

Enhancement of Private Sector Capacities  
On Disaster Risk Reduction and Management

# BUSINESS CONTINUITY MANAGEMENT (BCM) SYSTEM

## ISO 22301:2019

### Handbook for Training of Trainers



## **MESSAGE FROM THE 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 Programme, 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 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 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 CEYLON CHAMBER OF COMMERCE

The Ceylon Chamber of Commerce is proud to lead the development of the Business Continuity Management System (BCMS) Handbook and Curriculum, funded by the World Food Programme (WFP) and supported by the 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 Programme 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

TABLE OF CONTENTS .....	I
EXECUTIVE SUMMARY .....	VI
HOW TO USE THIS BCMS HANDBOOK.....	VII
GLOSSARY.....	VIII
BCMS VOCABULARY .....	X
1. INTRODUCTION.....	15
1.1. BCMS IN DISASTER MANAGEMENT SYSTEM IN SRI LANKA.....	16
1.1. ENHANCING PRIVATE SECTOR RESILIENCE THROUGH BCMS.....	17
1.2. SME'S BUSINESS RESILIENCE: CHALLENGES AND GAPS.....	17
1.3. ENHANCING SME RESILIENCE THROUGH BUSINESS CONTINUITY MANAGEMENT SYSTEM.....	19
2. BUSINESS CONTINUITY MANAGEMENT SYSTEM: WHAT? AND WHY? .....	21
2.1. BENEFITS OF IMPLEMENTING BCMS.....	22
2.2. KNOW THE HISTORY OF BCMS AND ITS EVOLUTION .....	25
2.3. BCMS; SRI LANKAN CONTEXT .....	28
3. BCMS FRAMEWORK .....	30
3.1. BCMS INTERNATIONAL STANDARDS.....	30
3.2. STANDARDIZATION AND CERTIFICATION .....	34
3.3. ISO 22301 CERTIFICATION PROCESS .....	35
3.4. PROPORTIONALITY IN BCMS.....	36
3.5. RECOGNIZE THE IMPORTANCE OF BCPs IN BCMS.....	37
3.6. BCMS DEVELOPMENT PROCESS .....	40
3.7. PLAN-DO-CHECK-ACT (PDCA) CYCLE IN BCMS.....	42
4. CONTEXT OF THE ORGANIZATION.....	44
4.1. UNDERSTANDING OF THE ORGANIZATION.....	44
4.2. EXPECTATIONS OF INTERESTED PARTIES.....	44
4.3. WHAT IS THE PURPOSE OF BCMS? .....	46
4.4. SCOPE OF THE BCMS.....	47
5. LEADERSHIP AND TEAM .....	48
5.1. LEADERSHIP AND COMMITMENT .....	48
5.2. BCMS POLICY .....	49
5.3. ROLES AND RESPONSIBILITIES .....	49
5.4. BCMS TEAMS .....	50
6. BUSINESS IMPACT ANALYSIS .....	52
6.1. PRIORITIZED ACTIVITIES (PAs) AND RECOVERY TIME OBJECTIVES (RTOs).....	52
7. RISK ASSESSMENTS.....	55
7.1. IDENTIFICATION OF RISKS .....	56
7.2. ANALYSIS OF RISKS .....	57
7.3. EVALUATION OF RISKS.....	58
7.4. VULNERABILITIES OF BUSINESSES FOR PROCESS INTERRUPTIONS.....	58

