovery Time Objective RTO

Period of time following an incident within which a product and service or an activity is resumed, or resources are recovered

For products, services, and activities, the RTO is 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.

Residual Risk

Retained risk; risk remaining after risk treatment; It represents the risk that cannot be completely eliminated, even after applying all reasonable safeguards.

Residual risk can contain unidentified risks.

Resilience

Ability to absorb and adapt to a changing environment

In the context of urban resilience, the ability to absorb and adapt to a changing environment is determined by the collective capacity to anticipate, prepare, and respond to threats and opportunities by each component of an urban system.

Risk

Effect of uncertainty on objectives

An effect is a deviation from the expected. It can be positive, negative, or both, and can address, create, or result in opportunities and threats.

Objectives can have different aspects and categories and can be applied at different levels.

Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood.

Risk Acceptance

Informed decision to take a particular risk

Risk acceptance can occur without risk treatment or during the process of risk treatment.

Accepted risks are subject to monitoring and review.

Risk Analysis

Process to comprehend the nature of risk and to determine the level of risk

Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk analysis includes risk estimation.

Risk Appetite

amount and type of risk that an organization is willing to pursue or retain

Risk Assessment

Overall process of risk identification, risk analysis, and risk evaluation

Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

Risk Communication

Exchange or sharing of information about risk between the decision maker and other interested parties

The information can relate to the existence, nature, form, probability, severity, acceptability, treatment, or other aspects of risk.

Risk Criteria

Terms of reference against which the significance of a risk is evaluated

Risk criteria are based on organizational objectives and external and internal context.

Risk criteria can be derived from standards, laws, policies, and other requirements.

Risk Evaluation

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk evaluation assists in the decision about risk treatment.

Risk Identification

Process of finding, recognizing, and describing risks

Risk identification involves the identification of risk sources, events, their causes, and their potential consequences.

Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and interested parties' needs.

Risk Management

Coordinated activities to direct and control an organization with regard to risk

Risk Mitigation

lessening or minimizing the adverse impacts of a hazardous event

Risk Reduction

Actions taken to lessen the probability of negative consequences, or both, associated with a risk

Risk Sharing

Form of risk treatment involving the agreed distribution of risk with other parties

Legal or regulatory requirements can limit, prohibit, or mandate risk sharing.

Risk sharing can be carried out through insurance or other forms of contract.

The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

Risk transfer is a form of risk sharing.

Risk Treatment

- Process to modify risk
- Risk treatment can involve:
- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing risk to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention,” and risk reduction.

Risk treatment can create new risks or modify existing risks.

Supply Chain

Two-way relationship of organizations, people, processes, logistics, information, technology, and resources engaged in activities and creating value from the sourcing of materials through the delivery of products or services

The supply chain may include vendors, subcontractors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user.

Vulnerability

Vulnerability analysis

Process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence

1. INTRODUCTION

Business organizations strive to create a positive impact on society by delivering high-quality products or services that fulfill customer needs and enhance community well-being. At the same time, they prioritize the safety and well-being of their employees, recognizing them as their most essential resource. However, true success involves not only thriving during favorable conditions but also maintaining operations during challenging times, such as crises or disasters. Organizations must compete effectively in ordinary circumstances while also building resilience to survive and thrive during unexpected events or stresses (Table 1: Types of stress and impacts on businesses) like natural disasters, accidents, or other disruptions. No organization anticipates being destroyed by such incidents, but failing to prepare leaves them vulnerable.

Table 1: Types of stress and impacts on businesses

Stress Type	Examples	Business Impact
Climate & Environmental	Floods, droughts, landslides	Physical damage, lost production
Social & Workforce	Strikes, health crises	Labor disruptions, safety issues
Market & Economic	Inflation, market loss	Reduced revenue, cost increases
Regulatory & Policy	New laws, sanctions	Legal risk, halted operations
Technological & Cyber	Hacking, system failures	Data loss, interruption, compliance risk

As Benjamin Franklin famously said, “Failing to prepare is preparing to fail.” Without adequate preparation, an organization effectively sets itself up for failure when disaster strikes. A Business Continuity Management System (BCMS) offers a proactive approach to ensuring a business can withstand crises and continue to operate effectively.

Disruptions can significantly impact an organization’s ability to operate and deliver its products or services. Establishing a BCMS in advance, rather than reacting after an incident, enables the organization to respond swiftly and efficiently. This proactive approach helps restore operations before critical impacts occur, ensuring the organization’s resilience and continued success even in challenging circumstances.

1.1. BCMS in Disaster Management System in Sri Lanka

In Sri Lanka, the Business Continuity Management System (BCMS) is a crucial component of the Disaster Management (DM) framework, aligning with the National Disaster Management Plan (NDMP) 2023-2030 and the National Emergency Operations Plan (NEOP) to enhance resilience and preparedness.

BCMS plays a vital role across all phases of the disaster management cycle, from prevention to preparedness to response to recovery. It enables businesses to maintain critical operations during disasters and recover swiftly. The NDMP identifies the private sector as a key player in disaster resilience, emphasizing business continuity in manufacturing, production, services, and employment.

Chapter 3.14 of the NDMP and Operational Sub-Strategy 3.4 focuses on engaging Micro, Small, and Medium Enterprises (MSMEs) to adopt risk-informed, and climate-resilient investments, promoting BCMS with technical assistance from the Ceylon Chamber of Commerce (CCC). This strategic approach ensures operational continuity, minimizes economic losses, and supports community resilience, all contributing to national socio-economic stability.

The NEOP further reinforces the private sector's role in disaster response, advocating for active involvement from national to subnational levels and enhancing collaborative emergency management efforts. Institutional disaster management plans, including BCMS frameworks, are essential for safeguarding economic stability, reducing operational disruptions, and promoting a culture of resilience within Sri Lanka's broader disaster management strategy.

The Sendai Framework for Disaster Risk Reduction (SFDRR) 2015–2030 emphasizes reducing disaster risks and building resilience at all levels, while a Business Continuity Management System (BCMS) ensures organizations can continue operations and recover quickly from disruptions. Both frameworks share common goals in enhancing preparedness, risk management, and resilience. The key alignments between BCMS and the Sendai Framework are:

- Understanding Disaster Risk: BCMS uses Business Impact Analysis (BIA) and Risk Assessments to identify vulnerabilities and critical processes.
- Strengthening Disaster Risk Governance: BCMS establishes a structured governance framework for business continuity.
- Investing in Disaster Risk Reduction for Resilience: BCMS includes risk mitigation strategies, such as redundant systems, alternative supply chains, and crisis response planning, and Encourages investment in technology, infrastructure, and capacity building.
- Enhancing Disaster Preparedness and "Build Back Better": BCMS develops and tests Business Continuity Plans (BCPs) to ensure readiness for crises.

1.2. Enhancing Private Sector Resilience through BCMS

The private sector is vital to the economy, with its resilience impacting communities, supply chains, and national recovery during disasters. BCMS provides a structured approach to embedding resilience, aligning with Disaster Risk Management (DRM) principles. By adopting BCMS, organizations can mitigate disaster-related losses, support societal recovery, and ensure long-term sustainability.

Small and Medium Enterprises (SMEs), the backbone of local economies, are especially vulnerable due to limited resources and tight margins. Tailoring BCMS to their needs enhances their ability to withstand disruptions, making it a strategic asset rather than just a survival tool. By integrating BCMS, SMEs can protect their businesses, support community resilience, and strengthen disaster risk management efforts, contributing to stable and thriving economies.

1.3. SME's Business Resilience: Challenges and Gaps

The Capacity Needs Mapping of SMEs in Disaster Risk Reduction and Management was conducted by the World Food Program (WFP) in collaboration with the Ceylon Chamber of Commerce (CCC) and examined the private sector's disaster preparedness and response capabilities. The study highlighted critical challenges and gaps for strengthening SME resilience, as described below.

- Small and Medium Enterprises (SMEs) are a cornerstone of the Sri Lankan economy, representing over 75% of all businesses (Source: Ministry of Industry & Commerce, 2013). Despite their critical role, many SMEs lack structured Business Continuity Plans, leaving them vulnerable to business interruptions. This vulnerability stems from limited financial resources, insufficient awareness, and inadequate technical support, preventing effective resilience planning. With tight profit margins, SMEs struggle to allocate resources for long-term resilience, increasing their susceptibility to natural disasters.
- The absence of formal risk assessments and preparedness plans among SMEs is a significant concern. The recent survey indicates that around 55% of businesses, particularly SMEs, either rely on informal measures or lack preparedness protocols altogether, unlike larger enterprises. Many SMEs do not have emergency response plans or are unsure of their existence.
- Resource availability for BCMS is a critical concern, with only 25% of businesses having sufficient financial, equipment, and trained personnel to manage business interruptions effectively. This challenge is more severe for SMEs due to severe resource constraints.
- Training and capacity building for BCMS are significant challenges for smaller businesses. Limited access to relevant training programs, coupled with existing training programs that do not meet industry-specific or regional needs, has resulted in a lack of knowledge of BCMS, low employee awareness, unclear roles and responsibilities, and poor collaboration during emergencies.

- Infrastructure and Technology Preparedness also emerged as pivotal challenges for SMEs' business resilience. Many SMEs lack the financial capability to invest in infrastructure improvements with stronger building materials and resilient construction designs. While awareness of technological preparedness is relatively high, a significant number of businesses have not tested their systems, leading to weaknesses in communication systems, emergency alerts, and business continuity technologies.
- Investments in disaster preparedness are inadequate, with only 15% of businesses having allocated specific budgets for disaster risk management activities. Limited profitability, constrained cash flows, and distrust in insurance products often contribute to this shortfall, leaving SMEs extremely vulnerable in the event of a disaster, leading to longer recovery times and increased reliance on external aid.
- Survey finding reveals a significant gap in learning from past disasters. Despite over 60% of businesses experiencing a disaster within the past five years, the majority of them did not conduct a formal review to assess their responses or document lessons learned. This highlights a missed opportunity to build resilience by integrating past experiences into future preparedness strategies.

Addressing these gaps is essential for building a more resilient SME sector capable of sustaining operations during crises and contributing to national disaster risk management efforts.

1.4. Enhancing SME Resilience through Business Continuity Management System

Addressing the challenges and gaps in SME resilience, the program focuses on developing expertise in Business Continuity Management (BCMS). It emphasizes tailored capacity-building initiatives designed to address the specific risks and requirements of different sectors. In meeting mass-scale enterprise needs while ensuring the long-term sustainability of knowledge and capacity retention, it has focused on a trainer-training module aligned with the ISO 22301:2019 standard for Business Continuity Management (BCMS). This training not only raises awareness but also builds the practical capacity to handle emergencies.

Building foundational knowledge on BCMS, this training program introduces SMEs to ISO 22301:2019 standards, focusing on identifying prioritized business processes and assessing risks specific to business types. Through interactive sessions, case studies, and scenario planning exercises, participants gain a proper understanding of the critical role of BCMS in ensuring business resilience.

The program offers tailored training modules to address the diverse needs of different sectors, particularly agriculture, plantation, tourism, apparel, and fisheries. It provides sector-specific guidance on managing risks, such as droughts and pest infestations, in agricultural businesses, while focusing on safeguarding supply chains and critical infrastructure in manufacturing enterprises. This customized approach ensures that SMEs develop sector-specific strategies to mitigate the risks effectively.

In national economic development agendas, SMEs are encouraged to operate within intricate supply chains, particularly in just-in-time delivery models. The training program focuses on integrating suppliers into business continuity plans, developing shared frameworks, and establishing predefined emergency protocols to build a BCMS-compliant business ecosystem. This approach enhances SMEs' resilience and minimizes the ripple effects of disruptions across supply chains.

Strengthening physical and technological resilience, the program guides SMEs on retrofitting existing infrastructure with robust building standards and formal drainage systems. It also encourages adopting technology solutions such as mobile-based systems and remote monitoring tools through partnerships with tech firms offering affordable, tailored solutions.

The training program introduces budgeting strategies for BCMS activities, explores affordable insurance products, and encourages the development of contingency funds. These measures aim to reduce SMEs' reliance on external aid and improve their ability to recover swiftly from crises.

Additionally, the program focuses on conducting formal reviews of past incidents to evaluate responses and document lessons learned. This practice promotes continuous improvement and helps businesses refine their emergency protocols based on real-world experiences, ultimately contributing to a culture of resilience.

2. BUSINESS CONTINUITY MANAGEMENT SYSTEM: WHAT? AND WHY?

Business continuity is the capability of an organization to continue the delivery of products or services at acceptable predefined capacities following a disruption. Business continuity management is the process of implementing and maintaining business continuity to prevent loss and prepare for, mitigate, and manage disruptions. It is equally applicable to large, medium, and small organizations operating in industrial, commercial, public, and not-for-profit sectors. However, large enterprises and SMEs vary widely in resource availability and allocation, affecting their capacity to prepare for, respond to, and recover from crises. **Table 2** describes the human, physical, and financial resource availability by large enterprises and SMEs.

Table 2: Comparison of Resources for Meeting Emergency Needs in Large vs Small Enterprises

	Large Companies	SMEs
Human	Large companies often have more personnel available when restoring business operations to pre-disaster levels by transferring employees. Employees may be able to work from home if the company has sufficient technological resources.	Small businesses often do not have employees who can help restore operations since they have alternative livelihoods. Business owners who are injured may face significant setbacks until the owner is able to physically operate the company.
Physical	Large companies can mitigate the loss of business assets from natural disasters by operating multiple locations with multiple business assets. If one location is inoperable, larger companies can transfer operations to another facility to maintain normal production output.	Small businesses usually operate in a single location, commonly the home. Disasters may significantly damage the assets discontinuing operations. SMEs may spend considerable amounts of time to repair or wait until they can obtain a replacement.

Financial	If disasters are particularly devastating, large companies may have additional capital for restoring business operations. Insurance may also cover the losses financing resumption of business activities.	Small businesses do not usually have amounts of capital to pay for personal or business expenses resulting in obtaining external financing for operations, which may lead to future cash outflows. Small companies are reluctance to insure against natural disaster losing the opportunity for resumption of activities.

2.1. Benefits of implementing BCMS

Disruptions to business activities can arise from a wide variety of incidents, many of which are difficult to predict or analyze. By focusing on the impact of disruption rather than the cause, business continuity enables an organization to identify activities that are essential to its ability to meet its obligations. Business Continuity further enables an organization to determine the necessary actions to protect its resources, such as personnel, facilities, technology, information, supply chain, interested parties, and reputation before a disruption occurs. With that recognition, the organization can put in place a response structure, so that it can be confident of managing the impacts of a disruption. Business continuity can be effective in dealing with both sudden disruptions and gradual ones. The following figures conceptually illustrate how business continuity can effectively mitigate impacts in these situations.

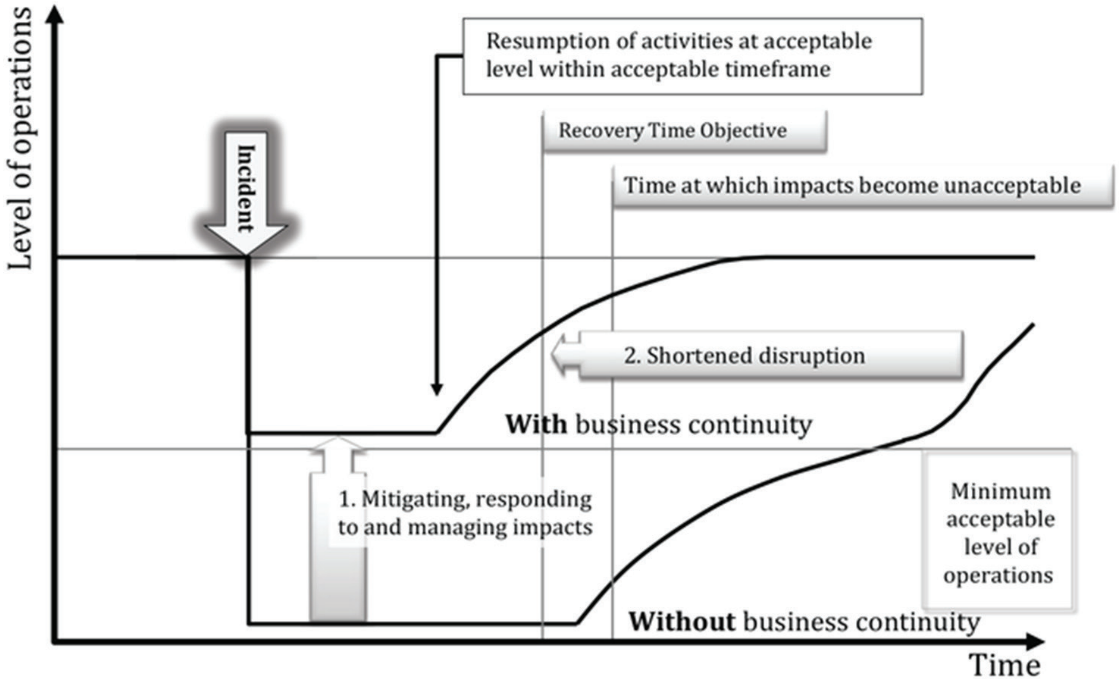

Level of operations
Incident
Resumption of activities at acceptable level within acceptable timeframe
Recovery Time Objective
Time at which impacts become unacceptable
2. Shortened disruption
With business continuity
1. Mitigating, responding to and managing impacts
Minimum acceptable level of operations
Without business continuity
Time

Figure 1: Illustration of business continuity being effective for sudden disruption
Source: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en:sec:8

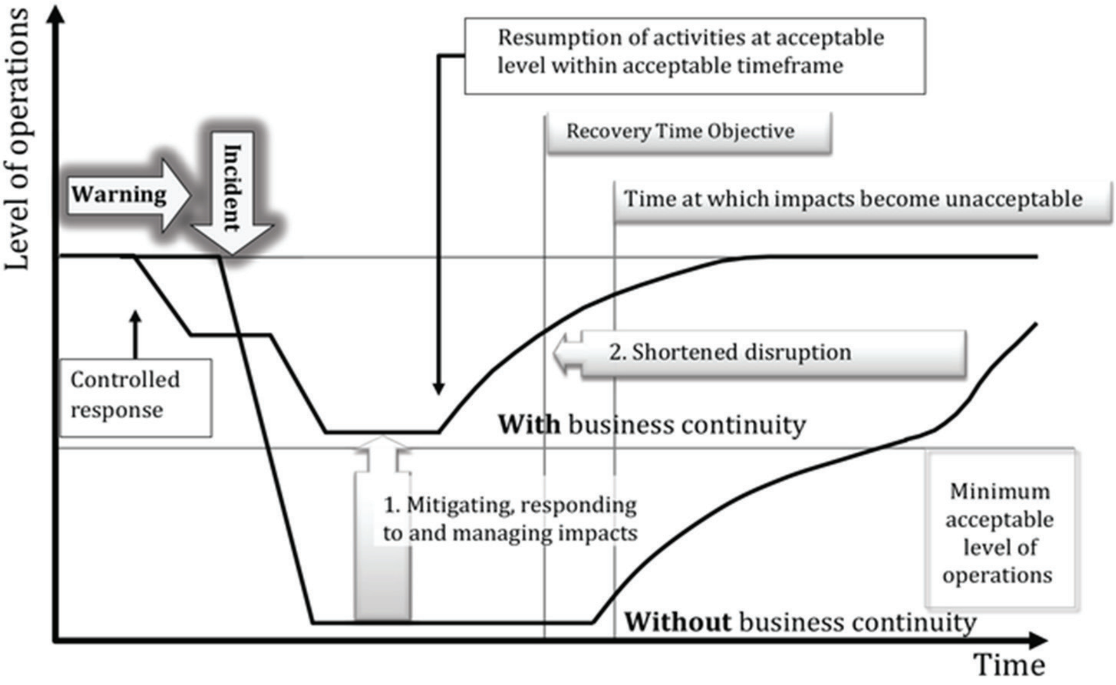

Level of operations
Resumption of activities at acceptable level within acceptable timeframe
Recovery Time Objective
Time at which impacts become unacceptable
Warning
Incident
2. Shortened disruption
Controlled response
With business continuity
1. Mitigating, responding to and managing impacts
Minimum acceptable level of operations
Without business continuity
Time

Figure 2: Illustration of business continuity being effective for gradual disruption
Source: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en:sec:8

Business continuity is typically specific to an organization, but its implementation often has significant implications for the wider community and third parties. An organization often relies on external entities while others depend on their operations. Effective business continuity, therefore, not only strengthens an organization's preparedness but also contributes to a more resilient society.

