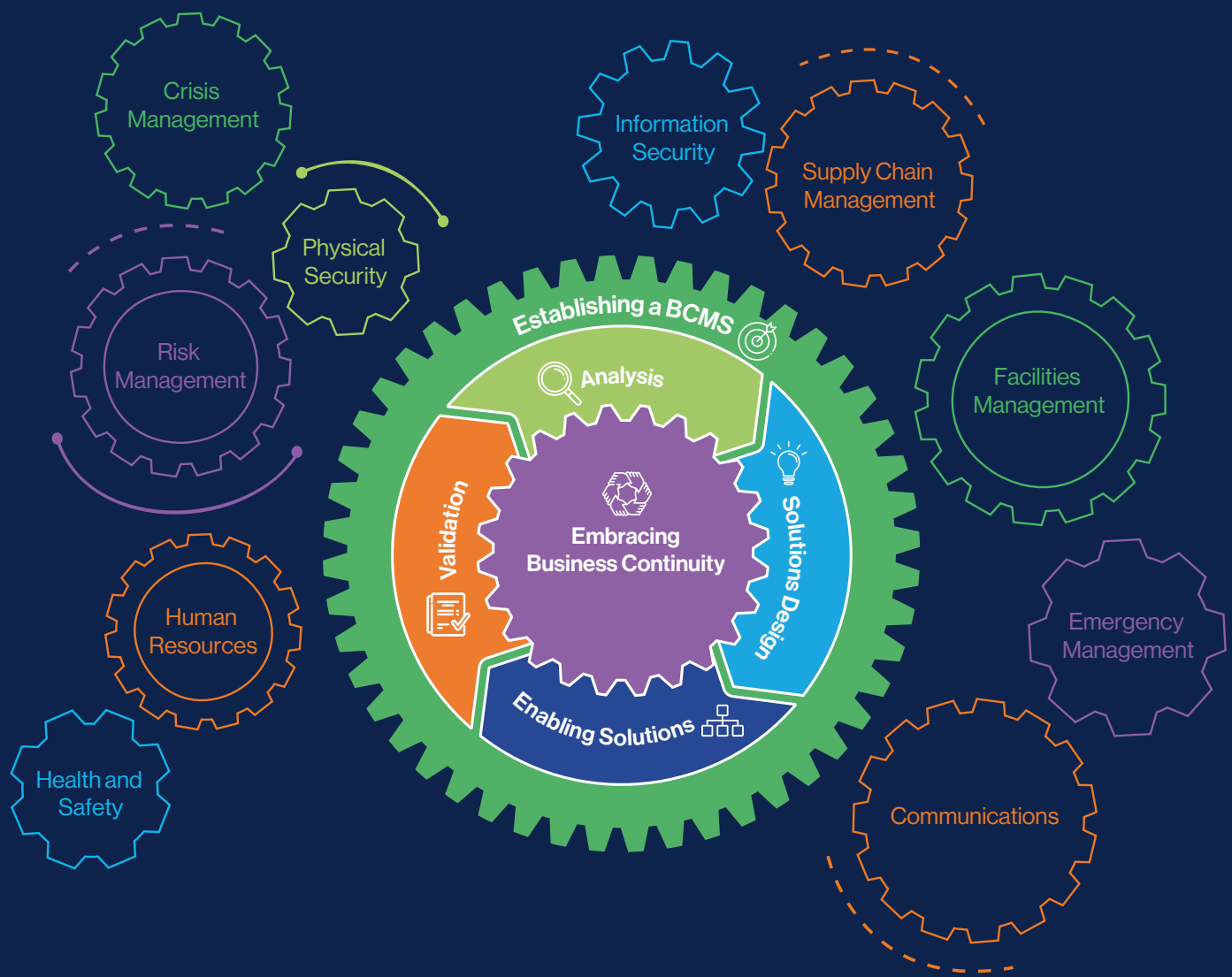
bci Leading the way to resilience

Edition 7.0

Good Practice Guidelines

The global guide to good practice in business continuity



Business Continuity Management Systems (BCMS)

ISBN: 978-1-3999-5059-6

British Library

This publication has been legally deposited with the British Library.

BCI, 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, U.K.

bci@thebci.org

www.thebci.org

Contents

Introduction to the BCI's Good Practice Guidelines Edition 7.0

Welcome to the comprehensive guide to good practice in the field of Business Continuity (BC).