7.5.	AVAILABILITY OF HAZARD AND RISK INFORMATION AND ACCESSIBILITY .....	59
8.	BUSINESS CONTINUITY STRATEGIES AND SOLUTIONS.....	61
8.1.	PROTECTION OF PRIORITIZED ACTIVITIES.....	62
8.2.	STABILIZING, CONTINUING, RESUMING, AND RECOVERING PRIORITIZED ACTIVITIES .....	62
8.3.	MITIGATING, RESPONDING TO, AND MANAGING IMPACTS .....	63
8.4.	SELECTION OF STRATEGIES AND SOLUTIONS.....	64
9.	RESOURCE REQUIREMENTS .....	65
9.1.	PEOPLE .....	65
9.2.	INFORMATION AND DATA.....	65
9.3.	BUILDINGS, WORKPLACES, AND ASSOCIATED UTILITIES .....	66
9.4.	EQUIPMENT AND CONSUMABLES.....	67
9.5.	ICT SYSTEMS .....	67
9.6.	TRANSPORTATION AND LOGISTICS.....	68
9.7.	FINANCE.....	68
9.8.	PARTNERS AND SUPPLY CHAIN.....	69
10.	CONDUCT EXERCISES TO ENSURE THE FUNCTIONALITY OF THE BCMS .....	71
10.1.	MAINTENANCE ASPECTS OF BCMS.....	72
	REFERENCES.....	73

## 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
<b>Human</b>	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.
<b>Physical</b>	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.
<b>Financial</b>	If disasters are particularly devastating, large companies may	Small businesses do not usually have amounts of capital to pay for

have additional capital for restoring business operations. Insurance may also cover the losses financing resumption of business activities.

personal or business expenses resulting in obtaining external financing for operations, which may lead to future cash outflows. Small companies are reluctant 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.

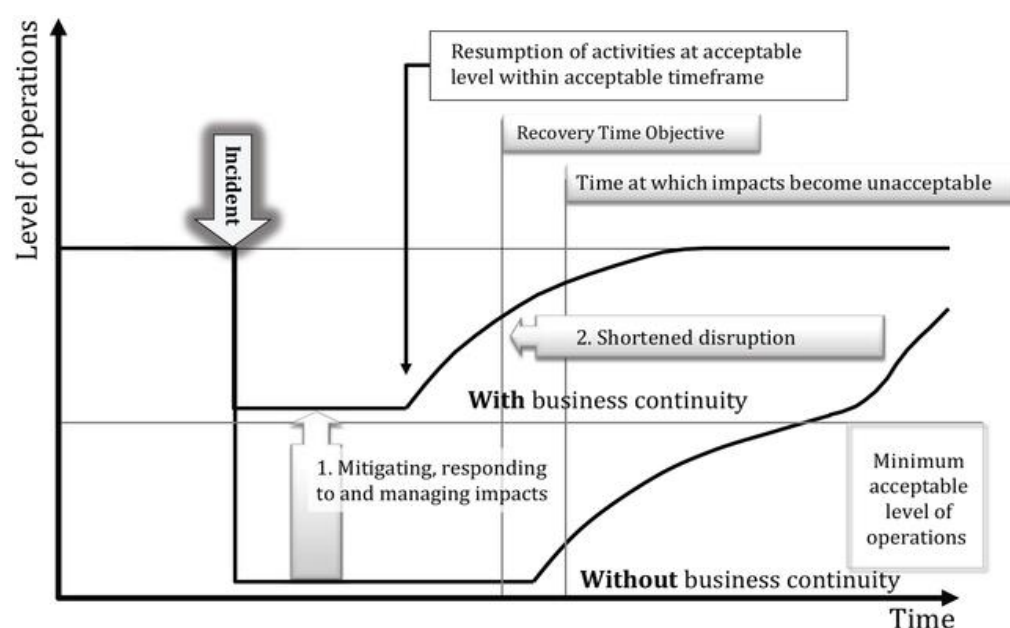


Figure 1 Illustration of business continuity being effective for sudden disruption