A BCMS enhances the organization's ability to operate during disruptions. It also results in an improved understanding of the organization's internal and external relationships, better communication with interested parties, and the establishment of a culture of continual improvement.

Implementation of the BCMS can provide numerous benefits, including,

a) Protecting lives, assets, and the environment – Ensuring the safety and well-being of individuals and safeguarding organizational resources
b) Creating value for the firm – Helping to maintain stock prices and overall business value
c) Safeguarding and enhancing reputation, confidence, and credibility – Building trust and confidence among interested parties by demonstrating resilience
d) Contributing to competitive advantage – Enabling uninterrupted operations during disruptions to gain an edge over competitors
e) Reducing costs from disruptions – Minimizing financial losses and maintaining operational efficiency during crises
f) Strengthening organizational resilience – Enhancing the ability to adapt and recover swiftly from unexpected events by addressing vulnerabilities and showcasing robust operational strategies

g) Reducing legal and financial risks – Mitigating liabilities and maintaining compliance with legal and regulatory requirements

h) Protecting revenue flows – Securing key assets and sustaining core operations to maintain financial stability

i) Contributing to profitability and competitiveness – Driving incremental gains in shareholder value, profitability, and market position

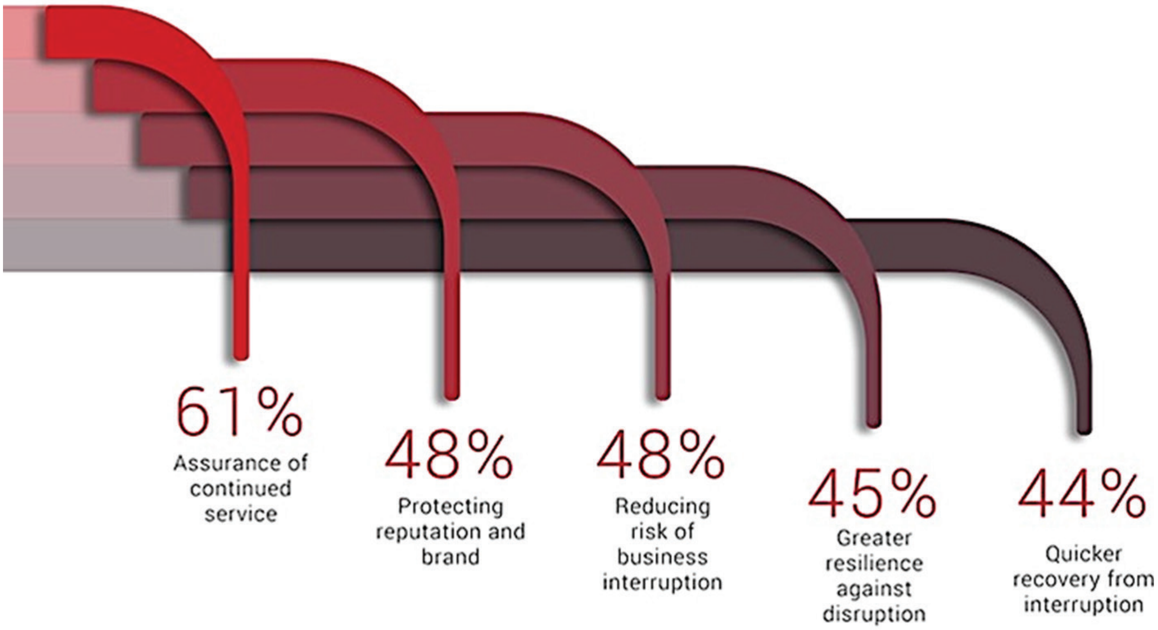


Figure 3: Top reasons why BCMS is a necessity

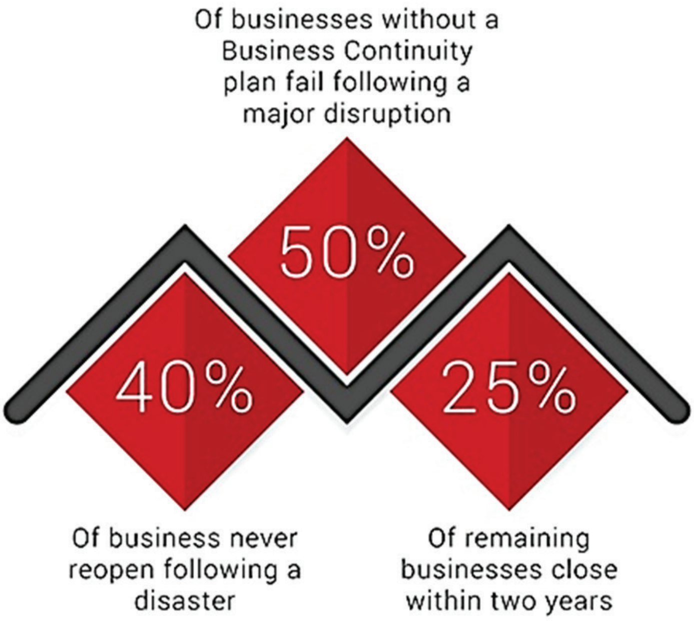
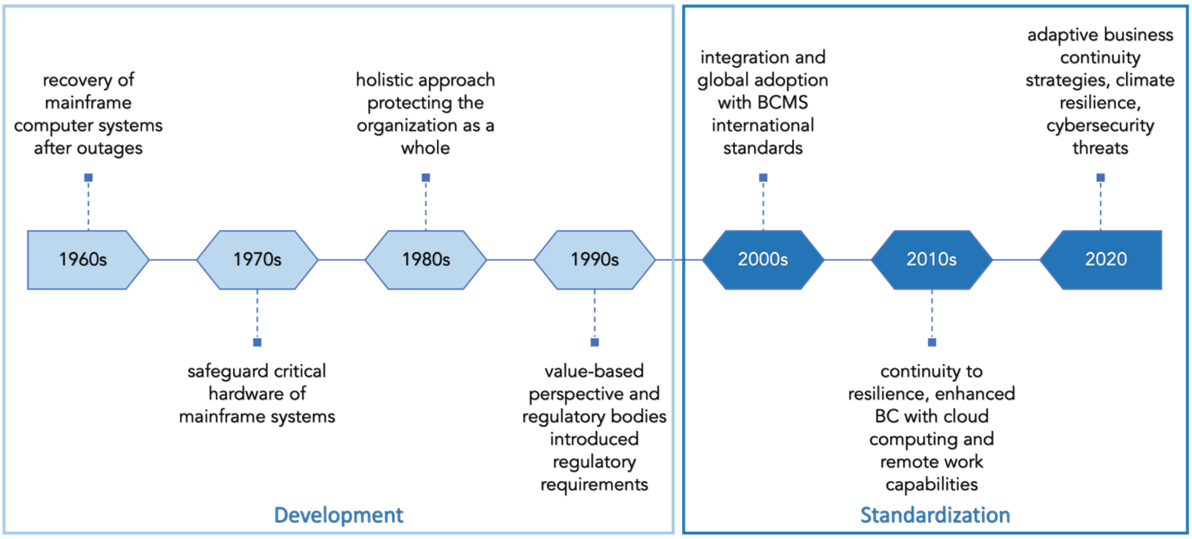


Figure 4: Consequences of not having BCMS

Source: NQA / Deloitte & Touche, 2008 / The U.S. Department of Labour

2.2. Know the history of BCMS and its evolution

The development of Business Continuity Management System has evolved over decades (Figure 5) in response to the changing nature of risks and the increasing interdependence of businesses and societies.



recovery of mainframe computer systems after outages
holistic approach protecting the organization as a whole
integration and global adoption with BCMS international standards
adaptive business continuity strategies, climate resilience, cybersecurity threats
1960s
1970s
1980s
1990s
2000s
2010s
2020
safeguard critical hardware of mainframe systems
value-based perspective and regulatory bodies introduced regulatory requirements
continuity to resilience, enhanced BC with cloud computing and remote work capabilities
Development
Standardization

Figure 5: Illustration of Evolution of BCMS

1950s–1960s: Resilience of mainframe IT systems

Business continuity traces its roots to basic backup and recovery methods, particularly in the IT sector. With the organizations investing millions of dollars in mainframe computer systems, they recognized the risk of catastrophic losses if these facilities were damaged or destroyed. This understanding led to the development of backup and recovery plans to ensure the restoration of systems following outages or disasters.

IBM introduced disaster recovery services in the 1960s, focusing on backing up mainframe systems and data.

1970s: Technology Mindset

The primary focus during the 1970s was on protecting computer systems, particularly mainframes. At the time, it was commonly assumed that business disruptions were primarily caused by technology failures. As a result, the priority was to safeguard the critical hardware of mainframe systems.

Business continuity was initially introduced by protecting the water-cooling pipes that regulated the operating temperature of these massive mainframe computers. The efforts focused on ensuring the cooling systems operated effectively, preventing overheating, and maintaining operational stability.

1980s: Beyond the IT systems

In the 1980s, business continuity evolved into a more formalized discipline with a clear mission to protect the organization as a whole. As IT shifted from mainframe systems to end-user personal computers, disaster recovery planning expanded beyond safeguarding significant investments in mainframe systems. Organizations began addressing broader operational considerations beyond IT systems, focusing on employees, technologies, and business processes critical to maintaining operational stability. This holistic approach aimed to ensure the company could remain resilient and functional during disruptions. Business Impact Analysis (BIA) was brought into practice at this time.

This evolution emerged in the term "business continuity planning" (BCP), focusing on maintaining essential business functions during and after a disruption. In the interest of BCP a few books and articles were published on the subject.

In 1988, the Disaster Recovery Institute (DRI International), was established as the first organization offering professional accreditation in disaster recovery.

The growing importance of operational resilience is further emphasized by financial regulations, particularly in banking. For instance, the New York Stock Exchange began requiring member firms to have continuity plans in place.

1990s: Value-based perspective

In the 1990s, BCMS is considered to have the potential to add value to the organization. The value-based perspective departs from the technology and auditing perspectives, broadening the scope and purpose of BCMS for the entire organization, including employees and external interested parties.

Further, the bird flu outbreak during this decade highlighted that business disruptions were not solely technological failures. Incidents impacting an organization's workforce were recognized as equally detrimental to operations, emphasizing the need for a holistic approach to BCMS.

It became clear that the entire organization needed the protective aspects of disaster recovery. The growth of global supply chains and increasing reliance on IT systems made businesses more vulnerable to disruptions. Events such as the Gulf War, earthquakes, and terrorist incidents prompted many organizations to formalize their business continuity efforts.

A new accreditation group based in the UK, the Business Continuity Institute (BCI), was established in 1994.

The Y2K crisis led to widespread contingency planning, as organizations feared IT failures associated with the millennium date change.

2000s: Integration and Global Adoption

The September 11, 2001, terrorist attacks in the United States marked a turning point. Businesses worldwide realized the importance of holistic BCMS, addressing not just IT but also physical infrastructure, human resources, and crisis communication.

The National Institute of Standards and Technology (NIST), in the US, published the first Contingency Planning Guide for Federal Information Systems in 2002, which addresses system disruptions and introduces business continuity and organizational resilience planning. It was revised in 2010.

Events such as the 2004 Indian Ocean tsunami and Hurricane Katrina in 2005 further emphasized the importance of BCMS, especially in supply chain and logistics management. Governments and organizations began emphasizing organizational resilience alongside BCMS.

2010s–Present: From Continuity to Resilience

As digital transformation accelerates, organizations face new challenges like cyberattacks, data breaches, and ransomware, integrating BCMS with cybersecurity and IT governance.

The COVID-19 pandemic in 2019 demonstrated the critical importance of BCMS for organizations of all sizes. It also underscored the need for adaptability in addressing prolonged disruptions affecting the workforce, supply chains, and markets.

Modern BCMS increasingly focuses on sustainability and the broader societal impact of organizational disruptions. It continues to evolve in response to emerging risks, including climate change, geopolitical instability, and the rapid pace of technological advancements. Today, organizations recognize BCMS as not only a risk management tool but also a competitive advantage in maintaining trust, reputation, and operational stability during crises.

2.3. BCMS; Sri Lankan Context

The evolution of Business Continuity Management (BCM) in Sri Lanka has been shaped by a complex interplay of natural disasters and economic disruptions. Traditionally, risk management in the country focused primarily on disaster recovery, with limited emphasis on holistic continuity planning. However, significant events over the past two decades have accelerated the adoption of structured BCM frameworks across industries.

Recognizing the potential systemic risk posed by operational disruptions, the Central Bank of Sri Lanka (CBSL) advised Financial Institutions (FIs) in 2005 to develop robust Business Continuity Plans (BCPs) to ensure operational resilience. Many of the initial BCPs submitted were incomplete or followed varied standards, prompting CBSL to issue detailed guidelines to establish a consistent framework for BCPs. Subsequently, in December 2021, CBSL issued a direction No. 16 of 2021 outlining the Regulatory Framework on Technological Risk Management and Resilience for licensed commercial banks. In compliance with the directions of CBSL, National Development Bank (NDB) became the first commercial bank in Sri Lanka to receive the ISO 22301:2019 certification.

In 2007, the Insurance Board of Sri Lanka (IBSL) also introduced guidelines to enhance its supervisory approach and promote best practices in business continuity. Insurance companies registered under the Regulation of Insurance Industry Act, No. 43 of 2000, were encouraged to implement effective BCPs by July 31, 2007, ensuring that service levels for existing and new policyholders would be maintained during system failures.

The Sri Lanka Preparedness Partnership (SLPP), a flagship program of the Asian Disaster Preparedness Center, has played a significant role in introducing BCM. Under the strategic direction of the Disaster Management Centre (DMC), the SLPP trained nearly 1,000 small and medium enterprises (SMEs) across various districts, establishing a foundation for integrating the BCM concepts among stakeholders. A few trainer training programs were conducted for the participants from government, private, and non-government sectors, further advocating for the importance of BCM. Additionally, in the aftermath of the 2019 Easter Sunday attack, Hatton National Bank (HNB) sponsored a BCM training for hoteliers whose businesses were impacted. The SLPP has also published the BCP Guidebook “UNSTOPPABLE BUSINESS Recipe to Survive the Crisis”, which provides a brief introduction to the importance of disaster preparedness as well as Business Continuity Management (BCM).

The International Labour Organization (ILO) has contributed to the evolution of BCM in Sri Lanka, particularly following the severe damages caused by floods and landslides in 2016 and 2017. Collaborating with the DMC, the Ministry of Industries, and the Kalutara and Ratnapura District Secretariats, the ILO organized training sessions introducing BCP to government officers in the affected districts. This initiative, funded by the Government of Japan, led to the publication of a document titled “Business Continuity Plan – BCP” in 2019, providing foundational guidelines to help Micro, Small, and Medium Enterprises (MSMEs) develop their own Business Continuity Plans.

Today, a few leading institutes in Sri Lanka, in collaboration with accredited foreign entities, offer BCMS consultancies and training. These initiatives reflect a growing recognition of the need for structured BCM practices, enabling businesses to enhance their resilience and contribute to national economic stability.

3. BCMS FRAMEWORK

The Business Continuity Management System (BCMS) standards provide a structured framework that helps organizations prepare for, respond to, and recover from disruptive incidents. These standards outline best practices for identifying potential threats, assessing risks, and implementing effective continuity and recovery strategies. BCMS standards promote consistency, compliance with legal and regulatory requirements, and foster stakeholder confidence by demonstrating a proactive approach to managing risks. Additionally, these standards facilitate continuous improvement through regular reviews, audits, and updates, aligning organizational practices with evolving risks and industry best practices.

BCMS framework requires organizations to establish, implement, and maintain processes that will enable effective BCMS while managing interactions between these processes.

In implementing BCMS processes, the organization should,

a) Identify the required inputs and expected outputs
b) Define the sequence and interaction between processes
c) Establish criteria and methods (including monitoring, measurements, and performance indicators) to ensure the effective operation and control
d) Determine and allocate the necessary resources to ensure availability
e) Assign clear responsibilities and authorities
f) Address identified risks and opportunities
g) Evaluate the processes and implement any changes needed to achieve the intended results.
h) Continuously improve the processes and overall BCMS framework

The organization should maintain documented information to support the operations and retain documented records to ensure confidence that the processes are being implemented as planned.

3.1. BCMS international standards

BCMS has evolved significantly over the past two decades, driven by the increasing need for organizations to enhance resilience against disruptions. The development of international standards has provided a structured approach to implementing effective BCMS, ensuring the resilience of organizations.

This chapter traces the key milestones in the evolution of BCMS, from the introduction of BS 25999 in 2006 to the establishment of the globally recognized ISO 22301 standard in 2012 and its subsequent updates. The latest amendment in 2024 reflects the growing emphasis on climate action, further strengthening business resilience strategies.

- 2006 – The British Standards Institution (BSI) introduced BS 25999, the first business continuity standard, providing a structured framework for organizations to establish and maintain business continuity practices.
- 2012—The ISO 22301:2012 standard was introduced as the first internationally recognized framework for Business Continuity Management Systems (BCMS). As a result, BS 25999 was partially withdrawn in 2012 and fully retired in 2013. Other notable standards contributing to BCMS evolution included ANZ 5050 (Australia), SS 540 (Singapore), and NFPA 1600 (United States).
- 2019 – The ISO 22301:2019 edition, titled "Security and Resilience—Business Continuity Management Systems—Requirements," was released, updating the 2012 version to improve clarity and align with modern business continuity practices.
- 2024 – An amendment, ISO 22301:2019/Amd 1:2024, was introduced, incorporating considerations for climate action into BCMS. Organizations implementing or maintaining BCMS are advised to align with ISO 22301:2019 and its 2024 amendment to ensure compliance with the latest international standards.

Within the series, ISO 22300:2021 - Security and resilience – Vocabulary and ISO 22313:2020 - Security and resilience – Business Continuity Management Systems – Guidance provide helpful direction in support of the practical implementation and operation of a business continuity system.

The annual ISO survey tracks the number of valid certifications for various ISO standards worldwide. Table 3 presents the certification trends for ISO 22301 (Business Continuity Management), ISO 9001 (Quality Management), and ISO 14001 (Environmental Management) from 2019 to 2022, highlighting their adoption and growth over time.

Table 3: Yearly increase of valid ISO certificates in a few standards

	ISO 22301	ISO 9001	ISO 14001
2019	1,692	880,007	312,111
2020	2,205	916,842	348,473
2021	2,559	1,077,884	420,433
2022	3,200	1,265,216	528,903

Source: ISO Survey

In addition to **ISO 22301:2019**, several other ISO standards are relevant to business continuity management and the broader field of security and resilience. These standards provide supplementary guidance, terminology, and frameworks that align with or support the implementation of ISO 22301. Here are key related standards:

General Standards Supporting ISO 22301

1. **ISO 22300:2021** – Security and resilience – Vocabulary
   - Defines key terms and concepts used in the ISO 22300 series, ensuring consistency and clarity.

2. **ISO 22313:2019** – Security and resilience – Business continuity management systems – Guidance
   - Offers practical guidance on implementing, maintaining, and improving a BCMSS in alignment with ISO 22301.

Risk Management and Resilience

3. **ISO 31000:2018** – Risk management – Guidelines
   - Provides a framework for identifying, assessing, and managing risks, which is critical for effective business continuity planning.

4. **ISO 22316:2017** – Security and resilience – Organizational resilience – Principles and attributes
   - Explores broader organizational resilience, complementing ISO 22301 by addressing adaptability and long-term sustainability.

5. **ISO 22317:2021** – Security and resilience – Business impact analysis (BIA) – Guidelines
   - Focuses on conducting a business impact analysis, a fundamental component of ISO 22301 implementation.

6. **ISO 22318:2021** – Security and resilience – Supply chain continuity – Guidelines
   - Provides guidance for managing supply chain risks and ensuring continuity during disruptions.

Emergency Management and Incident Response

7. **ISO 22320:2018** – Security and resilience – Emergency management – Guidelines for incident management
   - Offers a framework for effective incident management to complement business continuity efforts.

8. **ISO 22322:2022** – Security and resilience – Emergency management – Guidelines for public warning
   - Focuses on effective communication and public warning during emergencies.

9. **ISO 22325:2016** – Security and resilience – Emergency management – Guidelines for command and control
   - Provides insights into establishing and managing a command-and-control structure during crises.

ICT and Data Security

10. **ISO/IEC 27001:2022** – Information security, cybersecurity, and privacy protection – Information security management systems – Requirements
    - Focuses on information security, ensuring that sensitive data is protected, aligning with BCMSS objectives.