The Good Practice Guidelines are written by and for BC professionals and are your go-to guide for establishing, implementing, maintaining, and continually improving a comprehensive business continuity management system (BCMS).

In recent years the business continuity management (BCM) profession has continued to evolve and its value is recognised by a wider global audience.

The acknowledgement of the importance of BC is due to the growing number of disruptive events, which include but are not limited to:

- Global financial crises,
- Severe weather events,
- Geopolitical instability,
- Supply chain disruptions,
- The outbreak of large-scale infectious diseases,
- Cyber attacks and data breaches, and
- Terrorist incidents.

While organizations must continuously adapt to the challenges deriving from such complex events, they also need to address the increased dependence on information technology and connectivity that is changing business as usual (BAU) processes.

In such demanding environments, the Good Practice Guidelines (GPG) provides professionals with six professional practices that help limit the adverse impacts of complex challenges. The growing demand for global guidance in BC is demonstrated by the adoption and broad acceptance of the International Organization for Standardization (ISO) family of BC standards and technical specifications. These ISO publications are referenced comprehensively throughout the GPG.

The processes that form a holistic management system have been refreshed and integrated into a revised set of Professional Practices (PPs) to help the BC professional establish or improve existing processes. This approach gives far more scalability and flexibility to BC professionals, while aligning more effectively with the modern operational structures of global organizations.

About the BCI

The Business Continuity Institute (BCI) is the world's leading professional association responsible for improving continuity and resilience by building the capability and professional development of individuals worldwide.

Founded in 1994, the BCI has defined a set of practices for individuals to develop and demonstrate their expertise in BCM. These are the six PPs described in the GPG.

The vision of the BCI is a world where all organizations, communities, and societies become more resilient through the implementation of management practices as presented in the GPG.

The BCI relies upon its core values of professionalism, reliability, and inclusivity to create the principles of excellence in the field of BC. The BCI therefore continues to be the trusted source of academic and practitioner knowledge on all aspects of BC theory and practice.

The BCI also offers a wealth of online resources via thebci.org. Ongoing global efforts by the BCI and the professional community ensure this GPG stays relevant through periodic revision.

What is business continuity management?

BCM is a discipline that enables the resilience of organizations through the careful management of the PPs presented in this GPG. It incorporates the tried and tested methodology that an organization should adopt as part of its overall approach to continue the delivery of products and services at a predefined capacity and within acceptable time frames during a disruption.

BCM identifies organizational continuity requirements and implements recovery strategies. It also supports the design and implementation of plans and procedures used by professionals to protect and continue the value-creating operations of an organization during a disruption.

What is the BCI's GPG?

Since it was first issued in 2001, the BCI's GPG has become one of the leading global guidance resources for BC professionals. Consequently, BCI members consider it to be one of the main references for anyone needing to know about BC and resilience as part of their role and responsibilities.

The GPG caters to individuals who wish to gain an internationally recognised accreditation in BC and become certified members of the BCI, by showing competence in all six PPs. The Certificate of the BCI (CBCI) examination tests the subject matter knowledge of the GPG across all PPs.

This GPG describes not only what professionals should do but also provides context about why and how to do it, as well as detailing the value of each PP.

This GPG supports the BCI Competency Framework*, which forms the foundation of the BCI's globally recognised and respected education programme delivered through the BCI's far-reaching network of licensed training partners and approved instructors.

This GPG and the Competency Framework in tandem enable the BCI to develop qualification syllabi that meet the needs of all BC professionals. This includes the CBCI qualification, which enables successful candidates to use the CBCI post-nominal credential, and access to academic materials as published by the BCI.

***For more information or to download the BCI Competency Framework visit thebci.org**

Tips on navigating the GPG

Headings used within the chapters of the GPG

Interwoven within each PP is a set of standardised headings designed to help BC professionals learn and incorporate information to process into their BCMS.

These consist of a common structure for the explanation of the different sections of each PP, including:

- General Principles,
- Concepts and Considerations,
- Process,
- Methods and Techniques,
- Outcomes and Review,

Not all headings are present in each PP.

Introduction

The introduction contains an executive summary of the upcoming content and introduces terminology, including relevant common abbreviations.

Principles and Considerations

Throughout the GPG, two of the recurring headings will be:

1. General Principles,

2. Concepts and Considerations.

Both headings encompass practitioner-led strategic reflections and additional details regarding the dependencies within a BCMS that must be considered before defining a process. Once the Principles and Considerations are defined, each section of the PPs proceeds to outline the processes and the related methods and techniques to establish them.