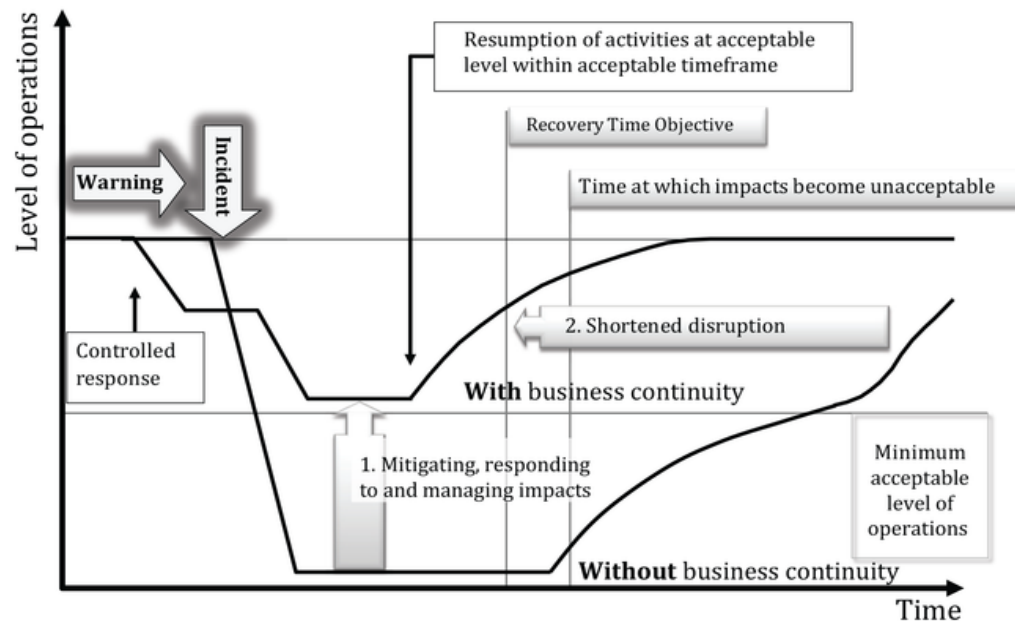


Figure 2 Illustration of business continuity being effective for gradual disruption