11. **ISO/IEC 27031:2011** – Information technology – Security techniques – Guidelines for ICT readiness for business continuity
    - Provides guidance on ensuring the availability and reliability of ICT systems during disruptions.

Sector-Specific Standards

12. **ISO 22395:2018** – Security and resilience – Community resilience – Guidelines for supporting vulnerable persons in an emergency
    - Addresses resilience in the context of communities and individuals, particularly vulnerable populations.

13. **ISO 22392:2019** – Security and resilience – Community resilience – Guidelines for conducting peer reviews
    - Offers guidelines for peer reviews in the context of community resilience and preparedness.

These standards collectively strengthen an organization's ability to prepare for, respond to, and recover from disruptions while supporting the core principles and requirements of ISO 22301.

3.2. Standardization and Certification

Achieving recognized standards in BCMS enhances organizational resilience and credibility. The pathway to standardization begins with an initial assessment of current business continuity practices and conducting a gap analysis to identify areas that need improvement in line with international standards ISO 22301:2019. Businesses can gradually build their BCMS, focusing first on critical processes and scaling up to a comprehensive framework over time. SMEs may initially focus on achieving basic compliance, demonstrating their adherence to core BCMS principles matching their resources and operational scope. Larger enterprises with more complex operations can pursue full ISO certification, incorporating advanced risk management strategies, detailed continuity plans, and rigorous testing procedures.

Standardization not only ensures a systematic approach to risk management and business continuity but also prepares organizations for external validation through certification. Certification by local or international certifiers provides independent assurance of compliance with BCMS standards. Local certifiers offer advantages such as cost-effectiveness and contextual relevance, while international certifiers provide broader recognition, particularly for businesses aiming to expand into global markets. Certification demonstrates a commitment to maintaining robust business continuity practices, enhancing stakeholder confidence and competitive advantage.

The certification process typically involves an external audit by an accredited certification body, where businesses are evaluated against the requirements of the standard. Successful certification validates the effectiveness of an organization's BCMS and its ability to manage disruptions effectively. Maintaining certification requires regular reviews and updates to the BCMS, ensuring it remains aligned with evolving risks and business priorities.

Standardization and certification enable organizations to align their practices with global best practices while tailoring their approach to fit their specific size, industry, and risk profile. By pursuing certification, businesses not only enhance their resilience but also contribute to broader national and industry-wide disaster preparedness and continuity initiatives.

3.3. ISO 22301 Certification Process

Achieving ISO 22301 certification follows a structured process to ensure that the organization's Business Continuity Management System (BCMS) complies with the standard's strict requirements.

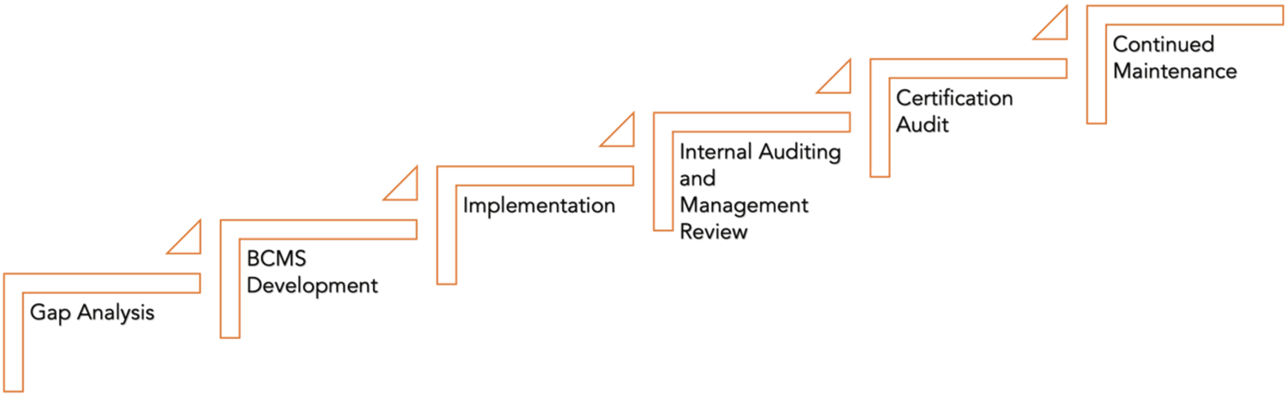


Figure 6: Certification Process

Step 1: Gap Analysis

The first step is a gap analysis, where the organization's current practices are compared to ISO 22301 standards. This identifies any existing processes, policies, or practices that do not align with the standard. A detailed report is typically created to highlight these gaps and provide recommendations to address them. Many organizations seek external consultants for an objective and thorough evaluation.

Step 2: BCMS Development

Using the findings from the gap analysis, the next step is to develop a BCMS that aligns with the organization's needs while ensuring compliance with ISO 22301.

Step 3: Implementation

Once the BCMS framework is established, the organization should implement the necessary policies, procedures, and processes to meet the ISO 22301 criteria and bridge any gaps identified.

Step 4: Internal Auditing and Management Review

Internal auditing plays a critical role in the certification process. This involves reviewing the BCMS to ensure that it complies with ISO 22301 and effectively manages business continuity risks. Audits should be conducted at planned intervals by qualified personnel capable of identifying non-conformities and recommending corrective actions.

Following internal audits, a management review takes place. This allows top management to assess the BCMS's overall performance, its suitability, adequacy, and effectiveness in supporting the organization's objectives and adapting to internal and external changes. The review generates actionable decisions for improving the BCMS and reassessing business continuity risks and strategies.

Step 5: Certification Audit

The certification audit is the final major step. Conducted by an accredited certification body, this process is carried out in two stages. The first stage evaluates the BCMS documentation against ISO 22301 standards, while the second stage assesses its practical effectiveness. If the organization meets the requirements in both stages, it is awarded ISO 22301 certification. The certificate is valid for three years and requires annual surveillance audits to ensure ongoing compliance.

Ongoing Maintenance

Achieving certification is not the final objective. Maintaining the BCMS is a continuous process that requires regular reviews, testing, and improvement to address the ongoing challenges of maintaining effective business continuity.

3.4. Proportionality in BCMS

The BCMS requirements shall align with the size and complexity of an organization and its processes. Proportionality in BCMS ensures that organizations adopt appropriate levels of BCM activities based on their size, industry, financial capacity, and operational complexity, allowing them to meet the minimum requirements without overburdening resources. This approach promotes manageable, scalable, and effective BCMS practices for businesses of all sizes, with compliance achievable through a phased approach over time. Based on the size of the business,

- Micro and Small Enterprises: Simple risk assessments, basic continuity plans, annual tabletop drills.
- Medium Enterprises: Moderate BCMS processes, scenario-based exercises, and biannual reviews.
- Large Enterprises: Comprehensive BCMS frameworks, live simulations, quarterly reviews.

Organizations in high-risk sectors may require robust BCMS approaches, whereas low-risk sectors may focus on core operational continuity, simplified risk assessment, and minimal testing requirements. For example,

- Manufacturing: Emphasize supply chain continuity and operational recovery drills.
- Service Industries: Focus on data recovery and customer communication plans.
- Agriculture and Fisheries: Prioritize seasonal risk management and resource allocation strategies.

The scale and turnover of a business also influence BCMS strategies. Small-scale enterprises with low turnover can adopt low-cost, simplified continuity strategies, whereas large-scale companies with high turnover should implement in-depth risk analysis and advanced response mechanisms. Multi-location businesses require coordinated drills and tailored plans for different work sites.

A flexible approach to testing and drills is desirable, with small businesses opting for cost-effective tabletop exercises and medium enterprises engaging in scenario-based testing. Large organizations should conduct full-scale simulations to evaluate cross-functional and cross-location resilience.

Adopting proportionality in preparedness activities enables organizations to align their BCMS strategies with available resources and operational needs, fostering greater resilience across diverse business environments.

3.5. Recognize the Importance of BCPs in BCMS

Business Continuity Management (BCMS) is a comprehensive management process that identifies potential threats to an organization and their impacts on business operations. It establishes a framework for building organizational resilience and the capability to respond effectively to disruptions. BCMS covers the policies, processes, and resources needed to ensure critical functions continue or are recovered promptly during a crisis. It is a proactive approach to safeguarding an organization’s people, assets, reputation, and operations.

Key Components of BCMS:

1. Risk Assessment: Identifying potential risks and vulnerabilities.
2. Business Impact Analysis (BIA): Determining the criticality of activities and their recovery priorities.

3. Business Continuity Strategies: Developing methods to ensure continuity of operations.
4. Testing and Maintenance: Regularly testing and updating plans to keep them effective.

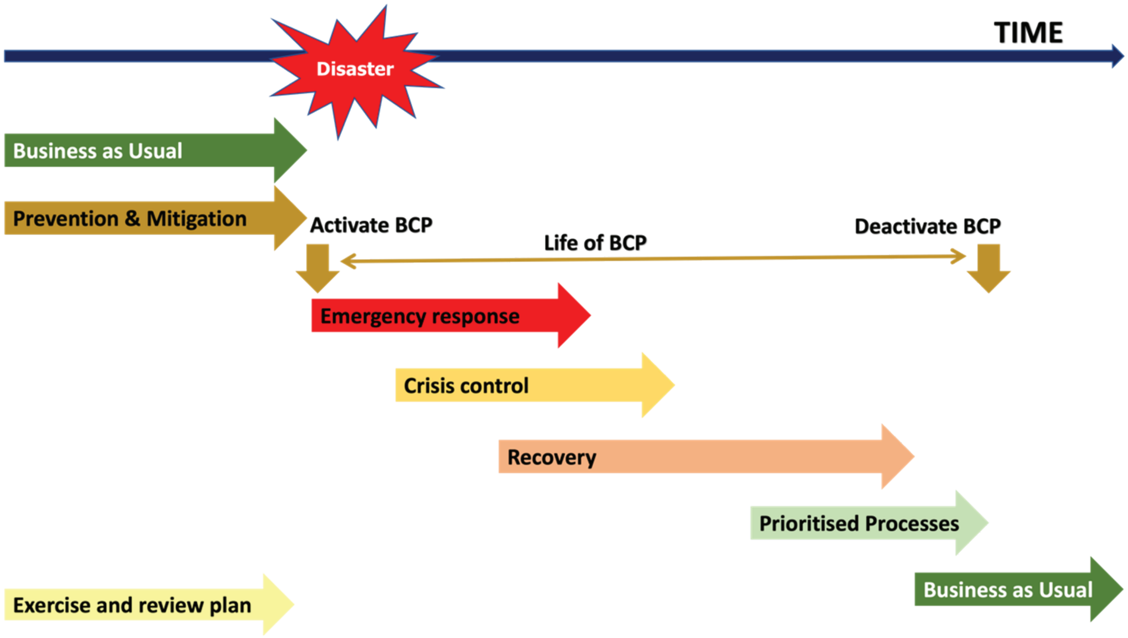
A Business Continuity Plan (BCP) is a key deliverable of BCMS. It is a documented plan that provides step-by-step instructions on how an organization will respond to and recover from disruptions. A BCP ensures that critical operations continue and that the organization can recover quickly and efficiently after an incident. It includes specific strategies and actions tailored to the organization's unique needs.

Key Elements of BCP:

1. Emergency Response: Steps for managing the immediate effects of a disruption.
2. Critical Function Recovery: Plans to resume essential operations within required timeframes.
3. Communication Plan: Guidelines for informing stakeholders during and after an incident.
4. Resource Allocation: Identification of necessary personnel, facilities, and technology for recovery.

BCMS is the overarching management process for resilience and continuity, while BCP is the specific, actionable plan that arises from BCMS to handle disruptions. Both are integral to ensuring that an organization can survive and thrive despite challenges.

The Business Continuity Plan (BCP) lifecycle is composed of specific stages designed to help an organization respond to and recover from disruptions efficiently. Among these, the activation and deactivation stages are particularly critical. Activation involves initiating the BCP when a disruption threatens essential operations, ensuring a swift and coordinated response to mitigate impacts. Deactivation occurs once stability is restored, focusing on transitioning back to normal operations in a controlled manner. Effective management of these stages ensures minimal disruption to business activities, reduces potential losses, and protects the organization's reputation.



BCP activation triggers when a significant threat disrupts business operations. The key steps involved are:

1. Emergency Response: Primarily concerned with the physical and immediate response to disasters and emergencies, focusing on saving lives and protecting property.
    - Assess the situation and ensure the safety of employees and stakeholders.
    - Contain the disruption to prevent further damage.

2. Crisis Management: Aim at managing and recovering from disruptive events (which may not always involve physical emergencies), often focusing on reputation management and organizational stability.
    - Assemble the crisis management team for oversight and decision-making.
    - Maintain clear communication with stakeholders and allocate resources efficiently.

3. Recovery: Focuses on rebuilding and restoring functionality after a crisis or emergency.
    - Restore critical processes and implement temporary measures for continued operations.
    - Monitor progress and adjust as needed.

4. Prioritized Processes:
    - Focus on prioritized business operations to minimize disruption.

Deactivation marks the return to normal business operations, ensuring all prioritized processes are stabilized and the organization transitions out of crisis mode to business-as-usual mode effectively.

3.6. BCMS Development Process

The BCMS development process involves a systematic approach to establishing a framework that ensures business continuity and aligns with ISO 22301 requirements. The process is graphically explained in Figure 7 BCMS Development Process.

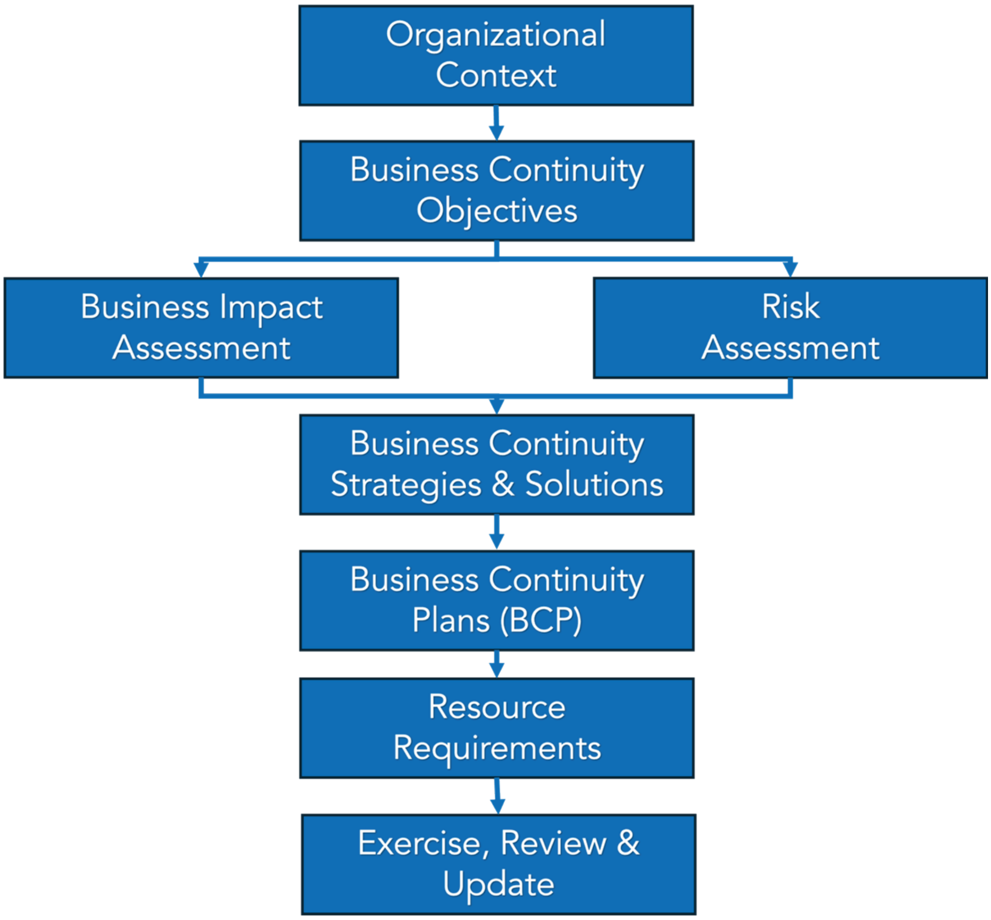

Organizational Context
Business Continuity Objectives
Business Impact Assessment
Risk Assessment
Business Continuity Strategies & Solutions
Business Continuity Plans (BCP)
Resource Requirements
Exercise, Review & Update

Figure 7: BCMS Development Process

The key steps in developing a BCMS are further explained below:

Step 1: Establish Organizational Context & Leadership Commitment

- Define the scope of the BCMS, considering the organization's size, structure, and key activities.
- Secure top management commitment to ensure necessary resources and support for BCMS implementation.
- Establish a Business Continuity Policy that outlines the organization's approach to business continuity.

Step 2: Conduct a Business Impact Analysis (BIA) & Risk Assessment

- Identify critical business functions and assess the impact of potential disruptions.
- Determine the maximum tolerable downtime (MTD) and recovery time objectives (RTO) for each function.
- Conduct a Risk Assessment to identify potential threats (natural disasters, cyber-attacks, supply chain failures, etc.) and evaluate their likelihood and impact.

Step 3: Define Business Continuity Strategies

- Develop appropriate strategies to mitigate risks and ensure continuity of operations.
- Strategies may include alternative work locations, redundant IT systems, emergency response plans, and crisis communication plans.

Step 4: Develop Business Continuity Plans (BCP)

- Create detailed Business Continuity Plans for responding to and recovering from disruptions.
- Plans should include:
    - Emergency response and crisis management procedures.
    - Roles and responsibilities of key personnel.
    - Communication protocols for internal and external stakeholders.
    - Recovery procedures for critical business processes.

Step 5: Implement the BCMS

- Integrate the BCMS into the organization's daily operations.
- Train employees on their roles and responsibilities in business continuity.
- Conduct awareness programs to ensure all staff understand the BCMS and its importance.

Step 6: Testing & Exercising

- Regularly test the BCMS through drills, simulations, and tabletop exercises to evaluate its effectiveness.
- Identify weaknesses in the system and make improvements based on test results.

Step 7: Monitor, Audit, and Review

- Establish a process for continuous monitoring and evaluation of the BCMS.
- Conduct internal audits to assess compliance with ISO 22301 and identify areas for improvement.
- Perform management reviews to ensure BCMS remains relevant and aligned with organizational goals.

Step 8: Continual Improvement

- Implement corrective and preventive actions based on audit findings and real-world incidents.
- Regularly update the BCMS to address new threats, regulatory changes, and business needs.

By following these steps, an organization can develop a robust BCMS that enhances resilience, minimizes disruption risks, and ensures effective response and recovery in the event of a crisis.

3.7. Plan-Do-Check-Act (PDCA) Cycle in BCMS

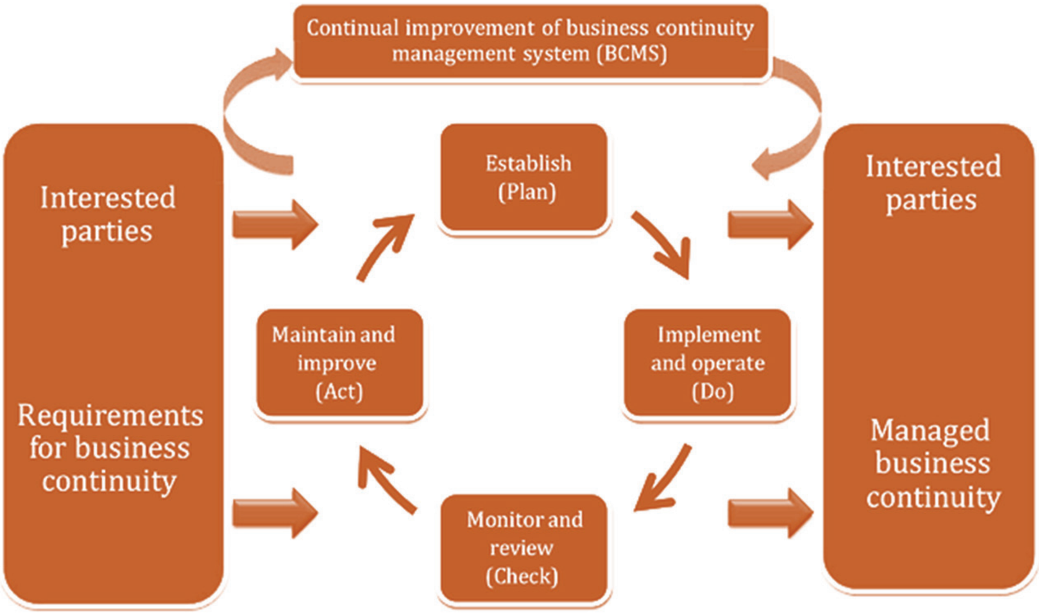

Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Implement and operate (Do)
Monitor and review (Check)
Maintain and improve (Act)
Interested parties
Managed business continuity

Figure 8: PDCA cycle applied to BCMS processes
Ref: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en:sec:8

BCMS applies the Plan-Do-Check-Act (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the effectiveness of the BCMS.