Process

The Process section provides step-by-step guidance coupled with a set of actions to be performed in a suggested order to meet the requirements as outlined in each chapter.

Methods and Techniques

Provides a selection of defined systems and practices that may be applied to enable the successful implementation of a process, taking into account Principles and Considerations.

Outcomes and Review

At the very end of a standalone process, the Outcomes and Review heading contains the required knowledge to define and review the metrics to gauge the level of efficacy and success of the system created to meet the defined targets.

Who is the GPG audience?

As a body of knowledge, the GPG is used as an information source for:

- BC professionals,
- The participants in training programmes, and
- The audience of awareness campaigns or those who wish to get a better understanding of BC.

The GPG is relevant to anyone with BC or a resilience-related role, including, but not limited to those working in:

- Risk management,
- Information security,
- Corporate security,
- Emergency management,
- Facilities management,
- Environment,
- Health and safety,
- Communications,
- Human resources, and
- Logistics.

What is the difference between the GPG and international standards?

The ISO standard for BC (ISO 22301:2019) specifies requirements for a BCMS. Organizations might choose to pursue ISO certification for their BCMS, which is achieved through an authorised certification representative.

In this latest version of the GPG, there are stronger links with BC-related ISO standards, such as:

- **ISO 22313:2020 Security and resilience**
  - Business continuity management systems
  - Guidance on the use of ISO 22301
- **ISO/TS 22317:2021 Security and resilience**
  - Business continuity management systems
  - Guidelines for business impact analysis
- **ISO 22301:2019 Security and resilience**
  - Business continuity management systems
  - Requirements
- **ISO/TS 22318:2021 Security and resilience**
  - Business continuity management systems
  - Guidelines for supply chain continuity management
- **ISO/TS 22331:2018 Security and resilience**
  - Business continuity management systems
  - Guidelines for business continuity strategy
- **ISO/TS 22332:2021 Security and resilience**
  - Business continuity management systems
  - Guidelines for developing business continuity plans and procedures

- **ISO 22361:2022 Security and resilience**
  - Crisis management
  - Guidelines
- **ISO 31000:2018 Security and resilience**
  - Risk management
  - Guidelines

The links to ISO are in the form of practical methodologies interwoven within the PP with a view to help actualise the requirements as defined by the ISO. The GPG is as prescriptive as possible about implementing the BCMS and describes the priority stages in developing, applying, and managing a successful management system. Where prescriptive methodologies are deemed not fit for purpose, a more strategic and high-level methodology is adopted, e.g. PP2, suggesting additional reference to professional practice.

Demonstrating knowledge and understanding of the six PPs is at the core of this GPG and may lead to individual certification through professional accreditation.

Further context around the links between the GPG and ISO standards

The GPG is developed by many leading global experts who have also contributed to developing national and international standards. The publications are aligned as well as complementary and, while they serve different purposes, they are an essential and valuable part of any BC and resilience professional's toolkit.

Those needing to understand BC can be confident that by using the GPG they are guided by internationally accepted leading practices.

How was the GPG created?

This GPG was created by combining the shared knowledge and extensive experience of many volunteers from the BC profession, spread across countries and continents, representing a wide range of industry sectors. This diverse group, including BCI members and non-members, provided feedback on the 2018 version of this GPG, which formed the basis for the updates and additions that produced this latest revision.

The terminologies used in this GPG are consistent with ISO. However, an organization may use different terms provided all interested parties clearly understand them.

What has changed from the previous edition of the GPG?

This latest edition of this GPG encompasses the progressive evolution of BCM as a discipline and the BCMS as the realisation of BCM. It incorporates updated processes and terminologies that have entered or evolved within the BC lexicon since the last review. Therefore, BCMS has replaced what used to be termed as the BCM Lifecycle.

This is to facilitate an effective management system to realise the benefits of BCM, therefore replacing the previous BCM Lifecycle with a more scalable and holistic BCMS.

Furthermore, the BCMS supports the organization's strategic objectives and proactively builds the capability to continue business operations during disruption. The BCMS includes identifying operational risk sources, creating response structures and plans supported by competent people to address incidents and crises, and promoting validation and continuous improvement. The BCMS is flexible and scalable; therefore, there may be changes between the internal and external operating context, delivering measurable value to the organizations where a management system process already exists.

To reiterate, the methodology behind creating a BCMS is designed to be scalable and applicable to all industry sectors and organizations, regardless of size, complexity, or geographical location.