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

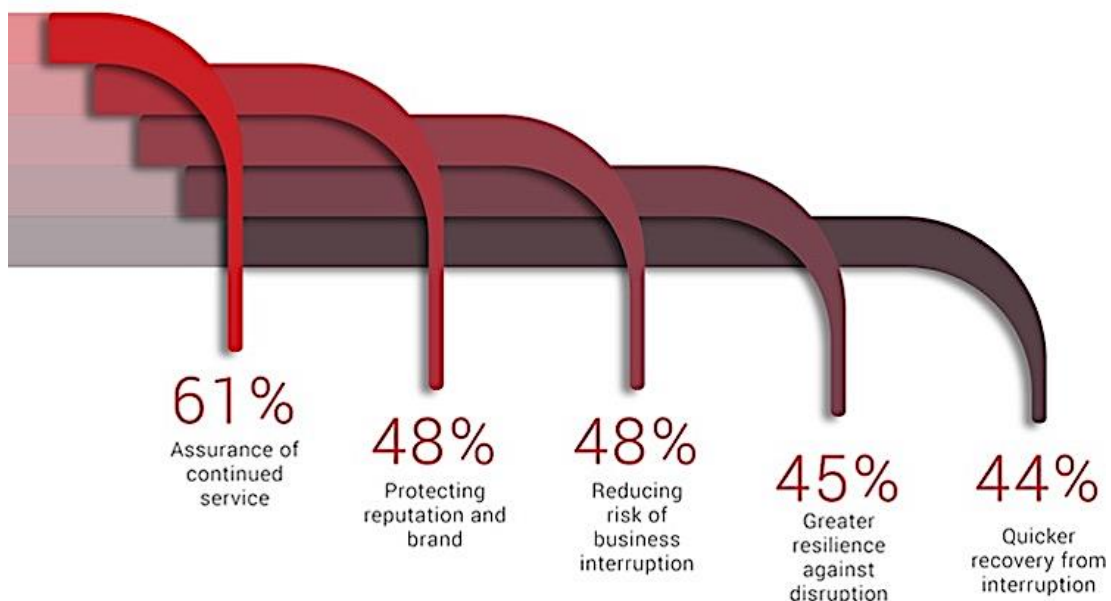


Figure 3 : Top reasons why BCMS is a necessity

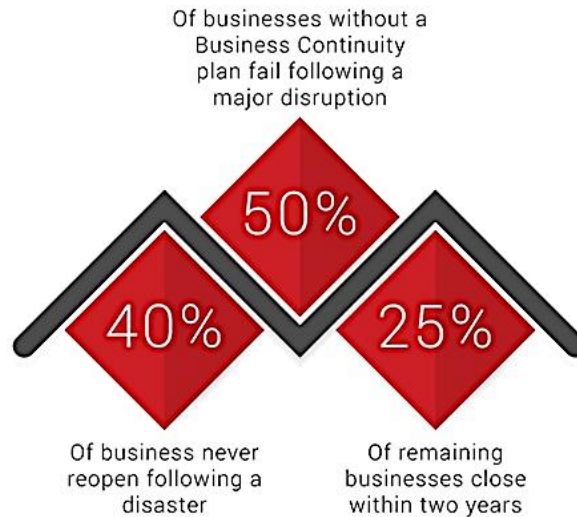


Figure 4 Consequences of not having BCMS

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.