Table 4: Plan-Do-Check-Act Cycle

Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization’s overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMSS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMSS and business continuity policy and objectives.

A key practical challenge with BCMS is that it comes into action infrequently. Unlike quality management systems, which are implemented into daily operations, business continuity is only fully brought into action when a disruption occurs. This necessitates a greater focus on,

- Business continuity plan (BCP) testing or drills ensure the plan is practical, effective, and familiar with staff and interested parties
- Retaining and refreshing organizational capabilities, maintaining the skills, knowledge, and resources needed to support the business continuity
- Periodic reviews of the system, its processes, and rationale to ensure it remains aligned with the organization’s evolving structure and needs.

4. CONTEXT OF THE ORGANIZATION

Action Step: At the end of Chapter 4: Context of the organization, complete Exercise 4 in the attached BCMS Manual.

4.1. Understanding of the organization

The organization should understand the external and internal factors, including both positive and negative conditions that are relevant to its overall objectives, its products and services, and the amount as well as its risk appetite. This information should be considered when implementing the organization's BCMS and assigning priorities.

4.2. Expectations of interested parties

When establishing the BCMS, the organization should consider the needs and requirements of all interested parties, including a range of people within and outside the organization. The organization should identify all interested parties (Figure 9) and assess their needs, expectations, and requirements, which are not only obligatory and stated requirements but also implied expectations. In implementing the BCMS, it is important to identify actions that are appropriate and tailored to the specific interests of interested parties. During this stage, organizations should include women, persons with disabilities, and other potentially vulnerable groups and their unique needs, particularly regarding safety and mobility.

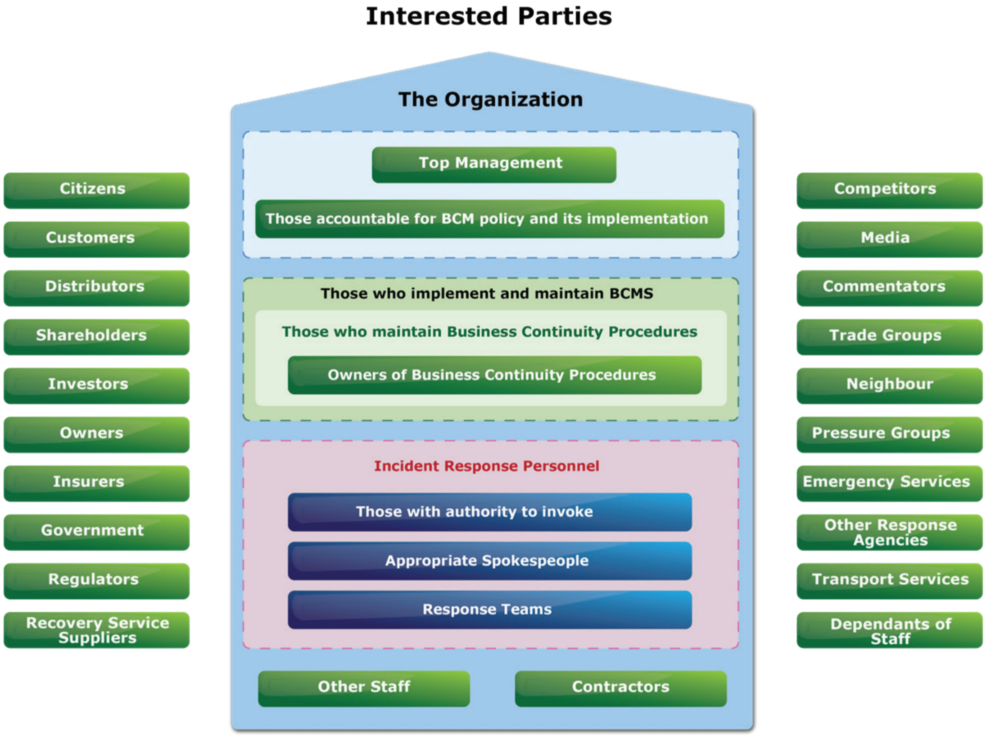


Figure 9: Internal and external interested parties
https://blog.BCMS-institute.org/BCMS/what-are-the-stakeholders-or-interested-parties

Table 5: Expectations of Interested Parties

Interested Party	Expectations in BCMS	Examples
Customers	Continuity of service, timely communication during incidents, data protection	Expect services/products to be delivered with minimal disruption even during crises
Employees	Safety, clear instructions during emergencies, job security	Want assurance their welfare is protected, and they will be informed during events
Management	Protection of strategic goals, regulatory compliance, reputation management	Expect business continuity to support organizational resilience and risk reduction
Suppliers/ Contractors	Clarity on their role during disruption, continuity of business relationships	May need continuity plans aligned with the organization, especially for critical supplies
Regulators/ Government	Legal compliance, public safety, sector-wide resilience	Expect organizations to meet BCMS standards like ISO 22301 or local laws
Shareholders/ Investors	Risk management, business resilience, protection of value	Expect minimal financial impact from disruptions and transparent reporting
Community/Public	Safety, environmental protection, ethical conduct during crises	Expect organizations not to endanger the community or environment during operations
Emergency Services	Cooperation, access to emergency plans, timely updates	Expect accurate information and support during incident response or evacuation

Similarly, there shall be legal and regulatory requirements that are relevant to its operations. Requirements can include:

a) Incident response, including emergency management and other relevant legislation
b) Business continuity, which can dictate the scope of the program or the extent or speed of recovery
c) Risk, requirements defining the scope or methods of risk management
d) Hazards (e.g., operating requirements relating to dangerous materials stored at the location).

The purpose of implementing BCMS should be clearly defined. Typically, BCMS aims to safeguard business operations against disasters and accidents. A well-defined purpose serves as a crucial benchmark for prioritizing key products or services and selecting appropriate business continuity strategies.

4.3. What is the purpose of BCMS?

1. Protecting People: The top priority is ensuring the safety and well-being of employees, visitors, and customers on the premises.
2. Protecting the Business: This includes fulfilling contractual obligations to customers and users, thereby maintaining business integrity and resilience.
3. Supporting Local Community: BCMS also emphasizes upholding social responsibility and contributing to the community and local economy. Businesses, regardless of size, are encouraged to support disaster response and recovery efforts by leveraging their resources and expertise, whether industry-specific or otherwise. By doing so, BCMS helps the community and also secures employment and protects employees' livelihoods.

4.4. Scope of the BCMS

The purpose of determining the scope of the BCMS is to identify its boundaries and applicability to ensure the inclusion of all relevant products and services, activities, locations, resources, suppliers, and other dependencies critical to the organization.

BCMS can be implemented in specific sections or departments based on the organization's needs and priorities. The scope can be limited to key areas critical to the organization's operations. Such as the main factory producing the organization's top brand product or the flagship store with the highest sales.

The scope of BCMS should be determined by evaluating the organization's unique business requirements and circumstances. It is essential to include core sections that are vital to the organization's survival within the BCMS framework.

While exclusions from the scope are possible, they must not affect the organization's ability to meet business continuity requirements as determined by the business impact analysis. Activities, resources, and supply chains that are required to deliver in-scope products and services cannot be excluded.

5. LEADERSHIP AND TEAM

Action Step: At the end of Chapter 5: Leadership and Team, complete Exercise 5 in the attached BCMS Manual.

5.1. Leadership and Commitment

Leadership and commitment at all levels of management are critical to the success of BCMS. Each level of management should actively demonstrate their engagement and accountability within their areas of responsibility. BCMS should be a regular agenda item at management meetings to emphasize its importance.

The BCMS leader will act as the primary contact for the business continuity management process and lead the BCMS development team. Executives will provide strategic input and in-depth insight into the critical business processes, while Business Process Owners or representatives will be responsible for reporting the critical business operations and the relevant resources needed for each of these business units to function.

Top management should exhibit leadership and commitment by:

a) Assigning and ensuring the fulfillment of managerial roles
b) Establishing and maintaining business continuity policy
c) Appointing competent staff with the appropriate authority to be responsible for the BCMS and ensuring its effective operation
d) Appointing a representative responsible for gender and disability inclusion within BCMS
e) Communicating the importance of business continuity and ensuring compliance with BCMS requirements
f) Allocating the necessary resources, including sufficient funding
g) Promoting continual improvement to BCMS practices
h) Ensuring the BCMS achieves its intended outcomes
i) Providing support to other levels of management, enabling them to demonstrate leadership and commitment within their areas

Other levels of management should demonstrate their leadership and commitment by:

a) Setting business continuity objectives aligned with the organization’s strategic goals
b) Integrating BCMS requirements into regular business processes
c) Maintaining awareness of applicable legal, regulatory, and other requirements
d) Establishing BCMS roles, responsibilities, and competencies
e) Achieving the intended BCMS outcomes
f) Actively engaging in the exercise program
g) Conducting internal BCMS audits

h) Conducting effective management reviews of the BCMS
i) Directing and supporting improvement of the BCMS

5.2. BCMS Policy

Top management should establish a clear BCMS policy that outlines the organization's intent and direction regarding business continuity in alignment with its objectives and purpose. The policy should demonstrate a commitment to meeting applicable requirements, including legal and regulatory obligations, and to continual improvement. It should define the scope of BCMS, including any limitations or exclusions, and identify authorities, delegations, and references to relevant standards, guidelines, and regulations.

The BCMS policy may also include commitments to funding, references to related policies, requirements for implementing BCMS, and a pledge to exercise and maintain BCMS practices. This policy should be documented, communicated across the organization, and shared with relevant interested parties.

Provisions should be established for the policy's approval, periodic review, and updates whenever significant internal or external changes occur.

5.3. Roles and Responsibilities

Top management should ensure the assignment and communication of responsibilities and authorities within the BCMS. A member of top management should be responsible and accountable for the BCMS. Additionally, top management may appoint other representatives to oversee the implementation and ongoing monitoring of the BCMS with clearly defined roles and responsibilities. These representatives from functions or locations within the organization should have their BCMS roles and responsibilities integrated into job descriptions.

Strong leadership from top management is essential to fostering an organizational culture that understands, engages with, and supports the BCMS. A BCMS leader is responsible for driving organization-wide BCMS activities. This individual should be granted the authority and responsibility necessary to fulfill their role effectively. Given that BCMS requires active collaboration across departments, the leader should be someone widely respected and trusted within the organization.

To ensure continuity, a BCMS deputy leader should also be appointed, as the leader may be unable to perform their duties during a disaster due to absence, injury, or other reasons.

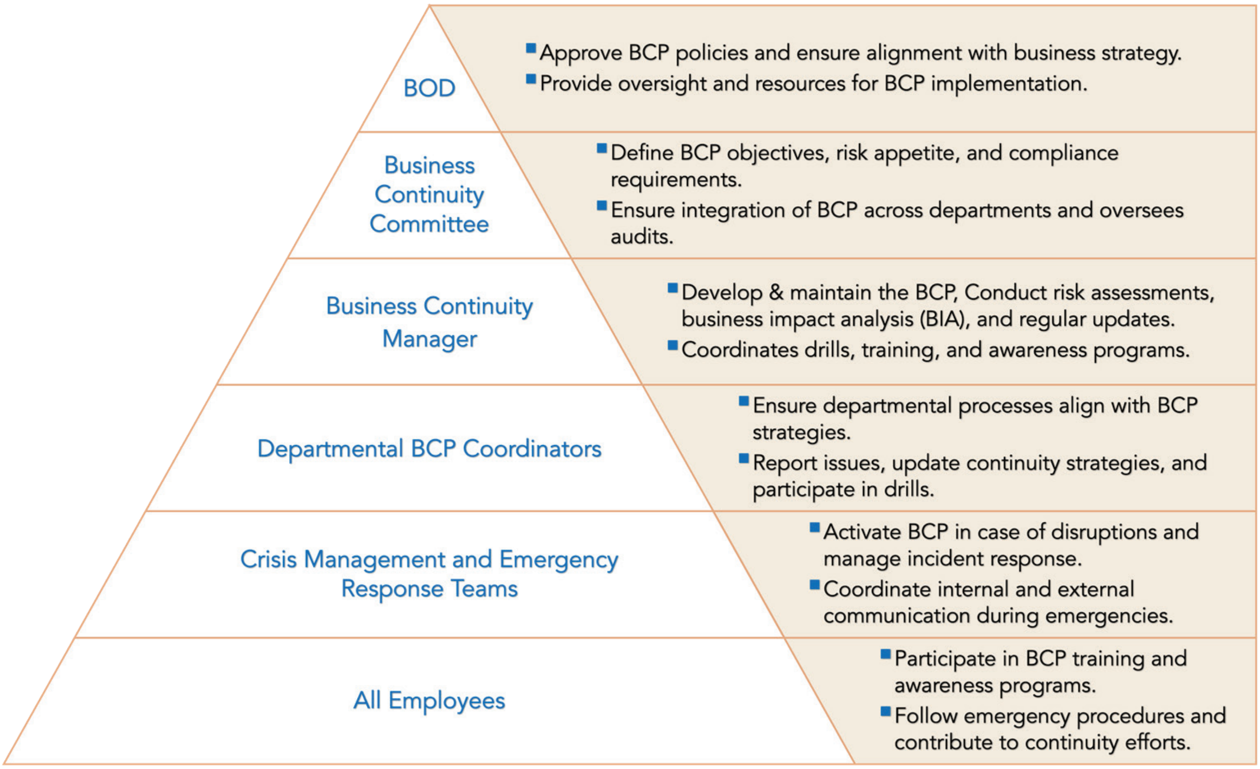

BOD
Approve BCP policies and ensure alignment with business strategy.
Provide oversight and resources for BCP implementation.
Business Continuity Committee
Define BCP objectives, risk appetite, and compliance requirements.
Ensure integration of BCP across departments and oversees audits.
Business Continuity Manager
Develop & maintain the BCP, Conduct risk assessments, business impact analysis (BIA), and regular updates.
Coordinates drills, training, and awareness programs.
Departmental BCP Coordinators
Ensure departmental processes align with BCP strategies.
Report issues, update continuity strategies, and participate in drills.
Crisis Management and Emergency Response Teams
Activate BCP in case of disruptions and manage incident response.
Coordinate internal and external communication during emergencies.
All Employees
Participate in BCP training and awareness programs.
Follow emergency procedures and contribute to continuity efforts.

Figure 10: Roles and Responsibilities

5.4. BCMS Teams

Depending on the size of the organization, support teams should be formed to assist under the BCMS leader's direction. These teams may include:

a) BCM Team: Oversee the overall development of BCMS policy, objectives, and framework; conduct Risk Assessment and Business Impact Analysis; Coordinate awareness, training, and exercises; and ensure implementation, maintenance, and continual improvement.

b) Crisis Management Team: Responsible for addressing crises that threaten business operations, including both disaster-related and non-disaster-related incidents; makes strategic decisions during disruption and coordinates high-level efforts; communicates with regulators, media, and external stakeholders; and supports continuity and recovery decisions.

c) Emergency Response Team: Respond immediately to a disruption to contain the impact and ensure safety; liaise with emergency services (fire, police, medical); conduct safety drills.

d) Damage Assessment Team: Tasked with assessing damage in the event of a disaster.

e) Business Recovery Team: Focused on planning, managing, and implementing recovery operations according to Business Continuity Plans to re-establish operations.

f) Business Support Team: Provides essential support functions, often led by HR, Finance, and IT departments.

g) Communication Team: Handles internal and external communications during a disruption.

For small organizations, the BCMS team structure should be simplified, with fewer teams to enable realistic implementation.

Management must ensure that the BCMS leader and team have access to necessary resources, including an adequate budget, to carry out their responsibilities. The business owner or senior management should demonstrate a visible commitment to BCMS activities, as verbal instructions alone are insufficient for achieving success.

6. BUSINESS IMPACT ANALYSIS

Action Step: At the end of Chapter 6: Business impact analysis, complete Exercise 6 in the attached BCMS Manual.

An organization achieves its purpose by delivering products and services to its customers. To ensure uninterrupted delivery, it is crucial to understand the potential adverse impacts of disrupting the delivery of these products, services, and their supporting activities on the organization and interested parties over time. Additionally, it is important to understand the interrelationships and resource requirements of the activities that support products and services as well as the threats to those activities.

The organization should establish and maintain processes that systematically analyze the business impacts and assess the risks of disruption. The outcomes enable the organization to identify effective business continuity strategies and solutions. The analysis of business impacts and assessment of risks should be reviewed at planned intervals and whenever significant changes occur within the organization or the context in which it operates.

6.1. Prioritized Activities (PAs) and Recovery Time Objectives (RTOs)

When introducing BCMS to an organization, it is essential to identify its lifeline products or services, the key business activities driving top-selling products, and the locations or shops with the highest sales. A Business Impact Analysis (BIA) helps the organization prioritize the disrupted activities for early resumption. Its primary purpose is to identify and classify activities that require urgent recovery to prevent unacceptable levels of adverse impact. The BIA establishes the business continuity priorities and requirements by analyzing the products or services that need to be recovered and delivered first during a natural disaster or accident. These critically important business activities are known as “Prioritized Activities” (PAs). The analysis should cover all activities within the BCMS scope. The organization may select one or more PAs, depending on the business operations.

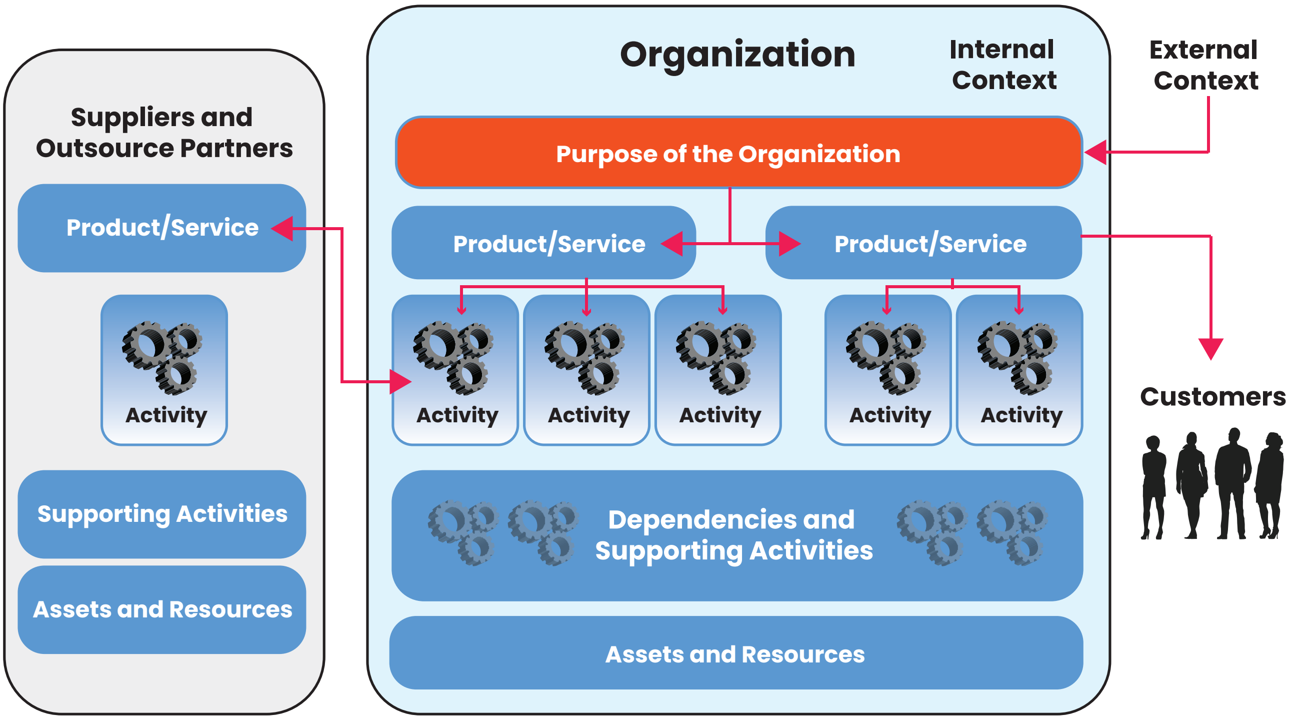


Figure 11: Understanding the Organization

Aspects	Examples
Financial	Losses from fines, penalties, lost profits, or reduced market share
Reputational	Damage to the organization’s image or brand perception
Operational	Disruption in flow, extent, and duration of business operations
Legal and regulatory	Risk of litigation or withdrawal of license to trade
Contractual	Breaches of agreements or confidence between partners, employees or customers
Business objectives	Failure to achieve objectives or take advantage of opportunities

Understanding the timeline of impact is also crucial for effective BCMS. The organization must determine the time it takes for disruptions to key activities to reach an unacceptable level. The senior management should set the thresholds of impact that are deemed unacceptable to the organization. The time frames will depend on the time sensitivity of the organization’s products and services. It can vary between seconds to months. This period is known as the “Maximum Tolerable Period of Disruption” (MTPD). This is the latest possible time by which the organization must resume its prioritized activities to avoid reaching a worst-case scenario that would end in bankruptcy. MTPD is the point at which the disruption causes irreversible or unacceptable damage. The minimum level of product or service that is acceptable to the organization can be expressed as the “Minimum Business Continuity Objective” (MBCO).