Where a BCMS has been successfully established, the subsequent reviews of the processes and projects that form the BCMS will require deeper dives into each element with a view to improving and evolving the management system. Alternatively, reviews of the management system could be necessary due to local laws or international bodies placing a different set of responsibilities on an organization. Consequently, this GPG provides references and signposting to international standards containing detailed methodologies and techniques that may be implemented to deal with the increased complexities of a globalised world.

This revised version retains the six PPs that are the building blocks of the BCMS and therefore represent the core of BC good practice. The six PPs are split into two management practices and four technical practices.

The focus and emphasis of the latest GPG have evolved as BC practices have become further established and as more organizations are implementing a BCMS or wish to further align to ISO 22301:2019.

The GPG Edition 7.0 retains the information needed to start afresh in an organization and implement a new BCMS. It also provides guidance to BC professionals reviewing or revising an existing management system.

Professional Practice (PP) Structure

The two management practices and the four technical practices follow a bespoke design structure that is important to conduct in the suggested order, especially if starting on a journey that will lead to a brand new BCMS.

A specific call out to the structure of **PP2**, Embracing BC. Readers will notice that the structure and content of **PP2** is delivered slightly differently to other PPs within the GPG. This is because the processes required to embrace BC across all parts of the organization involve substantial emotional intelligence and adaptability. While with other methodologies and techniques across all other PPs it is possible to be strategically prescriptive, the chapter on Embracing BC requires a different approach.

Therefore, it is structured to enable the BC professional to be:

- Self-aware and pragmatic,
- Observant of different organizational cultures,
- Continuously making required course corrections using experience and ingenuity, and
- Establishing and maintaining appropriate initiatives to make BC acceptable to all employees in the organization irrespective of seniority or hierarchy.

This paradigm shift has also meant that Embedding, which was the title of **PP2** in the GPG 2018 Edition, has evolved into Embracing BC to shift the focus from ticking boxes to improving the quality of BC outcomes and tailoring processes.

Several other changes have been undertaken throughout Edition 7.0 to assist the reader's understanding and navigation.

They include:

- Greater emphasis on when and how BC professionals may and should collaborate with professionals from other management disciplines to build more resilient organizations.
- Further references to supply chains and outsourced services are made throughout the guidelines, which means there is no longer a separate section in the GPG on this concept. The information has been interwoven into the body of the PPs.
- Further guidance includes understanding risk assessments and how disruption-related risk relates to BC.
- An increase in cross-references throughout the guidelines to the BCI publications and revised ISO standards.
- References to additional sources of information for further reading and guidance.

A greater distinction has also been made between BC and crisis management. While these are two distinctly different capabilities, they also need to work together.

Consideration has been given to how to manage the implementation of the risk treatments and the BC recovery strategy in **PP4**.

There is also revised methodology to produce recovery plans to return to BAU after a disruption.

Terminology

The use of terminology in Edition 7.0 has been carefully considered to reflect the evolving BC discipline. In most cases, the BCI has adopted ISO terms and definitions coupled with practitioner-approved definitions that have been adopted across all iterations of the GPG. Some terms that do not exist yet in ISO standards have been used but these are already part of the BC professional lexicon. In certain cases, definitions have evolved. For example, 'prioritised activities' replaces 'most urgent', 'priority activities', and 'important activities'. This supports consistent and clear definitions that have the same meaning globally and across multiple industries.

This GPG also leverages its own definitions in the interests of clarity and improved understanding.

For example:

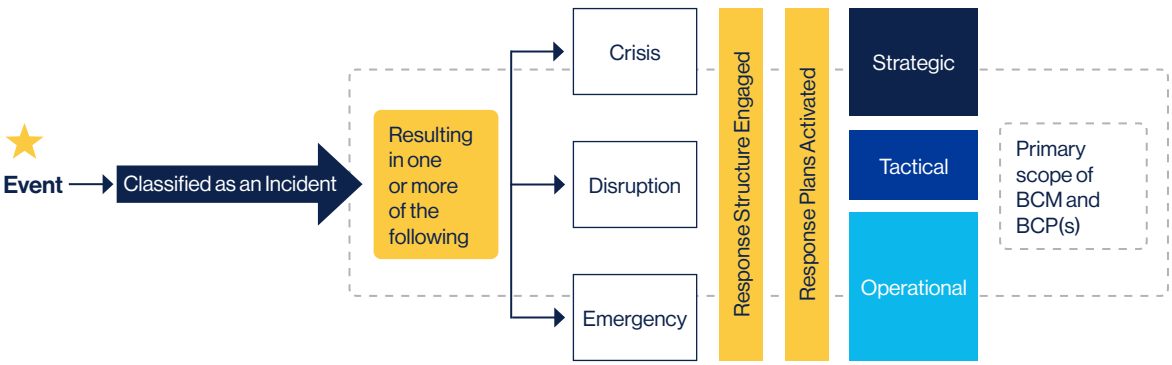
- 'Business continuity' is the collective term to include response, recovery, and resumption of activities impacted by a disruption.
- 'Business impact analysis' identifies the BC requirements, providing information to determine BC solutions.
- The previous use of the term 'business continuity recovery strategies' in **PP4** has been changed to provide further clarity and is now 'business continuity recovery strategies and solutions'.
- 'Business continuity requirements' are defined as the time frames, resources, and capabilities necessary to continue delivering prioritised products, services, processes, and activities following a disruption.