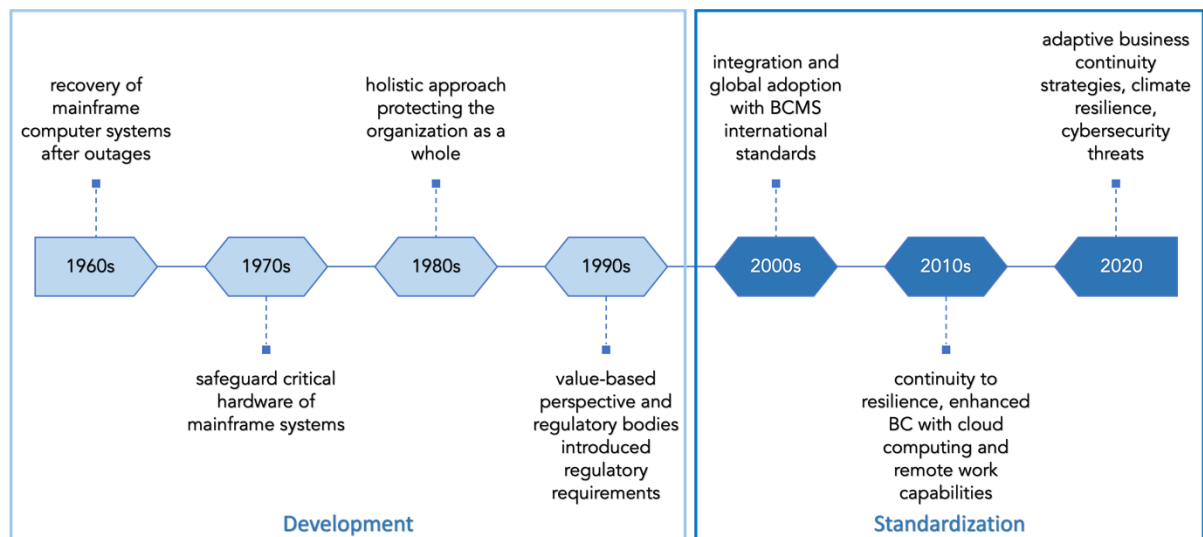


Figure 5 Illustration of Evolution of BCMS

### 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.

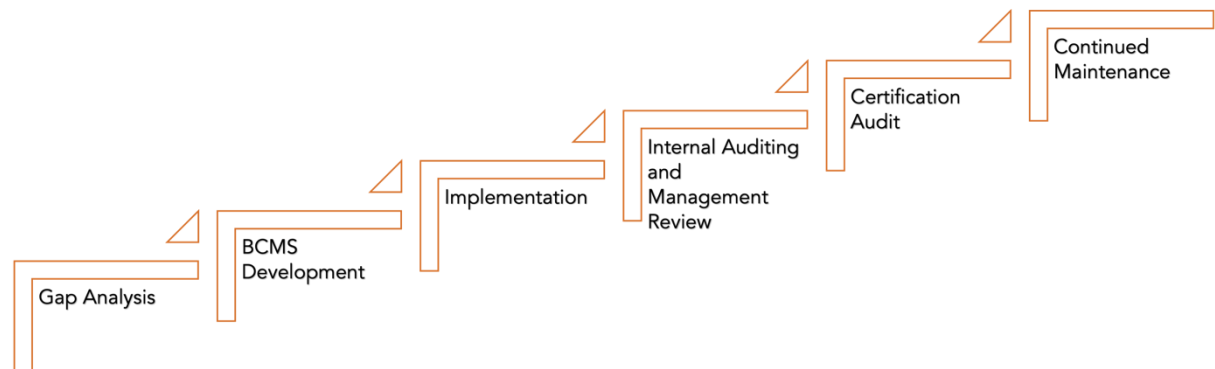


Figure 6 Certification Process

#### 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.

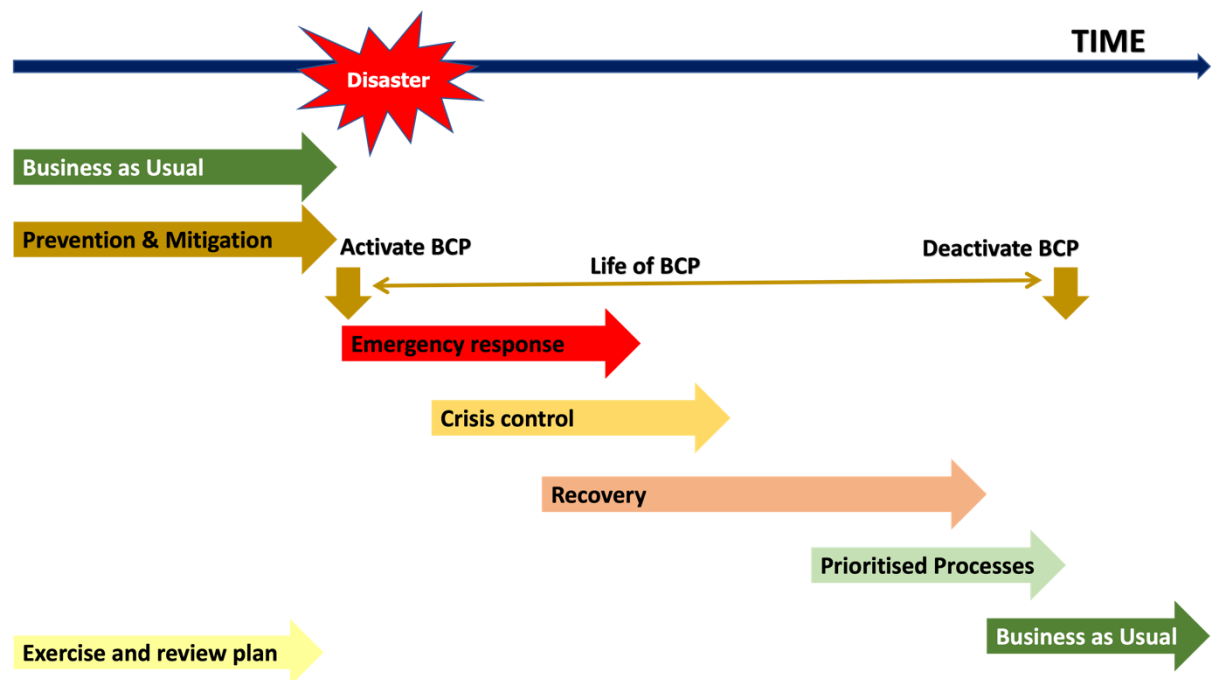
Key Elements of BCP:

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.