Actions should be identified to get the business operational again in the shortest possible timeframe, before heading towards exiting the business or filing for bankruptcy. The time frame for resuming an activity is known as the activity's "Recovery Time Objective" (RTO). RTO indicates how quickly we need to recover the process to avoid crossing the MTPD threshold. RTOs for each prioritized activity must be determined. Setting an activity's RTO may also need to consider the dependencies on related activities and the complexity of the recovery process. It may be appropriate for organizations with complex recovery processes to set multiple RTOs.

Table 6: Examples for MTPD and RTO

Process /activity	Impacts	MTPD	RTO
Cold storage system	Spoilage of perishable goods (e.g., dairy, meat, seafood)	4 hours	1 hour
Tourist hotel booking management system	Affects new reservations and modifications	2-3 days	12-24 hours

The criteria for evaluating the business impacts, including the types of impacts and time frames, should be established based on the context, business objectives, aims of the organization, and the needs of interested parties. These evaluation criteria should be reviewed and updated regularly, and more frequently during periods of change.

7. RISK ASSESSMENTS

Action Step: At the end of Chapter 7: Risk Assessments, complete Exercise 7 in the attached BCMS Manual.

Business risks are factors that threaten an organization's ability to operate effectively, potentially leading to lost profits or even business failure. Potential impacts included an inability to trade, temporary or permanent closure of premises, significant cost and time required for cleaning and rebuilding, limited access for customers, and disruption in the supply chain.

When identifying and managing risks, the organization needs to:

- Identify possible causes and impacts
- Assess how these risks affect the business objectives
- Record the identified risk in a risk management plan
- Detail the steps that could be taken to minimize the risk or the impact.

By considering potential risks and impacts in advance, organizations can develop procedures without added pressure of trying to manage the risk at the time.

Types of risks include:

- Direct risk – a threat to the business that is within the organization's control (Inadequate cybersecurity measures leading to data breaches, Poor inventory management resulting in stockouts or excess stock)
- Indirect risk – a threat to the business that is out of the organization's control (Economic downturns or changes in market conditions impacting sales, Supply chain disruptions caused by third-party vendor failures)
- Internal risk - risks an organization has the power to prevent or mitigate within the business (Equipment failure due to lack of maintenance, lack of staff training leading to errors)
- External risk - risks the organization has no control over (Natural disasters like earthquakes, or floods disrupting operations, Pandemics, or global health crises impacting workforce availability and supply chains)

Table 7: Risk Definitions

Aspect	Direct Risk	Indirect Risk	Internal Risk	External Risk
Definition	Threats directly affecting the business, within the organization's control	External threats indirectly impacting the business, often as a ripple effect	Risks originating from within the organization, preventable or mitigatable	Broad risks originating outside the organization, beyond its control
Origin	Internal	External	Internal	External
Control	Within the organization's direct control	Limited control; can manage impact.	Within the organization's control.	No control over occurrence or source.
Control level	High (can mitigate or eliminate)	Limited (can influence the impact)	High (can take proactive actions)	None (can only prepare or adapt)
Scope	Specific and immediate to the business.	Ripple effect from external factors	Arises from within the organization	Broad external factors
Preventability	Preventable with proactive measures	Impact can be mitigated or reduced	Preventable or mitigatable	Non-preventable; preparation required

The purpose of a risk assessment is to help the organization evaluate the risks of disruptions to its prioritized activities and take appropriate measures to address them. The organization should establish and maintain a formal risk assessment process to systematically identify, analyze, and evaluate the risks associated with disrupting its prioritized activities, as well as the supporting processes, systems, information, personnel, assets, suppliers, and other resources.

Risk assessment is a structured process that analyzes risks based on their likelihood and potential consequences, enabling informed decisions about any necessary treatments required. The organization should adopt an appropriate approach for identifying, analyzing, and evaluating risks that could lead to disruptions.

7.1. Identification of risks

Potential sources of risk to the organization's prioritized activities and the processes, systems, data, people, assets, suppliers, and other resources that support them should be identified. Risk can arise from:

i. Specific threats that may disrupt activities and resources such as:

- Fire
- Flooding
- Power outages
- Staff loss or absenteeism
- Computer viruses and cyber-attacks
- Hardware failure
- Climate-related events including heatwaves, storms, droughts, and changes in disease patterns

ii. Vulnerabilities within resources that could lead to disruptions, including:

- Single points of failure
- Inadequacies in fire or flood protection systems
- Lack of electrical or cooling resilience in extreme temperature conditions
- Inadequate staffing levels, or staff training in emergency response
- Poor IT security and resilience
- Exposure to climate-related risks such as facilities located in high flood zones, temperature-sensitive equipment without sufficient climate control

7.2. Analysis of risks

Risks come in different forms, with some having a significant impact while others are more moderate. Prioritizing which risks to focus on can be achieved by using a risk scale. This scale determines the likelihood of a risk occurring and its potential impact, assigning a risk score. A higher score indicates a greater priority for reducing the risk or impact. A proper evaluation and understanding of the risk allow for the identification of the most appropriate treatment approach. It involves:

i. Assessing the causes and sources of risk, the likelihood of both positive and negative consequences, and the effect that other factors could have on the likelihood

ii. Determining the risk levels, based on their likelihood and anticipated consequences, while considering the effectiveness and efficiency of existing controls

A key parameter in the analysis is likelihood, which should be validated based on experts' opinions, uncertainty, data availability & quality, and relevance of information, or limitations on modeling. The risk analysis can be qualitative - using descriptive assessments, semi-quantitative – combining numerical and descriptive methods, or quantitative - relying on numerical data and statistical analysis.

7.3. Evaluation of risks

Once the risks have been analyzed and prioritized, the organization should evaluate the effectiveness of its existing controls such as policies, resources, and tools to mitigate the identified risk. This evaluation should focus on which disruption-related risks require treatment, particularly for activities with high priority or with significant replacement lead time.

There are several options for risk treatment.

- Avoid: Change the plan to eliminate the risk
- Reduce: Implement measures to minimize the risk's likelihood or impact
- Transfer: Share the risk through outsourcing or insurance
- Accept: Acknowledge and monitor the risk if mitigation is impractical

7.4. Vulnerabilities of businesses for process interruptions

Businesses can experience interruptions to their operations due to disasters in several ways, depending on the nature and scale of the event. Some common disruptions include,

a) Physical Damage to Infrastructure
   - Damage to office buildings, factories, warehouses, or retail stores from natural disasters like earthquakes, floods, fires, or hurricanes
   - Equipment or machinery damage critical for production or services

b) Power and Utility Outages
   - Loss of electricity, water, or other utilities rendering facilities inoperable
   - Communication failures, such as internet or telephone outages, affect customer and supplier interactions.

c) Disruption to Supply Chain
   - Inability to procure raw materials, parts, or inventory due to transportation blockages or supplier disruptions
   - Loss of key suppliers or vendors due to their operational impacts

d) Staff Unavailability
   - Employee injuries, illnesses, or displacements during a disaster
   - Inability of staff to commute to work due to transportation or safety issues

e) Technology and ICT Failures
   - Damage to data centers, servers, or other critical ICT infrastructure
   - Cyberattacks or malware incidents that compromise business systems or data integrity
   - Lack of access to critical software or tools needed for operations

f) Customer Impact

- Reduced demand or inability to deliver products or services to customers due to widespread disaster impacts
- Challenges in maintaining customer support during service disruptions

g) Regulatory or Legal Issues

- Non-compliance with regulations due to missed deadlines or inability to access required documents
- Legal liabilities from failing to fulfill contractual obligations

h) Transportation Disruptions

- Blocked roads, damaged transport networks, or fuel shortages preventing movement of goods or people
- Delayed deliveries impacting operations or customer satisfaction

i) Financial Strain

- Immediate loss of revenue due to halted operations
- Increased costs for repairs, emergency resources, or alternative arrangements

j) Reputational Damage

- Inability to communicate effectively during and after a disaster, leading to negative customer or stakeholder perceptions
- Loss of trust if recovery takes too long or commitments are unmet

7.5. Availability of hazard and risk information and accessibility

Availability and accessibility of risk information are crucial for effective risk assessment in Business Continuity Management Systems (BCMS) in Sri Lanka. Reliable risk data enables businesses to identify vulnerabilities, assess potential impacts, and implement proactive mitigation strategies. Key sources include hazard maps, climate risk assessments, disaster history records, and sector-specific risk reports.

Table 8: Availability of Risk Information

Institute	Focus Areas
Disaster Management Centre (DMC),	Prime institution for disaster risk reduction (DRR) Sri Lanka's, offers hazard maps, risk assessments, and disaster-related historical data for various hazards, including floods, landslides, cyclones, and tsunamis. The Emergency Operations Centre (EOC) disseminates real-time hazard information.

National Building Research Organization (NBRO)	Focuses on landslide susceptibility analysis and mapping and providing technical guidance on risk mitigation and structural safety. It also monitors high-risk areas in real time and disseminate landslide hazard warnings.
Meteorological Department	Provides weather forecasts, hazard warnings, and historical data on climate-related risks.
Irrigation Department	Monitors flood hazard and prepares flood hazard maps tailored to different scenarios and return periods for several river basins.
Universities and research institutions	Conduct studies on hazards, risks, and resilience offering valuable insights through publications and research papers focused on localized risks and mitigation strategies.
UN agencies, the Asian Disaster Preparedness Center, the Red Cross Society, and the Sarvodaya Movement	Facilitate community resilient projects and generate localized hazard and risk information. Community-level hazard maps and participatory risk assessments are available for some high-risk areas.

UN agencies, the Asian Disaster Preparedness Center, the Red Cross Society, and the Sarvodaya Movement Facilitate community resilient projects and generate localized hazard and risk information. Community-level hazard maps and participatory risk assessments are available for some high-risk areas.

However, there are challenges in the availability and accessibility of hazard data. Information is often scattered across multiple institutions, making centralized access difficult. Certain hazards, such as industrial risks or specific localized vulnerabilities, may not be comprehensively mapped or assessed. While online resources are available, obtaining detailed or up-to-date information often requires personal requests or partnerships with institutions. Many businesses, particularly SMEs, are unaware of how to access or utilize hazard and risk information for BCMS.

8. RISK ASSESSMENTS

Action Step: At the end of Chapter 8: Business continuity strategies and solutions, complete Exercise 8 in the attached BCMS Manual.

Business continuity strategies are possible ways for the organization to meet its business continuity requirements, while business continuity solutions include specific approaches, arrangements, methods, procedures, treatments, and actions that can be put in place to implement business strategies. Each strategy should be comprised of at least one business continuity solution, though multiple solutions may be required to meet business continuity requirements.

Business continuity strategies and solutions:

a) Enable the organization to resume business operations within the required time frames (RTO) and at an acceptable capacity

b) Identify capabilities that the organization can implement and improve over time to mitigate disruption-related risks.

The identification of business continuity strategies and the selection of business continuity solutions should be based on the business impact analysis and the risk assessment while also taking into consideration the associated costs.

The organization should have in place procedures for identifying and selecting business continuity strategies and solutions, including review and approval of recommended solutions. The organization should identify appropriate strategies and solutions for protecting prioritized activities; stabilizing, continuing, resuming, and recovering prioritized activities; and mitigating and responding to managing impacts. All three phases are important and necessary for achieving the RTOs.

Table 9: Different phases of business continuity strategies

Phase	Focus	Timing	Goal
Protecting prioritized activities	Prevention	Before disruption	Avoid interruption
Stabilizing, continuing, resuming, recovering	Operational continuity	During and after disruption	Maintain or return to function
Mitigating, responding, managing impacts	Crisis management	Before, during, and after	Reduce effects and coordinate actions

8.1. Protection of prioritized activities

Protecting prioritized activities involves proactively safeguarding essential business functions before a disruption occurs. This can be achieved by reducing the risk of interruption, outsourcing activities to reliable third parties, or modifying how the activities are carried out if alternative methods are available. It includes planning, preparation, and the implementation of controls to prevent or minimize disruption to critical operations.

When identifying strategies and solutions for protecting prioritized activities, the organization should evaluate,

i. perceived vulnerabilities of the activity and the potential impacts of its disruption
ii. cost of protective measures compared to the anticipated benefits
iii. urgency of the activity, since there will be less time to resolve the issue
iv. overall feasibility and suitability of the proposed solutions

Examples include installing surge protectors and backups for critical servers, duplicating essential paper records in fireproof storage, securing supply contracts with alternative vendors for essential materials, and physically relocating high-value equipment away from flood-prone areas.

8.2. Stabilizing, continuing, resuming, and recovering prioritized activities

This involves actions taken during and after a disruption to maintain essential operations, resume them as quickly as possible if interrupted, and recover to normal operations. Setting RTOs for resuming prioritized activities at an agreed capacity enables the organization to identify strategies to shorten the period of interruption, reduce impacts, and enable the timely recovery of prioritized activities.

To ensure that prioritized activities can be resumed within their RTOs, compatible RTOs should also be set for the dependencies and supporting resources. Organizations should also determine the capacities at which dependencies and supporting resources would need to be resumed. When setting these RTOs, the organization may need to consider,

- the possibility of providing a different service until the point when full resumption is required
- ensuring that people are mobilized effectively
- providing encouragement and support for people returning to work at time of need
- workarounds (such as manual processes) that defer the need for resuming the dependency on supporting resources
- backlogs and time needed to recover lost information
- the complexity and scale of recovery requirements or the need for specialist equipment with a long lead time

Business continuity strategies may include the following.

a) Activity relocation: The transfer of some or all activities either internally to another part of the organization or externally to a third party, either independently or through a reciprocal or mutual aid agreement. When determining locations at which to resume an activity, damaged/affected sites and undamaged alternate sites should be considered.
b) Resource relocation or reallocation: Resources, including staff, are transferred to another location or activity within the organization, or externally to a third party.
c) Alternate processes and spare capacity: Establishing alternate processes or creating redundancy/spare capacity in processes and/or inventory.
d) Temporary workaround: Some activities may adopt a different way of working that provides acceptable results for a limited time. The workaround will probably be more time-consuming and/or labor-intensive (e.g. a manual operation as opposed to an automated system). For these reasons, workarounds are generally only suitable for short periods or deferring a return to business as usual.

8.3. Mitigating, responding to, and managing impacts

This focuses on reducing harm caused by the disruption, responding effectively to control the situation, and managing the consequences, such as communications, stakeholder reassurance, and long-term recovery. Strategies for mitigating, responding to, and managing the impacts of a disruption may include the following.

a) Insurance: The purchase of insurance can provide some financial recompense for some losses but will not meet all costs (e.g., uninsured perils, brand, reputation, interested parties' value, market share, human consequences). A financial settlement alone will not fully protect the organization and satisfy interested parties' expectations. Insurance cover is more likely to be used in conjunction with other solutions.
b) Asset restoration: Contracting the stand-by services of companies that specialize in the cleaning or repair of assets following their damage.
c) Reputation management: Developing an effective warning and communication capability and establishing effective incident communications procedures

For identified risks requiring treatment and in line with its overall attitude to risk, the organization should consider ways of reducing the likelihood, shortening the period, and limiting the impacts of a disruption.

If there is a specific hazard over which the organization has no control and which could significantly disrupt the organization (e.g., earthquake or flooding), the organization should, where appropriate.

- Identify strategies and implement solutions for limiting its potential impact
- Identify the external body responsible for monitoring the hazard
- Contact the external body to understand its notification protocols
- Analyze the notification protocols to determine if they align with the needs of the organization

8.4. Selection of strategies and solutions

The selection of business continuity strategies should be based on the extent to which they:

a. Ensure the timely resumption of prioritized activities at the agreed capacity within the time frames established during the business impact analysis.
b. Align with the organization's risk appetite, considering the type and level of risk it is willing to accept or mitigate.
c. Provide effective continuity solutions while maintaining cost efficiency and financial feasibility.

The organization should re-examine all solutions when changes are made to the operation of the organization. While ensuring continuity, organizations must take into account the different capacities of stakeholders and employees, including gender and disability-sensitive arrangements.

Business continuity solutions for stabilizing, continuing, resuming, or recovering a prioritized activity can often be prohibitively expensive. Where the organization estimates this to be the case, it should either select alternative solutions that are acceptable and meet its business continuity objectives or treat affected products and services as exclusions from the scope of the BCMS.

Where the organization estimates a threat to be extremely unlikely or the cost of protecting a prioritized activity to be prohibitively expensive, it may choose to accept the risk and re-evaluate it as part of its ongoing BCMS performance evaluation. Accepting the risk can also require the affected products or services to be removed from the scope of the BCMS.

9. RESOURCE REQUIREMENTS

Action Step: At the end of Chapter 9: Resource Requirements, complete Exercise 9 in the attached BCMS Manual.

The organization should determine the resource requirements to implement selected solutions.

9.1. People

The organization should ensure it has people with the necessary competencies to respond to and manage incidents, as well as participate in the resumption of prioritized activities.
The incident response personnel should form a group responsible for managing disruptions that significantly impact or have the potential to impact the organization. They should be organized into specialized groups such as incident management, communication, safety and welfare, security, and resuming activities. They should be capable of incident assessment, evacuation, and shelter management, arrangements at alternative worksites, internal and external communication and dealing with people aspects.

Response and recovery teams should receive training on their roles and responsibilities including interactions with first responders and other interested parties. Teams should be trained at regular intervals, with additional sessions for new team members. These teams should also be trained in the prevention of incidents that could escalate into crises.

The organization should identify appropriate people to enable the resumption of activities even with reduced staff availability. It is important to recognize that people may not respond as expected during an incident and may need encouragement, reassurance, and support. Employees, contractors and other interested parties with extensive specialist skills and knowledge should be included in the response structure. In the event of locating staff after an incident in the same or alternative worksite, the organization should consider the transportation of staff, accommodation, catering, personal family commitments, training on different equipment, and challenges related to working from home or remote.

9.2. Information and data

Information derived from data includes facts, statistics, numbers, etc. stored manually or electronically. If information or data required by an activity is irreversibly lost, resuming the activity may become impossible. Therefore, Information and data vital to the organization's operation should be protected and recoverable within the time frames identified during the business impact analysis.

When duplicating information and data, various methods may be used, including electronic formats and physical hardcopy formats. If copied information or data is stored too near to the original, the disruption could compromise the integrity or prevent access to it. Conversely, a long distance can prevent information/data from being available when needed.

Information and data essential to operations may include,

I. Contact information of internal and external parties including personnel and agencies required for managing emergencies
II. Supplier, details of interested parties
III. Legal documents such as contracts, insurance policies, title deeds
IV. Other service documents such as contracts, service agreements
V. Metadata
VI. Notification and alert messages are disseminated as an incident response measure
VII. Guidelines and criteria regarding who has the authority to invoke procedures

9.3. Buildings, workplaces, and associated utilities

Worksite solutions can vary widely, with multiple options can be available on the type of incident. The appropriate approach will depend on the organization's size, sector and spread of activities, need of interested parties, and geographical location.

The organization should formulate a solution that reduces the impact of the unavailability of its normal worksite. This may include,

- Alternative premises within the organization, including displacement of less critical activities
- Alternative premises provided by other organizations arranged through mutual agreements
- Command centers with dedicated facilities for managing operations during disruptions
- Alternative premises provided by third-party specialists
- Working from home or at remote sites
- Alternative workforce in an established site

Alternative premises should be carefully selected by taking account of a geographical area that could be affected by the same incident and affected essential services such as electricity, gas, water, and communication. If such a risk is expected, alternative premises should be distant from such a possible affected zone.