Lastly, GPG Edition 7.0 makes a clearer distinction between 'incident management' and 'crisis management', as well as the required level of response and capability. This concept is introduced in **PP1** and covered in detail in **PP5**.

It is important to reiterate that the GPG makes multiple BC related ISO references throughout its chapters. There are also references to concepts such as incidents, plans, and response structures throughout this GPG. These concepts are beyond the generally accepted scope of BC but are important considerations for professionals that wish to implement best practice. The following diagram shows the relationship between events and incidents, as well as the different classification terminology within the term Incident in the context of BC.

The diagram brings together information curated from multiple ISO standards as part of a response mechanism as well as processes outlined within this GPG. This is a good example showing how ISO standards as well as GPG concepts come together in a response structure. The increasing importance of enhancing resilience reinforces the value of building effective BC capabilities and is central to the purpose of the BCI and this GPG.

Further details can be found within **PP5**.



The BCMS: The Professional Practices (PP)

Management Practices

PP1 - Establishing a BCMS

This chapter outlines how a BCMS should be designed and implemented as a programme. **PP1** also establishes a policy and governance process to maintain a BCMS through an ongoing cycle of activities.

PP2 - Embracing Business Continuity

This chapter highlights the importance of Embracing BC. The premise for Embracing BC is designed to deliver outcomes that are the product of an organization with a strong BC culture, where individuals and teams have a deeper and more empathetic understanding of the BCMS and believe that BC is a core function.

Technical Practices

PP3 - Analysis

This chapter contains the two techniques used for analysing BC requirements: the business impact analysis (BIA) and the risk assessment (RA). The BIA estimates the impacts of disruption over time to determine the organization's response, recovery priorities, and resource requirements. The RA analyses relevant risks to prioritised activities to identify concentrations of risk or single points of failure that may result in disruption.

PP4 - Solutions Design

Solutions Design is dependent on the outcomes of **PP3**. It outlines the methodology to undertake a gap analysis comparing the current-state capabilities to the BC requirements. Where gaps exist, the organization must define strategies and solutions to resume business operations and mitigate unacceptable risks and single points of failure.

PP5 - Enabling Solutions

Enabling Solutions is dependent on the outcomes of **PP4** and outlines the methodology to implement the agreed solutions. The solutions are supported by response structures and business recovery plans. The resulting plans and processes are designed to be scalable and therefore able to be deployed in response to any incident type.

PP6 - Validation

Validation brings together all the PPs to test the cohesion of the BCMS and to prove or disprove the efficacy of the resources deployed to deal with incidents. This is achieved through a combination of exercising, maintenance, and review to ensure proportional and reasonable BC recovery strategies are set up to support response structures and BC plans.

The primary aim of **PP6** is to measure the competence of individuals, team cohesiveness, the quality of the BCMS, and the effectiveness of the BC capability.

Acknowledgements

The GPG Edition 7.0 is a revision of the 2018 edition and builds on the earlier 2013, 2010, 2008, 2005 and 2001 versions.

The objectives are to:

- Remain up to date and ensure the GPG provides practical guidance on BCMS implementation.
- Ensure the BCI global good practices remain aligned with relevant international standards.
- Ensure this GPG remains internationally relevant.

The BCI acknowledges and appreciates the following individuals for their contribution. **Without them, this project could not have come to fruition:**

Technical Advisory Group

Eren Aslan MBCI, Katherine Whitaker MBCI, Lisa Jones MBCI, Michael Crooymans Hon FBCI, Milena Maneva AMBCI, Ratna Pawan MBCI, Sanjiv Agarwala FBCI, Saul Midler Hon FBCI.