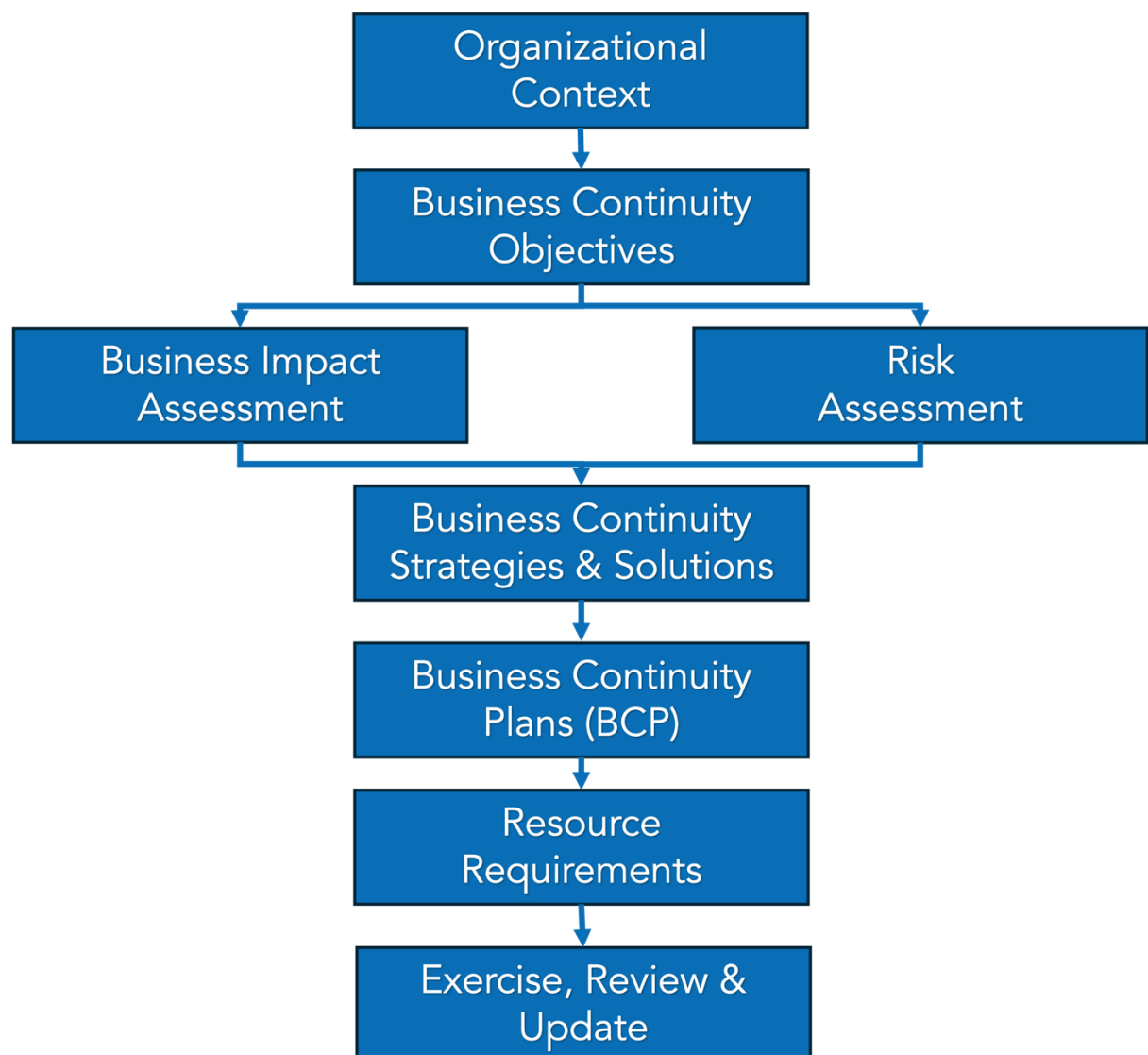


Figure 7 BCMS Development Process

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

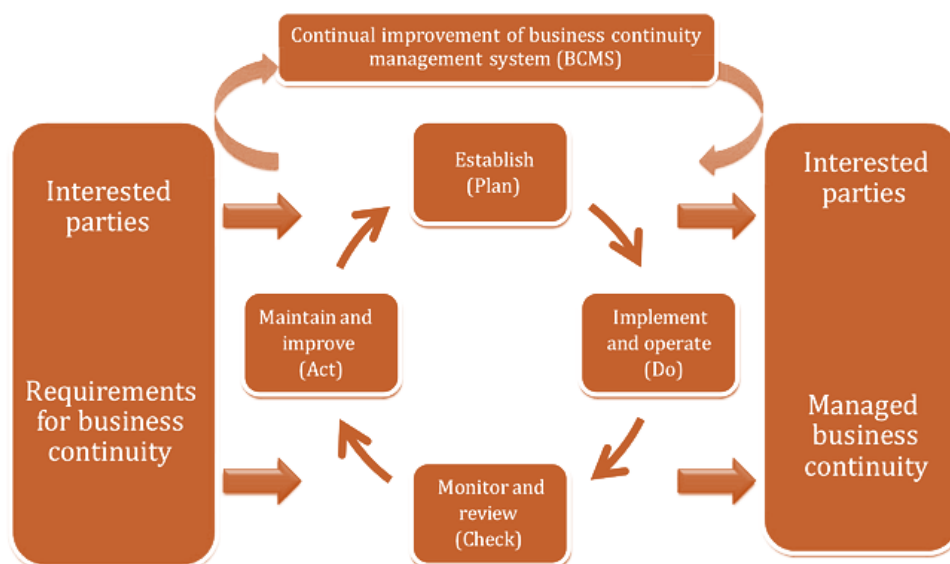


Figure 8 PDCA cycle applied to BCMS processes

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

<b>Plan</b> (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.
<b>Do</b> (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