In some situations, where RTO is short, sifting the workload rather than the staff may be more practical. This can require spare capacity at the alternate site or additional staff (whether by overtime or recruitment) and other resources to be made available.

9.4. Equipment and consumables

The organization should identify and maintain an inventory of the core supplies that support its prioritized activities. Some facilities and machinery can be difficult to acquire, be very expensive, require a long time for authorization, or have long lead times. Solutions for providing such resources may need to take such issues into account. Changing business practices, such as stock control or building management, can provide solutions.

Possible approaches for providing these may include,

- Storage of additional supplies at another location
- Arrangements with third parties for delivery of stock at short notice
- Diversion of just-in-time deliveries to other locations
- Holding of materials at warehouses or shipping sites
- Transfer of certain operations to an alternative location that has supplies
- Identification of alternative or substitute supplies
- Identification of facilities and equipment and multi-option planning by phases

If specialist supplies are required, the organization should identify the suppliers on which the prioritized activities depend, especially where a single source is involved. Solutions to ensure the continuity of supply may include,

- Increasing the number of suppliers
- Encouraging or requiring suppliers to have business continuity
- Contractual or service-level agreements with suppliers
- Identification of alternative, capable suppliers

When relocating activities, it's important to verify that suppliers are able to provide their products or services effectively at the new location.

9.5. ICT systems

In many organizations, activities rely on ICT systems, and they need to be restored before activities can be resumed. Where possible and practical, manual workarounds can be implemented temporarily while ICT systems are being reinstated.

Solutions for ensuring ICT systems availability for prioritized activities include,

- Maintaining identical technology at different locations that will not be affected by the same disruption
- Keeping older equipment as an emergency replacement or spare parts
- Establishing contracts for equipment supply or recovery services
- Providing adequate facilities for increased numbers of users with remote access
- Providing automatic failover to reinstate ICT systems without manual intervention
- Improving communications connectivity and adding redundant routing options
- Setting up un-staffed (dark) sites as well as staffed sites

9.6. Transportation and logistics

After an incident, transportation may need to be provided for staff if their normal means of transport is unavailable, transport staff to an alternative work location, or transport resources to a different location. Identifying possible scenarios of logistic disruptions, the organization should determine options in advance,

- Providing alternative means of transport
- Agreements with alternative transport providers
- Alternative routes to deal with unusual traffic conditions

9.7. Finance

The organization should ensure the necessary finance is available during and following a disruption for,

- Providing funds for emergency purchases, such as food, accommodation, facilities, consumables, and transport
- Reimbursement of staff expenses
- Major expenditures such as the rental or purchase of buildings and equipment
- There shall be financial controls and records of expenses to prevent abuses and facilitate insurance claims.

Table 10: Availability of finance in a disaster

Monetary Incentives	Description
Saving	Utilization for the working capital, recovery cost and bridging the loss of income before the business recovery
Contingency funds	Reserve fund to use particularly for an unpredictable event like an incident or disaster
Insurance	Different sets of products that allow covering from the losses incurred when a risk materializes. e.g. property insurance, catastrophic micro-insurance, agricultural micro-insurance
Financial assistance after a disaster	Provision of assistance to individuals and companies affected by a disaster for relieving immediate suffering and facilitating recovery and reconstruction e.g. tax deduction/exemption, soft loan/subsidies
Repayment holiday / amnesty	Enterprises disrupted by a disaster are given a period of grace during which they can temporarily stop making payments towards a loan
Business taxes	Tax credits, deductions and exemptions provided to businesses that invest in DRM, in such areas as the construction of resilient buildings.

Subsidies & grants	Promote the adoption of disaster preparedness practices (e.g. education and training in evacuation procedures), and the use of disaster risk reduction systems (e.g. warning systems, maintenance of evacuation routes and provision of vehicles, signs and shelters).
Soft loans	Financing arrangements for DRM systems or equipment, provide access to low interest loans for integrating resilient programs and practices into businesses.

9.8. Partners and supply chain

It is essential to understand the supply on which prioritized activities depend chain and analyze risks and impacts jointly with relevant suppliers. Suppliers, in turn, should be required to cascade the analysis to their suppliers. Where prioritized activities or business continuity solutions rely on products and services from a supplier, the organization should evaluate and obtain assurance on the suppliers' business continuity arrangements in place. The organization should assess the level of dependency on the supply chain and specific suppliers within it and understand the timescales for finding alternative arrangements. Ensuring suppliers' and partners' BCMS and evaluating them.

- BCMS requirements may be specified in the supply or partner contracts
- Conduct periodic audits
- Conduct joint BCMS exercises

10. CONDUCT EXERCISES TO ENSURE THE FUNCTIONALITY OF THE BCMS

Action Step: At the end of Chapter 10: Conduct exercises to ensure the functionality of the BCMS, complete Exercise 10 in the attached BCMS Manual. A scenario for the tabletop exercise will be given separately.

An organization’s business continuity procedures and arrangements cannot be considered reliable until exercised. Exercising develops teamwork, competency, confidence, and knowledge, and should include those who could be required to use the procedures. Robust and realistic exercises identify areas for improvement even in well-designed procedures. The organization should conduct an exercise program that validates over time the effectiveness of its business continuity strategies and solutions, plans, and procedures.

At early stages of maturity, exercising and testing may be limited to the use of checklists, drills, and awareness exercises. As the program matures, it may extend to include tabletop exercises and full-scale live simulations.

The exercise program should consider the roles of all parties, including third-party providers, suppliers, and others who would be expected to participate in recovery activities. An organization may include such parties in its exercises and may participate in exercises that they organize.

The different types of exercises can be carried out and they generally be discussions or simulations. Discussion-based exercises are designed to familiarize participants with business continuity plans and procedures in a low-stress environment. Simulation-based exercises are designed to be more realistic and challenging. They can be carried out in the normal operational environment, alternative premises, or command centers.

Plan reviews are informal reviews of plans and procedures that are used to familiarize participants with new or updated content. They are useful as a starting point when plans and procedures are first developed or when they are revised significantly.

On-site/off-site tabletop exercises use simple scenarios to familiarize participants with plans and procedures in a low-stress environment. They can also be used to review business continuity strategies and solutions for validation and improvement. An on-site tabletop exercise is usually the first type of formal exercise conducted by an organization.

Workshops are usually conducted off-site at alternative premises using reasonably complex scenarios. Exercise participants may represent a single plan or multiple plans depending upon the scope of the exercise. Similarly, exercise participants may be represented from one or more locations using scenarios that impact one or multiple locations. The purpose is for teams to practice working together and making decisions under more stressful time frames.

Full-scale exercises are designed to prepare participants for disruptions that impact the entire organization and require activation of the business continuity plan. They are complex, high-stress exercises that are carefully planned and controlled to ensure that they achieve their objectives and do not cause a disruption.

As part of the exercise, a review should be conducted with all participants to discuss the issues encountered and lessons learned. It is also important to track how well the system addresses the needs of all stakeholders, including those most vulnerable, such as women and people with disabilities. The organization should undertake a post-exercise debriefing and perform an analysis of the outcome. This information should be documented and updates made to the procedures as required.

10.1. Maintenance aspects of BCMS

Regular drills and routine checks play a crucial role in sustaining an effective Business Continuity Management System (BCMS). Embedding these practices into Standard Operating Procedures (SOPs), such as maintaining firefighting equipment and ensuring unobstructed evacuation routes, strengthens organizational preparedness.

Drills not only validate Business Continuity Plans (BCPs) but also uncover potential gaps, allowing for continuous improvement. Incorporating lessons learned from these exercises into periodic BCP reviews enhances overall resilience. Additionally, third-party assessments and recertification offer objective evaluations, ensuring ongoing compliance and accountability.

Despite challenges in maintaining consistency, organizations can achieve a structured and systematic approach to business continuity. This ensures that the BCP remains relevant, adaptable, and capable of mitigating disruptions effectively.

EDITORIAL BOARD

References

ADPC (2018). Training of Trainers Course on Business Continuity Management. Colombo, Sri Lanka. Asian Disaster Preparedness Center.

APEC (2013). Guidebook on SME Business Continuity Planning. Asia-Pacific Economic Cooperation.

CCC (2024). Capacity Need Mapping of SMEs in Disaster Risk Reduction and Management. Colombo, Sri Lanka.

DMC (2017). National Emergency Operation Plan August 2017. Colombo, Sri Lanka: Disaster Management Centre.

DMC (2023). National Disaster Management Plan 2022-2030. Colombo, Sri Lanka: Disaster Management Centre.

ILO (2019). Business Continuity Plan – BCP, Colombo, Sri Lanka: International Labour Organization.

ISO Survey. The ISO Survey. Retrieved from https://www.iso.org/the-iso-survey.html
Ministry of Industry and Commerce, 2013. National Policy Framework for Small Medium Enterprise (SME) Development. Colombo, Sri Lanka.

P&S Intelligence. Business Continuity Management Market Size & Share Analysis. Retrieved from https://www.psmarketresearch.com/market-analysis/business-continuity-management-planning-solutions-market

Business Continuity Management System Manual	
Company Name	
Version	
Edited/Revised on	

Version History		
Version	Revision Date	Description of Change

Prepared by	Title	Date
Approved by	Title	Date

Table of Contents

Exercise 4

4. Company Profile

4.1. Context of the organization

4.1.1. Description of the company

Note: Describe the company in terms of main sector of operation, number of years in operation, operational departments, linked value chain, market share volume, legal & regulatory status, etc.

4.1.2 Products /Services

Note: List the main product/service categories and products/services

Table 4-1 List of Products / Services

Product/service category 1	Product/service category 2
List of products/services	List of products/services

4.1.3 Interested Parties

Note: List key employment categories, suppliers, distributors/vendors, insurers, regulatory bodies, customer segments, etc. Expectations of the Interested Parties shall also be listed.

Table 4-2 List of Interested Parties

Categories of Interested Parties	Expectations
Categories of key employment	
Suppliers	
Distributors	
Insurers	
Bankers	
Regulatory Bodies	
Customer Segment	

4.2. Business Continuity Management System Framework

4.2.1 Business Continuity Management System Objectives

Note: List the specific purposes/objectives for establishing BCMS

Table 4-3 BCMS Objectives

Protecting People	
Protecting Business Activities	
Supporting Local Community	

4.2.2 Scope of the BCMS

Note: List the plant, office, or department to be covered in the BCMS and any exclusions with justification

Exercise 5

5.1 Leadership and Team

5.1.1 Business Continuity Management Team

Note: Identify the appropriate staff members in the company who can deliver the role and responsibilities of BCMS Positions.

Table 5-1 List of BCM Team

BCMS Positions	Assigned Staff	Roles and responsibilities
Business Continuity Manager	Name Position Tel.	□ *Leads the BCM team and the development, implementation, and maintenance of the BCMS.* □ *Coordinates all BC activities and ensures compliance with policies and standards.*
Crisis Management Team Leader	Name Position Tel.	□ *Makes strategic decisions during a crisis.* □ *Communicates with stakeholders, media, and authorities.*
Emergency Response Team Leader	Name Position Tel.	□ *Handles immediate response actions (e.g., evacuation, first aid, fire control).* □ *Works closely with local emergency services.*
Department 1 Recovery Team Leader	Name Position Tel.	□ *Restore essential business functions.* □ *Ensure continuity of critical processes.*
Department 2 Recovery Team Leader	Name Position Tel.	□ *Restore essential business functions.* □ *Ensure continuity of critical processes.*

BCMS Positions	Assigned Staff	Roles and responsibilities
BC Support /Logistics Team Leader	Name Position Tel.	□ *Ensures the physical safety of personnel and assets.* □ *Manages logistics, and utility restoration.*
Communication Team Leader	Name Position Tel.	□ *Manages internal and external communications during a disruption.* □ *Ensures consistent, timely, and accurate messaging.*

5.2 BCMS Policy

Note: Insert the BCMS policy statement.

At ………………………… [Company Name], we are committed to ensuring the continuity of our essential business operations in the event of disruptions, emergencies, or crises. Our Business Continuity Management System (BCMS) is designed to protect our people, safeguard our assets, and maintain the delivery of products and services to our customers. The BCMS is aligned with ISO 22301:2019 and forms an integral part of our risk management and organizational resilience framework.

This policy is communicated internally and made available to interested parties as appropriate. It is reviewed annually or upon significant change to ensure continued relevance.

Exercise 6

6.Business Impact Analysis

6.1 PA, MTPD, and RTO

Note: Determine the Prioritized Activities (PA), Maximum Tolerable Period of Disruption (MTPD) & Recovery Time Objective (RTO)

I. *List the products, activities, or processes (1)*

II. *Based on the Criteria in Table 6-2, rate the level of impact due to disruption to each activity using a scale of 1-4*

III. *Calculate the average impact level score (3)*

IV. *Compare the importance of activities and prioritize activities (PAs) (4)*

V. *Estimate MTPD (5) and RTO (6) for each PA in the number of days, weeks, or months*

Table 6-1 PA, MTPD, and RTO

(1) Product / Activity / Process	(2) Level of Impact				(3) Average Impact Level Score	(4) Priority	(5) Maximum Tolerable Period of Disruption (MTPD)	(6) Recovery Time Objective (RTO)
	Financial Income	Financial Expense	Non-financial External	Non-financial Internal				

Table 6-2 Criteria for analyzing the business impact

Level of Impact	Financial		Non-financial	
	Income reduced	Expense increased	External (Loss of reputation)	Internal (loss of employees' confidence)
1. Low	<25%	<25%	Low	Low
2. Medium	25 – 49%	25 – 49%	Medium	Medium
3. Significant	50 – 74%	50 – 74%	High	High
4. Severe	>75%	>75%	Severe	Severe

6.2 Internal Resources

Table 6-3 Internal Resource for PA 1

Resource	Requirement	Note
Personnel		
Building		
Equipment / Machinery		
Funds		

6.3 External Resources

Table 6-4 External Resource for PA 1

Resource	Detail	Service Provider	Contact details
Electricity			
Water			
Internet service			

6.4 Supply Chain

Table 6-5 Stakeholders List for PA 1

Stakeholders	Detail	Service Provider	Contact details
Supplier			
Supplier			
Distributor/Customer			
Distributor/Customer			

Exercise 7

7. Risk Assessment

7.1 Identification of Potential Hazards

Note: Identify (underline) the hazard/s that might affect the business and circle the level of concern for each

Table 7-1 List of Potential Hazards

Hazard	No concern	Low concern	High concern
Natural Hazards			
Flood	1	2	3
Earthquake	1	2	3
Forest fire	1	2	3
Drought	1	2	3
Windstorm	1	2	3
Pandemic	1	2	3
Contamination or Pest infection	1	2	3
	1	2	3
Human-made Hazards			
Machine Breakdown	1	2	3
Employee on strike	1	2	3
Fire	1	2	3
Electricity Outage	1	2	3
Data Loss	1	2	3
Hazardous substance	1	2	3
Political unrest	1	2	3
	1	2	3

7.2 Assessing and Prioritizing Risk

Note: Follow the steps given below for Assessing and Prioritizing Risk

I. *Filled in the name of hazards (1) which are regarded as "High Concern" in Table 7-1*

II. *Analyze the likelihood of occurrence (2) of the hazard based on the scale 1-5 using criteria given in Table 7-3*

III. *Evaluate the impact of the hazards (3), (4), (5), and (6) in Table 7-4 based on the criteria given in Table 7-5, and calculate the average level of impact (7)*

IV. *Transfer the Level of Impact (7) to Table 7-2*

V. *Calculate the Risk Score (8) by multiplying the likelihood (2) by the impact (7)*

VI. *Prioritize (9) the hazards based on the Risk Score (8)*

Table 7-2 Risk Calculation

(1) Hazard (High Concern)	(2) Likelihood of Occurrence (L)	(7) Level of Impact (I)	(8) Risk Score (L x I)	(9) Priority

Table 7-3 Hazard Ranking Criteria

Level	Criteria	
	Based on historical data	Based on perceived likelihood
1: Low	May occur and has occurred once in the last 10 years	May occur only in exceptional circumstances; highly unlikely (<5% chance)
2: Moderate	Has occurred once within the last 5 years	Could occur at some time, but not expected in the near term (5–20%)
3: Significant	Has occurred twice in the last 5 years	Might occur at some time; moderate probability (20–50%)
4: High	Has occurred 3 or more times in the last 5 years	Will probably occur in most circumstances (50–80%)
5: Very High	Has occurred 5 or more times in the last 5 years	Expected to occur in most cases; high probability (>80%)

Table 7-4 Impact Calculation

(1) Hazard	(3) Financial	(4) Physical Assets	(5) Employees	(6) Reputation	(7) Average Level of Impact

Table 7-5 Impact Ranking Criteria

Level	Financial	Physical assets	Employees	Reputation
1: Low	No to low impact; no additional expense	No to minor damage but can be resumed utilizing internal resources	No injury or considerable impacts	Acknowledged internally
2: Moderate	Moderate impact; low additional expense	Moderate damage but can be resumed utilizing internal resources	Insignificant injury or impacts a small group of employees	Acknowledged by certain group of customers
3: Severe	Severe impact; severe additional expense	Severe damage which requires external assistance for resumption in the short term	Moderate number of employees suffer injures or casualties	Acknowledged by the majority customers
4: High	High impact; high additional expense	High level of damage which requires external assistance for resumption in the medium term	Widespread impacts to the majority of the employees	Damages broasted and widely criticized
5: Very High	Very high impact; significant additional expense	Very high level of damage which requires external assistance and/or replacement of infrastructure	Substantial number of employees are affected e.g. casualties, injuries and psychologically	Widespread to news agencies, affects the long-term credibility

Exercise 8

8. Business Continuity Strategies and Solutions

Table 8-1 List of Potential Reasons for Business Interruptions to Consider When Identifying Strategies

Physical Damage to Infrastructure	Damage to buildings, factories, warehouses, or retail stores Equipment or machinery damage
Power and Utility Outages	Loss of electricity, water, or other utilities Communication failures, affect customer and supplier interactions
Disruption to Supply Chain	Inability to procure raw materials, parts, or inventory due to transportation blockages or supplier disruptions Loss of key suppliers or vendors due to their operational impacts
Staff Unavailability	Employee injuries, illnesses, or displacements during a disaster Inability of staff to commute to work due to transportation or safety issues
Technology and ICT Failures	Damage to data centers, servers, or other critical ICT infrastructure Cyberattacks or malware incidents that compromise business systems or data integrity Lack of access to critical software or tools needed for operations
Customer Impact	Reduced demand or inability to deliver products or services to customers due to widespread disaster impacts Challenges in maintaining customer support during service disruptions
Regulatory or Legal Issues	Non-compliance with regulations due to missed deadlines or inability to access required documents Legal liabilities from failing to fulfill contractual obligations
Transportation Disruptions	Blocked roads, damaged transport networks, or fuel shortages preventing movement of goods or people Delayed deliveries impacting operations or customer satisfaction
Financial Strain	Immediate loss of revenue due to halted operations Increased costs for repairs, emergency resources, or alternative arrangements
Reputational Damage	Inability to communicate effectively during and after a disaster, leading to negative customer perceptions Loss of trust if recovery takes too long or commitments are unmet

8.1 Resource Plan

Table 8-2 Resource Tracking Chart: Risk 1, PA 1

	Resources	Week 1							Week 2							Week 3							Week 4						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Internal																													
External																													
Supply Chain																													

Table 8-3 Resource Tracking Chart: Risk 2, PA 1

	Resources	Week 1							Week 2							Week 3							Week 4						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Internal																													
External																													
Supply Chain																													

8.2 Business Continuity Strategies

Table 8-4 Business Continuity Strategies, Risk 1, PA 1

Risk 1						
Prioritized Activity 1						
MTPD & RTO	MTPD:		RTO:			
Strategy Outline						
Necessary Resource	Prevention & Mitigation		Emergency Response	Recovery	Person/dept. in charge	External partners
	Short term	Long term				
Internal Resources						
Personnel						
Building						
Equipment /Machinery						
Funds						

External Resources						
Electricity						
Water						
Internet Service						
Stakeholder						
Supplier						
Supplier						
Distributor/Customer						
Distributor/Customer						

Table 8-5 Business Continuity Strategies, Risk 2, PA 1

Risk 2						
Prioritized Activity 1						
MTPD & RTO	MTPD:			RTO:		
Strategy Outline						
Necessary Resource	Prevention & Mitigation		Emergency Response	Recovery	Person/dept. in charge	External partners
	Short term	Long term				
Internal Resources						
Personnel						
Building						
Equipment /Machinery						
Funds						

External Resources						
Electricity						
Water						
Internet Service						
Stakeholder						
Supplier						
Supplier						
Distributor/Customer						
Distributor/Customer						

Note: Similarly, Risk 1 & 2, and PA2 can be considered for identifying recovery strategies and solutions.