Working Group Members

Affeiz Abdul Razak MBCI, Alessandro Caillat FBCI, Charlie MacLean-Bristol FBCI, David Window MBCI, Dean Beaumont FBCI, Des O'Callaghan FBCI, Fiona Raymond-Cox FBCI, Gary Vogel MBCI, Gianna Detoni FBCI (1957-2022), Helen Lipscombe MBCI, Ilango Vasudevan Hon FBCI, Jeff Lewis MBCI, Keith Frederick FBCI, Kuniyuki Tashiro FBCI, Macarena Rodriguez MBCI, Margaret Millett Hon FBCI, Mark Hoffman MBCI, Matthias Rosenberg FBCI, Mohammed Issa Hammad FBCI, Nashikta Angadh AMBCI, Nikolaos Loukeris MBCI, Paul Breed MBCI, Seshadri Srinivasan FBCI, Shane McMahon MBCI, Yves Davila MBCI.

Special thanks to the BCI Board for additional contributions and advice and to Samhita Sarkar Ganguly for project managing this edition of the GPG.

Glossary of Terms

Term	Definition	Source
Activity	One or more tasks with defined output.	ISO 22301:2019
Audit	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.	ISO 22301:2019
Business continuity (BC)	The capability of an organization to continue the delivery of products and services within acceptable time frames at a predefined capacity during a disruption.	ISO 22301:2019
Business continuity champions	Persons tasked with supporting the BCMS from the perspective of their area of expertise, by inputting and maintaining the system and periodically updating documentation.	GPG Edition 7.0
Business continuity management (BCM)	**The elements of BCM are as follows:** a) Operational planning and control. b) BIA and risk assessment. c) BC strategies and solutions. d) BC plans and procedures. e) Exercise programme. f) Evaluation of BC documentation and capability.	ISO 22313:2020
Business continuity plan (BCP)	Documented information that guides an organization to respond to disruption and resume, recover and restore the delivery of products and services consistent with its BC objectives.	ISO 22301:2019
Business continuity requirements	The time frames, resources, and capabilities necessary to continue to deliver the prioritised products, services, processes, and activities following a disruption.	GPG 2018
Business impact analysis (BIA)	A process of analysing the impact over time of a disruption on the organization.	ISO 22301:2019
Competence	The ability to apply knowledge and skills to achieve the intended result.	ISO 22301:2019
Controls	Measure that maintains or modifies risk. Controls include but are not limited to any process, policy, device, practice, or other conditions or actions which maintain or modify risk.	ISO 22300:2021
Crisis	An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.	ISO 22300:2021
Crisis management	Coordinated activities to lead, direct and control an organization with regard to crisis.	ISO 22361:2022
Disruption	Incident whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives.	ISO 22300:2021
Incident	An event that can be, or could lead to, a disruption, loss, emergency, or crisis.	ISO 22301:2019

Term	Definition	Source
Injects	Individual timeline events that are part of an exercise. They may include simulated media news clips, website articles, social media feeds, telephone calls, emails, and text messages.	GPG Edition 7.0
Interested parties	A person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. **Note:** this is the preferred term – stakeholder is permitted.	ISO 22300:2021
Invocation	The act of declaring that an organization's BC arrangements need to be put into effect in order to continue the delivery of key products or services.	ISO 22300:2021
Management system	Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.	ISO 22301:2019
Maximum tolerable period of disruption (MTPD)	Time frame within which the impacts of not resuming activities would become unacceptable to the organization.	ISO 22301:2019
Minimum business continuity objective (MBCO)	The minimum capacity or level of services or products that is acceptable to an organization to achieve its business objectives during a disruption.	ISO 22300:2021
Organization	The person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives.	ISO 22301:2019
Organizational culture	The values, attitudes and behaviour of an organization that contribute to the unique social and psychological environment in which it operates.	ISO 22316:2017
Organizational resilience	The ability of an organization to absorb and adapt to a changing environment.	ISO 22316:2017
Outsource	Acquisition of services (with or without products) in support of a business function for performing activities using suppliers' resources rather than the acquirer's.	ISO/TS 27036-1:2021
Personnel	People working for and under the control of the organization.	ISO 22301:2019
Policy	Intentions and direction of an organization as formally expressed by its top management.	ISO 22301:2019
Prioritised activities	Activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption.	ISO 22301:2019
Priority suppliers	Priority suppliers are those who support prioritised activities and are identified as having the greatest impact if they fail to deliver resources, thereby impacting the organization's ability to deliver its own products or services.	GPG Edition 7.0
Process	Set of interrelated or interacting activities which transform inputs into outputs.	ISO 22301:2019
Product and service	The output or outcome provided by an organization to interested parties.	ISO 22301:2019