<b>Check</b> (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.
<b>Act</b> (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.

## Interested Parties



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
Top 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.

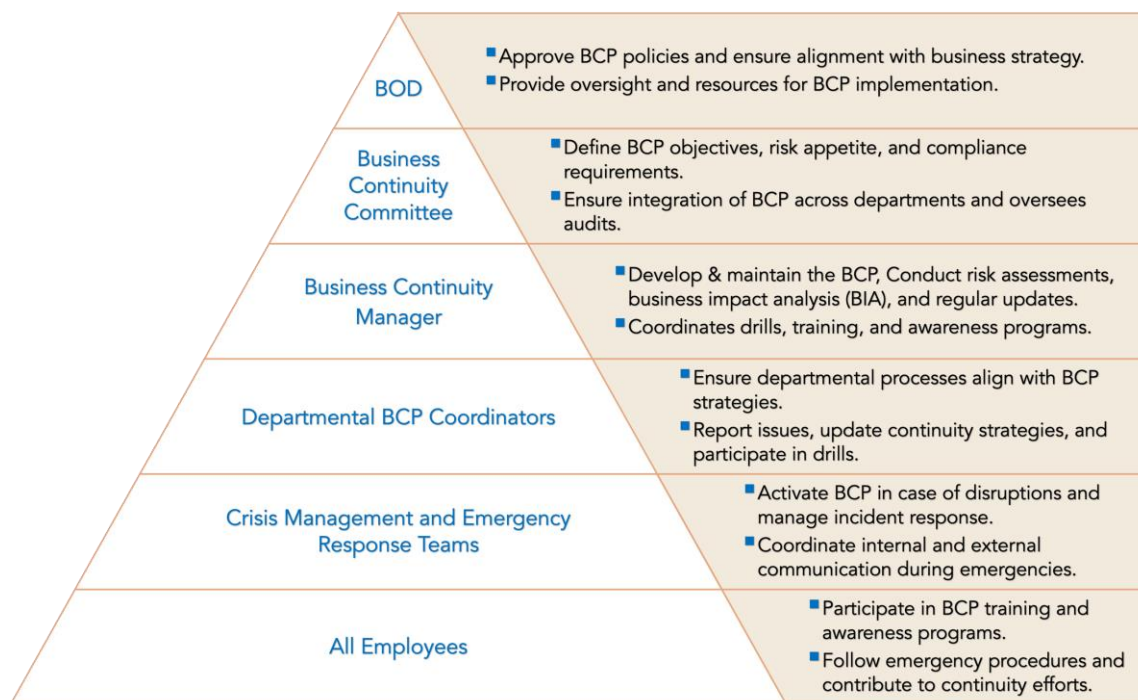


Figure 10 Roles and Responsibilities

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.