8.3 Emergency Response Plan

Table 8-6 Evacuation Information

Emergency Response Team Leader	
Evacuation point (Meeting point)	
Alternative point	
Person in charge of rescue	
Person in charge of medical first response	
Details of nearest hospital / medical facility	
Emergency response activation threshold	

Note:

1) The emergency response team is responsible for stabilization, rescue, medical care, and confirmation of employee safety, sanitation, and logistics.

2) Thresholds can be based on the scale, severity, or type of incident. Severity can be measured based on the number of affected people, potential business impact, duration of disruption, etc., e.g., Any event requiring coordination across multiple departments or locations; Disruption of critical business functions exceeding X hours; Health and safety incidents with risk of casualties; Regulatory or reputational risks escalating beyond acceptable levels.

8.3.1 Emergency Contact Lists

Table 8-7 Emergency Contact List (Internal)

Department	Name	Telephone	Responsibility / EM skills	Safety Status

Table 8-8 Emergency Contact List (External)

Category	Name	Telephone	Specialty	Status
Emergency Service Providers				
Suppliers				

Category	Name	Telephone	Specialty	Status
Customers / Distributors				

Table 8-9 List of Activities for Supporting Community

Activities	Officer In charge	Resource Need
Pre-Disaster (Prevention and Mitigation		
During a Disaster (Response)		
Post Disaster (Recovery)		

Exercise 9

9. Resource Requirements

9.1 People

Table 9-1 List of Groups / Teams

Groups / Teams	Assingments	Capabilities of members

9.2 Information and Data

Table 9-2 List of Information/Data

Information / data	Source

9.3 Buildings, Workplaces

Table 9-3 List of Buildings/Workplace Arrangements

Building / workplace requirements	Arrangements

9.4 Equipment

Table 9-4 List of Equipment Arrangements

Equipment requirements	Arrangements

9.5 Transportation and Logistics

Table 9-5 Logistic Arrangements

Logistic requirements	**Arrangements**

9.6 Financing

Table 9-6 Financing Arrangements

Financial Measures	Amount	Details

Exercise 10

10 Exercise

10.1 Exercise Schedule

Table 10-1 Exercise Plan

Type of Exercise	Objective	Scenario	Date	Participants	Location	Revision/Update

Note:

1. Type of Exercise - Tabletop, Simulation, Full-scale, Communication Drill

10.2 Tabletop Exercise

Table 10-2   Tabletop Exercise Details

Tabletop Exercise Company:	
Date & Time	
Location	
Objectives	Test BCP
Scenario	
Assumptions / Limitations	

Table 10-3 Tabletop Exercise Participants

Participants	
Name	Roles
Observers	

Table 10-4 Tabletop Exercise Flow

Exercise Flow	
Unfold scenario (Timeline)	
Key Decisions made	
Discussion points	

Table 10-5 Tabletop Exercise Performance

Performance	
What went well	
Gaps Identified	
Unclear roles	
Delay in decisions	

Table 10-6   Tabletop Exercise Recommendations

Recommendations to Improve BCP	

Case Study: Rising from the Ashes: How Company A built resilience through Business Continuity Management System

(Note: The Company A (The identity of the organization has been withheld for reasons of confidentiality. In this publication, it is referred to as 'Company A') case illustrates how the absence of a Business Continuity Management System (BCMS) can leave even a well-established business vulnerable to collapse following a disaster, potentially leading to permanent closure. However, through adaptive actions and strategic partnerships, the company managed to survive and subsequently developed a comprehensive Business Continuity Management System (BCMS) with clear mitigatory and response strategies. This transformation highlights the critical importance of proactive preparedness and resilience planning.)

1. Context of the Company A Pvt Ltd

Company A, established in 2009 under the Board of Investment (BOI) of Sri Lanka, emerged as a leading manufacturer of flexible packaging solutions for food and industrial applications.

Located in the Mawathagama Export Processing Zone, the company gained a reputation for quality and innovation, driven by Japanese- and European-grade machinery and rigorous quality standards, including ISO 22000, HACCP, and GMP certifications.

Company A offered a diverse range of packaging solutions, including reels, pouches, and sheets, crafted from materials such as aluminum foil, BOPP, PET, nylon, PVC, and others. Their value-added services encompassed in-house design, high-precision gravure printing (up to 8 colors), laboratory-grade quality testing, and reliable island-wide distribution. Within the Sri Lankan flexible packaging sector, Company A held a market share of approximately 10%. This position was secured through high-quality products, island-wide delivery, export orientation, and a strong presence in the FMCG packaging segment. Their in-house gravure printing and award-winning designs set them apart in a competitive market.

The annual turnover is in the range of LKR 1.2 – 1.5 billion and employs approximately 150 staff, including skilled machine operators, design and QA personnel, logistics, and administration.

By 2016, Company A had already earned national recognition with awards such as the Wayamba Wijayabhimani (2013, 2015), Lanka Star Awards (2014–2016), and CNCI Achiever Award (2014), reflecting operational excellence and industry leadership.

2. The Crisis

In 2016, disaster struck. A massive fire broke out and completely destroyed Company A's entire factory, including buildings, machinery, and inventory. This catastrophic event brought operations to a sudden halt and posed a critical threat to the survival of the company. At the time, Company A lacked a documented contingency or business continuity plan. The incident not only devastated its physical assets but also tested the company's ability to respond strategically and demonstrate strong leadership under intense pressure.

3. Leadership & Decision-Making

The Managing Director took decisive action immediately after the fire:

- Quick assessment of damage and needs.
- Mobilized internal teams and external partners.
- Refused to shut down permanently, he chose to rebuild fast.

His focus was not just survival but bouncing back stronger.

4. Crisis Management and Continuity Planning (In the absence of a pre-developed Business Continuity Plan)

In support of the decision, the company staff strategically team up for:

- Immediate damage assessment and site clearance.
- Engage insurance, financial partners, and government agencies for emergency support.
- Making swift actions to continue prioritizing critical orders.
- Develop a rapid rebuilding plan and resume operations within four months.
- Procure advanced machinery and redesign production processes for improved safety and efficiency.

This phase demonstrated remarkable crisis leadership, stakeholder coordination, and employee loyalty, enabling the company to fulfill pending orders and retain key clients despite the interim disruption.

5. Prioritized Response; Operational Continuity

Following the fire, recognizing the importance of retaining customer confidence, Company A prioritized fulfilling orders for its key clients to preserve trust and sustain long-term business relationships. This showed a clear commitment to continuity despite the crisis.

Company A quickly established partnerships with peer factories within Sri Lanka. These collaborations allowed the company to temporarily outsource key aspects of the production process. By leveraging established industry networks, Company A ensured that quality standards were upheld while its own facilities were under reconstruction.

Company A promptly assessed its external storage and logistics chains. Finished goods and semi-finished materials located in warehouses or already in transit were identified and recovered.

These resources were used to meet the most urgent customer requirements, demonstrating agility and resourcefulness under pressure.

Company A took a proactive approach to communication. Clients were contacted immediately with honest updates, revised timelines, and possible alternatives. This open and transparent dialogue helped the company maintain credibility and strengthen customer loyalty during the disruption.

6. Resilient Recovery Process

As outsourced operations stabilized immediate supply demands, Company A simultaneously launched an aggressive plan to rebuild its manufacturing base. Within just four months, the company had installed essential machinery, restored critical infrastructure, and resumed in-house production, an extraordinary turnaround made possible by strong leadership, decisive planning, and stakeholder support.

This recovery phase was more than a return to normal; it became the launchpad for a formal Business Continuity Management System (BCMS). The lessons from the fire catalyzed long-term investments in infrastructure resilience, emergency preparedness, and supply chain diversification. Company A embedded risk assessments, continuity planning, and regular drills into its core operations, transforming from a reactive organization into a resilient one, better prepared for future shocks.

7. Mobilization of Staff

Rather than laying off staff during the downtime, Company A reassigned experienced personnel to oversee outsourced production lines. Employees also played a vital role in maintaining quality assurance, coordinating logistics, and managing client relations. This strategy not only preserved institutional knowledge but also reinforced employee morale and accountability.

8. Financing for Recovery

Company A had insurance coverage partially on assets, including buildings, machinery, and inventory. They worked closely with the insurance company to promptly assess damages, submit claims, and expedite settlements. This was able to provide only 10% of the core capital needed to rebuild the factory and reinvest in high-end machinery.

However, Company A’s strong goodwill and longstanding relationships with banks, external stakeholders, and clients played a crucial role in enabling a swift and strategic recovery. As a registered BOI enterprise, Company A benefited from preferential loan terms and financial facilitation through national banking institutions. In the absence of adequate insurance payouts, the company secured working capital loans and equipment financing, likely leveraging its creditworthiness, leadership credibility, and trust built over time with commercial banks and partners.

Internally, Company A restructured its budgets, reprioritized spending, and redirected internal reserves to maintain essential business operations like staff salaries, outsourcing costs, and client servicing. Leadership emphasized financial discipline and lean operations during the transition.

Long-standing supplier and customer relationships further supported liquidity through favorable credit terms and continued order flows. Further, well-maintained client confidence ensured continued cash flow through advanced orders and staggered payments.

9. Building Business Continuity and Organizational Resilience

Post-recovery, Company A transformed its approach to business continuity and risk management. Key strategies included:

1. Infrastructure Resilience:

- Rebuilt factory with fire-resistant materials and structural fire zoning.
- Installed modern fire suppression and detection systems.

2. Operational Risk Management:

- Established a formal Business Continuity Management System (BCMS).
- Developed risk registers, recovery time objectives (RTOs), and fallback procedures.
- Introduced preventive maintenance and upgraded safety interlocks.

3. Quality and Compliance Reinforcement:

- Enhanced internal QA/QC labs.
- Retained and expanded certifications (ISO 22000, HACCP, GMP).
- Introduced product traceability and batch-level tracking systems.

4. Workforce Resilience:

- Conducted regular fire and emergency drills.
- Trained staff in disaster response, machine safety, and business continuity awareness.
- Fostered a safety-conscious culture through continuous engagement.

5. Governance and Documentation:

- Strengthened internal audits and compliance oversight.
- Introduced comprehensive SOPs and incident-reporting protocols.
- Embedded continuous improvement (Kaizen) and lessons-learned reviews.

6. Supply Chain and Customer Assurance:

- Developed alternative sourcing arrangements and maintained buffer stocks.
- Communicated proactively with customers about contingency measures.

7. Brand Recovery and Recognition:

- Publicized the successful comeback through media and award platforms.
- In 2019, won three National Business Excellence Awards, and MD Nashad Nawas received the "Most Excellent Young Entrepreneur of the Year" award.

10. Outcomes and Lessons Learned

Company A not only recovered from total devastation but also emerged stronger, surpassing its pre-crisis performance. The fire became a turning point that led to modernization, deeper risk awareness, and stronger stakeholder trust. Today, the Company A ranks among the top five companies in Sri Lanka's flexible packaging industry, commanding over 45% market share. Just two years after the shock, Managing Director was recognized as the "Youngest Entrepreneur of the Year 2018" at the "Entrepreneur of the Year 2018" organized by FCCISL. Company A has been awarded the "Gold Award in the Printing and Related Services Sector" at the National Business Excellence Awards 2019, organized by the National Chambers of Commerce, Sri Lanka. In 2022, Company A was honored with the "Best Energy Efficient & Environmentally Friendly (Sustainable) Enterprise Award" organized by the Industrial Services Bureau of Northwestern province. Today, Company A serves as a model for industrial resilience, demonstrating that adversity can be transformed into opportunity through well-executed business continuity planning.

11. Conclusion

Company A's story highlights how a crisis, though devastating, can catalyze long-term transformation. Their experience underscores the importance of leadership, planning, staff training, and governance in building resilient enterprises capable of withstanding future shocks. As such, Company A serves as a powerful example of successful Business Continuity Management in the Sri Lankan manufacturing sector.

Case Study: Company B – Business Continuity Management during the COVID-19 Pandemic

(Note: The Company B (The identity of the organization has been withheld for reasons of confidentiality. In this publication, it is referred to as 'Company B') case illustrates how the absence of identifying risk to human health (Like the COVID-19 Pandemic) in the Business Continuity Management System (BCMS) can leave even a globally established business vulnerable to operational disruption. Nevertheless, the flexibility and adaptability of the BCMS allowed it to respond effectively and ensure continuity. Subsequently, the company updated its BCMS, incorporating mitigatory and response strategies, response protocols, and insight from the post-incident review. This highlights the importance of proactive preparedness and resilience in business planning.)

1. Context of the Company B

Company B is one of South Asia's largest apparel and textile manufacturing conglomerates, headquartered in Sri Lanka. Supplying globally recognized brands such as Nike, Victoria's Secret, and lululemon, Company B employs over 100,000 people across more than 15 countries.

Known for its innovation, sustainability, and ethical manufacturing practices, Company B also places significant emphasis on risk management and business resilience.

Before the COVID-19 pandemic, Company B had a decentralized Business Continuity Management System (BCMS), with frameworks in place to handle supply chain disruptions, technology failures, and natural disasters. However, the system had not been tested against a global pandemic scenario.

2. The Onset of the COVID-19 Crisis

In early 2020, the global outbreak of COVID-19 quickly escalated into a full-blown health crisis. As cases surged and governments imposed lockdowns, Company B faced a cascade of operational challenges:

- Complete and partial shutdowns of factories across Sri Lanka and other regions.
- Cancellation or suspension of orders from key export markets.
- Workforce safety risks, particularly in high-density manufacturing environments.
- Disruption of global supply chains and movement restrictions for raw materials.

The COVID-19 outbreak rapidly evolved into a business continuity crisis, impacting production, delivery, finances, and the welfare of Company B's vast employee base.

3. Activating the BCMS

Recognizing the gravity of the situation, Company B activated its Business Continuity Management System at the group level. The immediate priorities were:

1. Protecting employee health and welfare
2. Ensuring essential business operations
3. Maintaining stakeholder trust and communication

A Pandemic Response Task Force was formed under the leadership of the Executive Committee. This team coordinated real-time responses across business units, facilities, and geographic locations.

4. Crisis Response Measures

Company B responded with agility and creativity across several domains:

Employee Safety and Factory Restructuring

- Rapid implementation of health screening, quarantine protocols, and social distancing measures in factories.
- Staggered shifts and transport bubbles to minimize contact.
- Establishment of onsite medical support and access to PCR testing in collaboration with public health authorities.

Remote Work and IT Enablement

- Within a week, over 2,000 office employees shifted to remote working using cloud-based infrastructure and collaboration tools.
- Cybersecurity protocols were enhanced to support the expanded digital workforce.
- Pivoting to PPE Production
- Company B leveraged its manufacturing expertise to design and produce personal protective equipment (PPE), including reusable face masks, surgical gowns, and face shields.
- This strategic pivot ensured cash flow continuity while contributing to global pandemic response efforts.

Strengthening Communication

- Transparent, frequent updates were delivered to employees, buyers, vendors, and regulators.
- A dedicated team managed internal and external crisis communication, enhancing stakeholder confidence.

5. Business Recovery and Transformation

By the second half of 2021, Company B was well on the road to recovery. Key milestones in the business continuity journey included:

- Progressive reopening of manufacturing facilities under government health guidelines.
- Launch of vaccination drives in partnership with health authorities to ensure employee immunization.
- Development of 'Smart Factory' solutions using automation and IoT to reduce future disruption vulnerability.

Business units such as Company B Intimates and Company B Active were able to regain order volumes faster than regional competitors. The PPE business created new market channels and built resilience in product diversification.

6. Lessons Learned and BCMS Improvements

The COVID-19 experience was transformative for Company B. Post-crisis evaluations led to several critical updates to the BCMS framework:

- Pandemic-specific SOPs were integrated into facility-level BCPs.
- Cross-functional simulations and tabletop exercises were introduced to improve real-time decision-making.
- A business resilience unit was established to lead enterprise risk reviews and scenario planning.

Employee welfare emerged as a central tenet of business continuity. Company B strengthened its occupational health infrastructure, recognizing that protecting people is foundational to sustaining operations.

7. Conclusion – Resilience in Action

Company Bs' proactive, people-centered, and innovative response to the COVID-19 crisis demonstrated the value of a robust and flexible BCMS. While the pandemic posed unprecedented challenges, Company B was able to:

- Maintain operational stability.
- Pivot to new business opportunities.
- Protect its workforce and brand reputation.

The company emerged not only as a survivor of the crisis but as a model of adaptive resilience for the global apparel industry. The experience validated business continuity as a strategic function, permanently embedded into Company Bs' governance and planning structures.

Case Study: Application of Business Continuity Management System (BCMS) for Company C Facing Flood and Cyclone Risks

(Note: Case study illustrates how resilience can be embedded into the culture of hotel business operations. A well-structured Business Continuity Management System (BCMS) enables an organization to respond effectively to disruptions and maintain continuity of critical functions. One of the key lessons from this case is the importance of clear and timely guest coordination during emergencies. Ensuring guest safety, providing transparent communication, and maintaining service standards, even during adverse events, played a vital role in minimizing panic and preserving trust. Post-incident reviews conducted by the hotel revealed the need to regularly update mitigation measures, response strategies, and operational protocols to match evolving risks. These efforts not only supported operational recovery but also contributed to strengthening the hotel's reputation as a safe and dependable destination. The case underscores the importance of proactive preparedness, guest engagement, and reputation management as integral parts of building long-term resilience into business planning.

Company C, in this case study, is a **fictional hotel***, created to illustrate how a tourism business might implement a BCMS in response to flood and cyclone risks. It does not refer to a real hotel, but it is modeled to reflect the realistic conditions and practices of mid-sized resorts located in tropical, hazard-prone coastal areas, such as those found in Sri Lanka.)*

1. Context of the Company C

Company C, a mid-sized luxury resort on the eastern coast of the island, is a prominent player in the region's tourism industry. The hotel is situated in a highly hazard-prone area, exposed to the dual threats of seasonal flooding and cyclones. Recognizing that natural disasters could severely disrupt operations, harm guests and employees, and damage its reputation, the hotel leadership adopted a Business Continuity Management System (BCMS). This system aimed to build preparedness, reduce risks, enable effective response, and support fast recovery to ensure the continued viability of the hotel even in the face of repeated disasters.

2. Risk Environment and Background

The hotel's location in a coastal lowland region renders it vulnerable to frequent and intense monsoon floods, often accompanied by high winds due to tropical cyclones. During the cyclone season, which typically spans from November to February, the hotel experiences increased threats, including wind damage, power outages, road blockages, and storm surge-related flooding. These threats pose serious risks not only to physical infrastructure and business operations but also to guest safety and employee welfare. Furthermore, the increasing unpredictability of climate patterns has intensified the likelihood of such events occurring more frequently, with greater severity.

3. Implementation of the BCMS Framework

The BCMS framework at Company C was built upon the ISO 22301:2019 standard for societal security and business continuity. The first step involved a thorough business impact analysis (BIA), through which the hotel identified its mission-critical functions:

- Guest safety and accommodation
- Food and beverage service
- Sanitation
- Communications
- Reservation systems

The BIA helped quantify potential impacts under various disaster scenarios, justifying investment in continuity planning.

Risk assessments revealed that

- The hotel's basement housed electrical and HVAC (Heating, Ventilation, and Air Conditioning) systems vulnerable to flooding.
- Rooftop structures were not designed to withstand sustained high winds.
- There were inadequate measures for emergency evacuation during nighttime.

These findings informed the development of targeted mitigation strategies, such as

- Relocation of critical equipment
- Reinforcement of structural components
- Revision of the emergency evacuation plan

4. Mitigation, Preparedness, and Response Strategies

- Flood barriers and permanent stormwater pumps were installed to protect infrastructure.
- Reinforced glazing and bracing systems were added to protect windows and balconies.
- The hotel invested in two diesel generators with automated switching systems to maintain the electricity supply during grid failure.
- Emergency lighting systems were upgraded to ensure visibility throughout the hotel during power outages.

Staff training played a central role in preparedness, ensuring that both the staff and guests were aware of the emergency procedures.

- A core response team was established, with members trained in first aid, fire safety, and emergency evacuation.
- Regular mock drills were conducted.
- Emergency contact lists were maintained and updated.
- The hotel also introduced a guest information card, provided during check-in, with safety instructions in multiple languages.

5. Recovery Planning and Post-Disaster Strategies

The recovery phase of the BCMS included specific measures to restore hotel operations in the shortest possible time.