Term	Definition	Source
Programme	Group of programme components managed in a coordinated way to realize benefits.	ISO 21503:2022
Recovery point objective (RPO)	The point to which information used by an activity is restored to enable the activity to operate on resumption to pre-defined levels.	ISO 22300:2021
Recovery time objective (RTO)	The time frame within the MTPD for resuming disrupted activities at a specified minimum acceptable capacity.	ISO 22301:2019
Resources	All assets (including plant and equipment), people, skills, technology, premises, and supplies and information (whether electronic or not) that an organization must have available to use, when needed, in order to operate and meet its objectives.	ISO 22301:2019
Risk	Risk is defined as the 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.	ISO 31000:2018
Risk assessment	Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment should be conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiries as necessary.	ISO 31000:2018
Risk management	Coordinated activities to direct and control an organization with regard to risk.	ISO 31000:2018
Risk source	An element that alone or in combination has the potential to give rise to a risk.	ISO 22300:2021
Risk treatment	The process of modifying risk. **Note 1 to entry:** 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 in order to pursue an opportunity, removing the risk source, changing the likelihood, changing the consequences, and sharing the risk with another party or parties (including contracts and risk financing) and retaining the risk by informed choice. **Note 2 to entry:** risk treatments that deal with negative consequences are sometimes referred to as 'risk mitigation', 'risk limitation', 'risk prevention', and 'risk reduction'. **Note 3 to entry:** risk treatment can create new risks or modify existing risks.	ISO 22300:2021
Scenario	A scenario is a pre-planned storyline that drives an exercise, as well as the stimuli used to achieve exercise project performance objectives.	ISO 22300:2021
Service level agreement (SLA)	A commitment between a product or service provider and a client organization, aspects of which would include quality, availability, responsibilities, and continuity capabilities, which are agreed upon between the two parties.	GPG Edition 7.0 ISO 22318:2021
Simulation	A simulation is the imitative representation of the functioning of one system or process by means of the functioning of another.	ISO 22300:2021

Term	Definition	Source
Stakeholder	This is a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. The term 'interested party' (preferred term) can be used as an alternative to 'stakeholder'.	ISO 22301:2019
Supply chain continuity management (SCCM)	Management process that identifies potential impacts to an organization from disruption to its supply chain and provides an approach to manage and protect the organization's business activities from supply chain disruption by ensuring continuity of supply of resources as well as the ability to continue delivery of its products and services.	ISO 22318:2021
Test	A unique and particular type of exercise which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned.	ISO 22300:2021
Threat	A potential cause of an unwanted incident that may result in harm to individuals, assets, a system or organization, the environment, or the community.	ISO 22301:2019
Top management	A person or group of people that directs and controls an organization at the highest level.	ISO 22301:2012
Workforce	People/workers who provide a service or input to contribute to the business or organizational outcomes. This can include employees, contractors, and volunteers.	GPG Edition 7.0
Workplace	A workplace is any location where people conduct business for their employer or themselves.	GPG Edition 7.0

BCI Professional Practices

PP1: Establishing a BCMS

Establishing a BCMS is the PP that outlines how the programme will be designed and implemented.

A BCMS will understand the organization's needs and necessity for establishing BC policies and objectives, together with the importance of operating and maintaining processes, capabilities, and response structures for ensuring the organization will survive disruptions, while monitoring and reviewing performance and effectiveness of the BCMS, where continual improvement is based on qualitative and quantitative measures. The purpose of a BCMS is to prepare for, provide and maintain controls and capabilities for managing an organization's overall ability to continue to operate during disruptions.

Introduction

Establishing a BCMS involves coordinating a series of interrelated activities to:

1. Define the scope of the BCMS.
2. Establish a BC policy.
3. Establish high-level governance of the BCMS.
4. Determine the objectives of the BCMS.
5. Determine how the objectives of the BCMS will be met.
6. Develop detailed operational processes and associated roles and responsibilities.
7. Validate the BCMS.
8. Ensure the organization has a culture that supports the BCMS.
9. Establish how the BCMS will be monitored, reviewed, and continually improved over time.