#### 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:

- 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.
- 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.

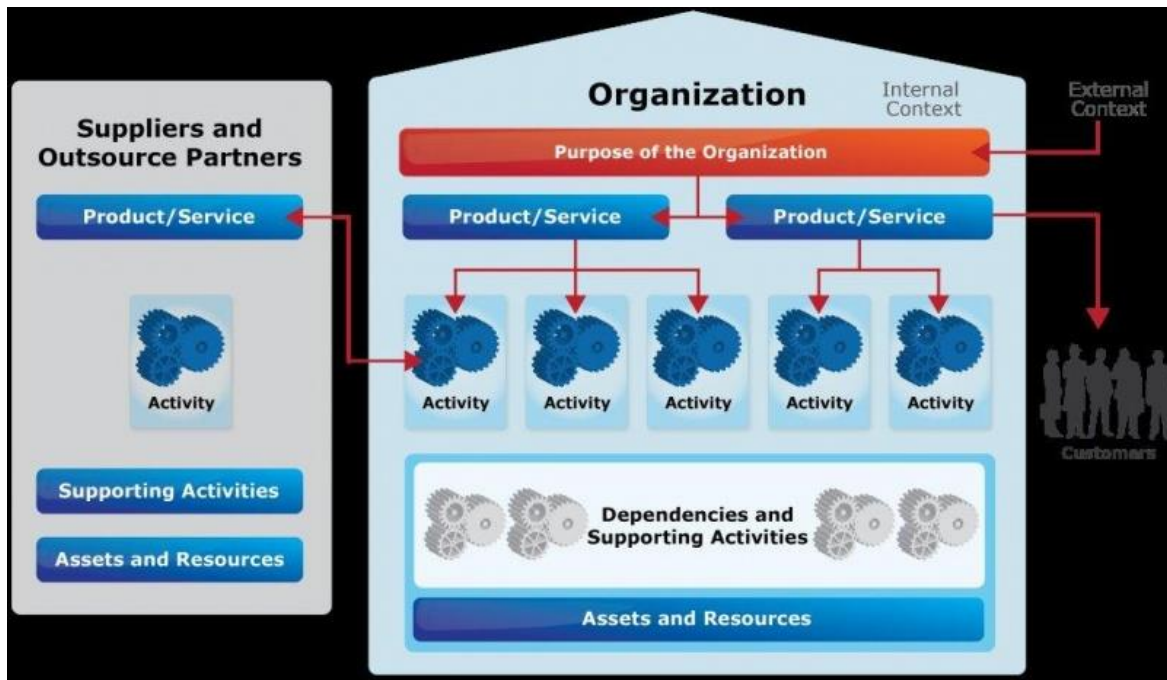


Figure 11 Understanding the Organization

<https://BCMSpedia.org/w/index.php?title=Organization>

The type of impacts can include,

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*

<b>Process /activity</b>	<b>Impacts</b>	<b>MTPD</b>	<b>RTO</b>
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
<b>Definition</b>	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
<b>Origin</b>	Internal	External	Internal	External
<b>Control</b>	Within the organization's direct control	Limited control; can manage impact.	Within the organization's control.	No control over occurrence or source.
<b>Control level</b>	High (can mitigate or eliminate)	Limited (can influence the impact)	High (can take proactive actions)	None (can only prepare or adapt)
<b>Scope</b>	Specific and immediate to the business.	Ripple effect from external factors	Arises from within the organization	Broad external factors
<b>Preventability</b>	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.

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. BUSINESS CONTINUITY STRATEGIES AND SOLUTIONS



*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

<b>Monetary Incentives</b>	<b>Description</b>
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.

## 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>