- An off-site data backup system was maintained to allow remote restoration of the reservation and billing systems.
- The hotel developed agreements with nearby service providers, including transport and alternative accommodation options, to relocate guests if necessary.
- A recovery task force was responsible for post-disaster damage assessment, prioritization of repairs, insurance claims, and media communication.

Following each major event, post-incident reviews were conducted. After the cyclone 'Buravi' in 2020, which led to minor flooding in the garden villas, the review process led to further elevation of outdoor power sockets and restructuring of landscape drainage to divert water more efficiently.

6. Regulatory Compliance and Alignment with National Policy

The hotel's BCMS was aligned with national disaster risk reduction (DRR) policies and building codes issued by the country's Urban Development Authority and Tourism Development Authority. Company C ensured compliance with flood zoning regulations and cyclone-resistant building guidelines. The hotel's contingency plans were submitted to the District Disaster Management Centre, which facilitated coordination during actual events.

Furthermore, the hotel adhered to occupational health and safety standards, maintained legally required insurance coverage for business interruption and property loss, and incorporated pandemic contingency measures in light of the COVID-19 experience.

7. Community Engagement and External Coordination

The hotel recognized the importance of external partnerships in ensuring continuity. It established communication channels with the local police, fire brigade, and regional disaster response unit. Staff members participated in district-level disaster preparedness programs and workshops. During disasters, the hotel provided temporary shelter and meals to displaced local residents, enhancing its social license to operate and building goodwill.

In addition, the hotel invested in early warning systems, integrating national meteorological alerts with its internal communication system to ensure prompt responses. Staff were trained to act on these alerts, initiating staged responses based on the severity of the threat.

8. Challenges and Recommendations for Improvement

Despite its achievements, Company C identified several areas for continuous improvement.

a) Communication failures due to mobile network outages during cyclones highlighted the need for satellite phones or shortwave radios.

b) Gaps in training among new recruits due to high staff turnover emphasized the importance of integrating BCMS modules into onboarding programs.

c) The hotel also recognized the need for more robust water storage systems, as municipal supply is often disrupted after major floods.

d) It was recommended that the hotel upgrade its IT disaster recovery systems, including the use of cloud-based platforms for better resilience.

e) Future plans included investing in rooftop solar systems with battery storage, both as a green initiative and to enhance energy independence.

f) It was also advised to conduct third-party audits of the BCMS annually to ensure ongoing compliance and continuous improvement.

9. Conclusion and Reflections

The Company C case illustrates how a tourism enterprise operating in a high-risk coastal environment can use a Business Continuity Management System to safeguard operations, protect lives, and maintain customer trust during natural disasters. By integrating risk reduction, emergency response, recovery, and continuous improvement processes, the hotel not only minimized the impact of flooding and cyclones but also enhanced its competitive edge in a sector where reliability and guest confidence are paramount.

This experience underscores the importance of embedding resilience into the core of business strategy, particularly in sectors directly affected by climate variability. The BCMS at Company C evolved from a compliance-driven exercise into a culture of preparedness and adaptability. It now serves as a model for other tourism establishments in hazard-prone regions aiming to ensure business continuity and sustainable growth in an era of increasing environmental uncertainty.

Case Study: Company D, Embedding Resilience through ISO 22301, Certified BCMS

(Note: Recognizing the growing risks posed by digital transformation, cyber threats, and natural or human-induced disruptions, Company D (The identity of the organization has been withheld for reasons of confidentiality. In this publication, it is referred to as 'Company D') undertook a major resilience initiative culminating in its certification to ISO 22301:2019 in December 2023. This case study examines the structure and implementation of Company D's Business Continuity Management System (BCMS), explores how the bank aligned with regulatory requirements, identifies key risks and corresponding recovery strategies, and highlights best practices and lessons learned.)

1. Organizational Context

Company D is one of Sri Lanka's prominent licensed commercial banks, playing a pivotal role in the country's financial services landscape. Initially established as a development finance institution in 1979, Company D transitioned into full commercial banking operations in 2005. With a wide branch network and a growing digital banking portfolio, Company D serves a diverse clientele, including retail, corporate, and SME segments.

Operating in a highly regulated and technology-driven environment, Company D faces evolving challenges such as cyber threats, increasing customer demand for uninterrupted digital services, regulatory compliance pressures, and exposure to climate-related and socio-political risks. As a systemically important bank, maintaining operational resilience and public confidence is vital. This context underscored the need for a robust Business Continuity Management System (BCMS) aligned with international standards and local regulatory expectations.

2. Regulatory Framework and Compliance Requirements

Company D's BCMS was developed in accordance with the directives issued by the Central Bank of Sri Lanka, notably Direction No. 01 of 2021, which outlines guidelines for IT Risk Resilience and Cybersecurity. This regulation mandates financial institutions to establish comprehensive Business Continuity Plans, Disaster Recovery procedures, and to conduct regular testing of these systems.

To strengthen its resilience framework, Company D adopted international best practices, most notably through alignment with ISO 22301:2019 for Business Continuity Management Systems and ISO 27001 for Information Security Management. Additionally, principles recommended by the Basel Committee were integrated to support operational resilience. The ISO certification not only enhanced internal standards but also served to bolster regulatory confidence and market credibility.

3. Leadership and teams

Strategic direction and accountability for the BCMS were maintained through top-level leadership, with the Board and senior management providing oversight. This alignment between operational resilience and corporate governance ensured that business continuity objectives were interwoven with organizational strategy.

A dedicated Crisis Management Team (CMT) was formed to oversee response actions during emergencies. The team functioned within a clear escalation hierarchy and was supported by structured internal and external communication protocols. Crisis simulations and playbooks ensured the team was prepared for rapid and coordinated action.

4. Business Impact Analysis (BIA)

Company D undertook a comprehensive Business Impact Analysis (BIA) to assess the criticality of its core operations. Each function was examined for its potential financial and reputational impact in the event of a disruption. To support this process, the bank employed business impact mapping to identify interdependencies among key services. Critical operations, such as real-time payment systems, ATM services, internet banking, and treasury functions, were analyzed in terms of both upstream and downstream dependencies. This holistic evaluation enabled the bank to set clear recovery priorities, with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) tailored to customer expectations, regulatory requirements, and operational realities. As a result, Company D ensured that services with the greatest impact on customer experience and financial stability were restored with minimal delay.

5. Recovery Time and Point Objectives (RTO/RPO)

Using insights from its BIA, Company D set recovery objectives to ensure minimal service disruption. The core banking platform had a target RTO of two hours, while ATM and online services were expected to be restored within four hours. The RPO for all critical systems was defined to limit data loss to a maximum of thirty minutes, supported by near real-time replication.

6. Risk Assessment

Company D adopted a comprehensive approach to risk identification, encompassing a wide spectrum of potential disruption scenarios. Cybersecurity threats, including phishing attacks, ransomware, and unauthorized system access, were prioritized due to their prevalence and their capacity to compromise customer-facing services. Infrastructure-related risks, such as data center outages and server failures, were also identified as critical vulnerabilities. The bank extended its assessment to environmental threats like urban flooding and earthquakes, alongside socio-political risks such as strikes and civil unrest. Emerging risks, including third-party service disruptions and health-related crises like epidemics, were also factored into the scenario planning. By systematically evaluating the likelihood and impact of each risk, Company D was able to develop a focused and adaptive business continuity planning framework.

7. Continuity Strategies

To ensure the uninterrupted delivery of essential services, Company D implemented multiple continuity strategies.

a) To mitigate the risk of prolonged IT outages, Company D established a secondary Disaster Recovery (DR) site, geographically separate from the primary data center. This facility mirrored the production environment and was equipped for real-time data replication. Automated failover mechanisms allowed seamless transition in the event of disruptions. Redundant communication networks supported this infrastructure, ensuring uninterrupted connectivity.

b) To prepare for physical access restrictions or facility damage, the bank identified alternate operational sites and equipped them with secure IT infrastructure. Employees in key roles were issued remote access credentials and mobile workstations. Secure access via Virtual Private Networks (VPNs) and dual-authentication protocols safeguards data integrity during remote operations.

c) In cases where technology could not be immediately restored, the bank relied on manual processing techniques. Frontline staff were trained in paper-based transaction procedures, and temporary ledger entries were digitized at the earliest opportunity. These manual workarounds maintained business continuity during system outages without compromising operational integrity.

d) The BCMS incorporated a structured communication plan to ensure accurate and timely dissemination of information during incidents. Automated alerts were used to notify internal teams, while external stakeholders, including regulators, clients, and the media, were engaged through approved communication channels. The use of pre-drafted media statements and designated spokespersons maintained consistency in public messaging.

e) To manage continuity risks from third-party service providers, Company D embedded resilience clauses into its Service Level Agreements. Critical vendors were required to maintain tested continuity plans, and the bank conducted periodic joint exercises to validate integration between its own BCMS and those of its partners.

f) The bank maintained daily encrypted backups of its core data, stored off-site and subjected to routine integrity checks. These backups included version-controlled archives to facilitate precise data restoration. Compliance with internal security protocols and external regulatory guidelines ensured legal and operational safeguards.

8. Testing, Training, and Awareness

The bank institutionalized regular testing of its BCMS through full-scale simulations and scenario-based tabletop exercises. Staff training programs were tailored to operational roles, ensuring readiness across all departments. A culture of continual improvement was nurtured through internal audits and post-exercise evaluations, allowing iterative refinement of the continuity framework.

9. Conclusion

Through the implementation of its BCMS and successful ISO 22301 certification, Company D strengthened its resilience framework and gained industry-wide recognition. The initiative enhanced both customer and regulatory trust. Internally, staff demonstrated improved role clarity and responsiveness during crisis simulations, and operational disruptions were managed with confidence and efficiency.

Company D's structured and certified approach to business continuity stands as a model of resilience for financial institutions operating in emerging economies. The use of layered recovery strategies, spanning from automated IT disaster recovery to manual fallback systems, underscores the comprehensiveness of its BCMS.

Case Study: Sustaining the Catch: How Company E Thrived Through Business Continuity Planning

(Note: The Company E (The identity of the organization has been withheld for reasons of confidentiality. In this publication, it is referred to as 'Company E') case illustrates how the Business Continuity Management System (BCMS) can be adapted to the complexities of the fisheries value chain connecting upstream actors such as fishing communities with downstream stakeholders in the EU and global markets. The real-life test during the national fuel crisis and the subsequent post-incident review demonstrate how critical operations can continue even during major disruptions. It also emphasizes the importance of upgrading the BCMS, enhancing the continuity through extended or cascading crises. This case highlights the vital importance of proactive preparedness and resilience in ensuring business continuity and long-term sustainability.)

1. Context of the Company E

Company E is a medium-scale seafood processing and export company located in Negombo, Sri Lanka. Specializing in fresh and frozen tuna, shrimp, and cuttlefish, the company supplies premium products to clients in Europe and East Asia. With over 150 employees and a daily processing capacity of 10 metric tons, Company E plays a vital role in the regional fisheries value chain.

2. BCMS Objective

Before adopting BCMS in 2021, Company E had faced multiple disruptions over the years that exposed its operational vulnerabilities.

- The COVID-19 pandemic, from 2020 to 2022, led to extended border closures, halting seafood exports, and interrupting raw fish procurement.
- The MV X-Press Pearl Maritime Disaster in 2021 banned fishing along Panadura to Negombo, leaving processors lacking raw materials, export markets raising contamination concerns.
- Frequent power outages also pose a risk to cold storage facilities, potentially leading to product spoilage and financial loss.
- Additionally, the company had suffered a major export setback when a shipment was rejected due to non-compliant documentation, which significantly affected its reputation.

These incidents highlighted the company's vulnerability to operational, environmental, and regulatory risks, prompting management to acknowledge that reactive crisis handling was no longer adequate. To ensure the continuity of critical business functions and to adhere to international compliance requirements, the company recognized the need for a structured and proactive resilience framework. As a strategic response, Company E committed to establishing a company-wide Business Continuity Management System (BCMS) aligned with ISO 22301, aiming to,

1. Safeguard its operations
2. Protect customer trust
3. Strengthen long-term sustainability

3. Business Impact Analysis (BIA)

As the first step of BCMS establishment, Company E conducted a comprehensive Business Impact Analysis (BIA). This involved mapping the organization's core processes, identifying critical dependencies, and assessing the consequences of potential disruptions. Key departments such as cold storage operations, fish procurement, quality control, export logistics, and documentation were evaluated.

The BIA revealed that,

- Cold storage was the most time-sensitive function, where any downtime beyond two hours could lead to irreversible losses due to spoilage.
- Export documentation was also classified as highly critical, with errors or delays having severe implications for compliance and customer satisfaction.
- Procurement and transport were likewise identified as time-sensitive areas given their dependence on external suppliers and national infrastructure.

Each function was assigned recovery time objectives (RTO) guiding the prioritization of continuity strategies.

Business Function	**Impact if Disrupted**	**RTO**
Cold storage operations	High (spoilage, export loss)	2 hours
Export documentation	Medium-High (non-compliance)	4 hours
Fish procurement	High (no raw material)	8 hours
Quality assurance (lab)	Medium (product recall risk)	12 hours

The insights from the BIA enabled Company E to understand which business functions required immediate restoration following a disruption and helped allocate appropriate resources for risk mitigation.

4. Risk Assessment

Following the BIA, a detailed risk assessment was undertaken to identify, evaluate, and prioritize threats that could impact the business. Risks were categorized into operational, environmental, technological, regulatory, and reputational domains. Each risk was rated based on likelihood and potential impact.

Risk Type	Specific Threat	Likelihood	Impact	Risk Rating
Power outages	National grid failures	High	High	Critical
Extream weather	Affecting fishing and logistics	High	High	Critical
Rejected exports	Due to poor traceability	Medium	High	High
Pandemic	Labor and logistics disruptions	Low-Medium	High	High
Fire in cold rooms	Electrical faults	Low	Very High	High

Some of the most critical risks identified included power failures, fuel shortages, export rejection, and fire hazards within cold rooms. The possibility of a future pandemic or public health emergency was also considered. Of particular concern was the company's dependency on a limited number of suppliers and its single-location storage infrastructure.

5. Mitigation and Response Measures

In response, Company E adopted a structured risk treatment strategy.

a) Power and Utility Continuity:

- 200 kVA diesel generator (Standby) for processing and cold storage continuity with emergency fuel reserves.
- Solar PV installation to reduce dependency on the national grid.
- Real-time monitoring system for temperature control with SMS alerts.

b) Transport and logistics operations:

- Strengthened the logistics operations through partnerships with multiple shipping agents, reducing reliance on a single provider.

c) Supply Chain Resilience:

- Signed MOUs with alternative fishing cooperatives from multiple regions (e.g., Kalpitiya, Trincomalee), ensuring a broader sourcing base.
- Implemented a rotating buffer inventory of key inputs (ice, packaging, brine).
- Periodic supplier audits for quality and continuity assurance.

d) Minimum workforce:

- Training of staff for cross-skills, enabling flexibility in relocating personnel across critical functions.
- Longer working shifts for essential staff members with onsite accommodation arrangements during restricted mobility.

e) Document Control and Compliance:

- Migrated all traceability data and export records to a cloud-based ERP system.
- Introduced dual verification of export documentation to reduce errors.
- Set up a compliance calendar with reminders for EU and FDA-related requirements.

Additional infrastructure improvements were introduced, such as fire detection systems and enhanced cold storage insulation. Company E also revised its insurance portfolio, obtaining comprehensive business interruption and marine cargo coverage, and engaging external auditors to assess regulatory compliance and test the effectiveness of the continuity plan.

6. Teams, Testing, and Training

A Business Continuity Officer was appointed, and a formal Crisis Management Teams (CMT) were formed with defined roles for operations, logistics, finance, communications, and compliance. These teams conducted bi-annual drills, including mock responses to container rejection, extended power failure, and disease outbreaks. External consultants were hired for annual reviews and audits of the BCMS system. BCMS reviews were incorporated into monthly management meetings. Staff training became a core feature of the BCMS, with new recruits receiving BCMS orientation and monthly awareness sessions held for all employees.

7. True Test to Ensure the Functionality of BCP

The national fuel crisis in mid-2022 served as the true test of Company E's BCMS. With widespread fuel shortages, many fishing boats remained docked for extended periods, severely disrupting the supply of raw material. As a result, most seafood processing facilities were forced to suspend operations due to the unavailability of inputs and logistical challenges. Company E also faced challenges in maintaining timely deliveries and the daily commuting of staff.

Despite these constraints, Company E was able to sustain its operations by activating BCMS response strategies. The key measures included,

- Ensuring the continuity of processing and cold storage through alternative power sources, such as diesel generators and solar backup systems.
- Prior arrangements with fishing cooperatives in multiple coastal regions also proved effective, enabling it to continue sourcing raw materials even as local supplies dried up.
- Implemented its minimum workforce strategy by deploying cross-trained employees and offering accommodation to essential staff, thereby maintaining critical functions with limited personnel.

However, there were unexpected delays in transport due to limited availability of fuel and the company's restricted reserves. To address urgent commitments, the company airlifted a limited volume of high-value exports to Europe through courier logistics.

Effective communication with overseas buyers during this period reinforced customer confidence. While competitors failed to meet contractual obligations, Company E honored all its orders and even gained new clients who appreciated its reliability and professionalism under pressure.

The post-incident review highlighted key successes, including

- Continuity of Critical Operations: Use of diesel generators and solar power ensured uninterrupted cold storage and processing.
- Raw Material Sourcing: Diversified procurement arrangements with fishing cooperatives in other regions helped maintain input flow.
- Workforce Adaptation: A minimum workforce strategy using cross-trained staff and on-site accommodation allowed essential operations to continue.
- Logistics Innovation: Limited high-value consignments were airlifted to fulfill urgent export obligations.
- Stakeholder Communication: Transparent, proactive communication with buyers retained trust and led to new client acquisition.

Despite the overall success, the crisis exposed several vulnerabilities:

- Fuel Reserve Limitations: The company's internal fuel reserves were inadequate for a prolonged disruption.
- Transport Dependencies: Heavy reliance on local logistics providers without fuel contingency arrangements led to delays.
- BCMS Scalability: Existing response plans were stretched under prolonged crisis conditions, showing the need for enhanced scalability to handle longer or bigger disruptions.
- Supplier Risk Management: No structured risk assessment existed for tier-2 or tertiary suppliers (secondary or smaller suppliers) impacted by fuel shortages.

For improving the BCMS, it is recommended to,

A. Enhance Fuel Contingency Planning:

- Establish minimum critical fuel reserve thresholds for essential operations.
- Formalize supply agreements with fuel providers for priority access during national emergencies.

B. Diversify Logistics Options:

- Create MOUs with multiple logistics partners, including those with alternative fuel fleets.
- Develop emergency routing plans and decentralized dispatch points to reduce reliance on a single location.

C. Expand Supplier Risk Assessment:

- Conduct a tiered risk analysis of the supply chain and integrate risk scoring into procurement strategy.
- Establish business continuity requirements for key suppliers, especially those in transportation and raw material sourcing.

D. Strengthen Workforce Continuity Measures:

- Invest in staff housing options or transport pooling mechanisms during disruptions.
- Create a roster of cross-functional emergency teams with periodic drills.

E. BCMS Review and Scalability Testing:

- Revise existing BCP scenarios to include multi-week disruptions and cascading failures.
- Conduct simulation exercises with extended time horizons to test adaptability and scalability.

F. Stakeholder Communication Protocols:

- Develop standardized templates and channels for crisis communication with buyers, staff, and regulators.
- Implement a real-time crisis dashboard to support decision-making and external updates.

8. Results and Outcomes

The implementation of the BCMS significantly improved Company E's resilience and market performance. In the 36 months following the system's adoption, the company experienced zero shipment rejections and uninterrupted export operations, even during national crises. Insurance premiums were reduced due to lower assessed risk, and two new buyers from Germany and Japan added Company E to their preferred supplier list.

Internally, employee awareness and confidence improved, and supplier relations strengthened. The company's ability to manage risk transparently enhanced its standing with regulators and certification bodies.

9. Conclusion

The Company E Fisheries case demonstrates that a well-structured Business Continuity Management System, grounded in accurate risk assessment and thorough business impact analysis, can provide the resilience necessary to survive and thrive in an uncertain environment. By investing in infrastructure, diversifying supply chains, digitizing compliance, and training people, Company E not only overcame disruptions but positioned itself as a leader in Sri Lanka's fisheries export industry. This case affirms that BCMS is not merely a compliance tool; it is a strategic asset that safeguards the future of the business.