Some of these activities are explained in detail across this chapter while others are explained in other PPs:

Table 1: activities needed to establish a BCMS.

Activities	PP
Define the scope of the BCMS.	**PP1**
Establish a BC policy.	**PP1**
Establish high-level governance of the BCMS.	**PP1**
Determine the objectives of the BCMS.	**PP3** The BC requirements are the objectives of the BCMS.
Determine how the objectives of the BCMS will be met.	**PP4** Risk treatments and BC solutions are designed to meet the BCMS objectives.
Develop detailed operational processes and associated roles and responsibilities.	**PP5** BC plans are detailed operational processes; the associated roles and responsibilities are the response structure.
Validate the BCMS.	**PP6** Validation confirms that the BC solutions meet the BC objectives/requirements.
Ensure the organization has a culture that supports the BCMS.	**PP2** Embracing the BCMS are ongoing developments of BC culture.
Set out how the BCMS will be monitored and continually reviewed over time.	**PP1** As part of the governance, this is set out at a high level in the BC policy (**PP1**) and covered in detail in all the other PPs.

None of the activities described in the PPs are one-time activities – and their outcomes are not static. Establishing and operating a BCMS is an iterative journey of continual improvement over time. Once a BCMS is established, however, some activities are likely to be repeated less frequently than others.

The activities explained in more detail in this section of the GPG are:

- **Coordinating the activities needed to establish a BCMS:** How the activities should be managed and who should be involved.
- **Determining the scope of the BCMS:** A clear statement of the areas of the organization that are covered by the BCMS.
- **Establishing a BC policy:** A high level statement of the organization's BC intentions and direction.
- **Establishing governance:** The roles, responsibilities and authorities needed to develop, operate, and monitor the BCMS in accordance with the BC policy.

These are just the first steps, the activities described in the other PPs are also needed to establish the BCMS.

Coordinating the Activities needed to Establish a BCMS

General Principles

- Establishing a BCMS for the first time requires all the activities listed in Table 1. Because the activities are interrelated, some are dependent on the outcome of others – so the activities need to be coordinated.
- Once the BCMS has been established, it becomes part of BAU. This does not mean that it is static. The performance of the BCMS is monitored and regularly reviewed to ensure it continues to meet the organization's needs and to identify opportunities for continual improvement. Establishing, operating, and improving a BCMS requires top management commitment and support, especially for establishing a BCM policy that is aligned with the strategic direction of the organization and for ensuring the resources needed for the BCMS are available.
- Establishing, operating, and improving a BCMS requires input from multiple interested parties with different needs, expectations, and perspectives.
- The number of stakeholders will depend upon the size, complexity, and type of the organization.

When a BCMS is being established for the first time, the organization may need to develop and implement an interim crisis management plan. This interim plan should be supported by subject matter experts with sufficient knowledge to manage a crisis effectively prior to the development of the full BCMS (**PP5**). The interim plan may then be reviewed and consolidated into the BCMS later.

Concepts and Considerations

- To establish a BCMS in large or complex organizations, coordination of activities is typically achieved through a programme made up of related projects and BAU activities. In smaller organizations, coordination of activities may be achieved through a single project.
- Once established, any major change to the BCMS – for example due to a significant change in the organization's operating context – may be managed through a further programme.
- If the organization has a project and programme management methodology, this should be used to coordinate activities. If not, using a recognised project and programme management methodology will be beneficial.
- Awareness and understanding of the external and internal operating context, including organizational strategy and risk tolerance (also referred to as risk appetite) is essential when working to establish a BCMS. The BCMS supports organizational goals and strategies.
- Early engagement with stakeholders affected by the BCMS is essential to understand their needs and expectations, avoid duplication of effort, and avoid conflict downstream. Stakeholders might include people with responsibility for corporate governance, enterprise risk management, facilities, safety and security, and other core business functions. Taking an organization-wide view and collaborating cross-functionally at an early stage will contribute to the effectiveness of the BCMS and therefore to the overall resilience of the organization.
- Other policies and programmes in the organization that are relevant to BC should be identified and opportunities for collaboration considered and coordinated.
- For example, the people and culture department may have policies for internal communications, and the corporate communications department may have predetermined agreements for external communication due to a regulatory or customer requirement. These should be identified and referenced within the BCMS.
- The organization should determine the documented information necessary for the BCMS. As the BCMS is being developed, decisions and processes should be documented and the documents controlled.

Process

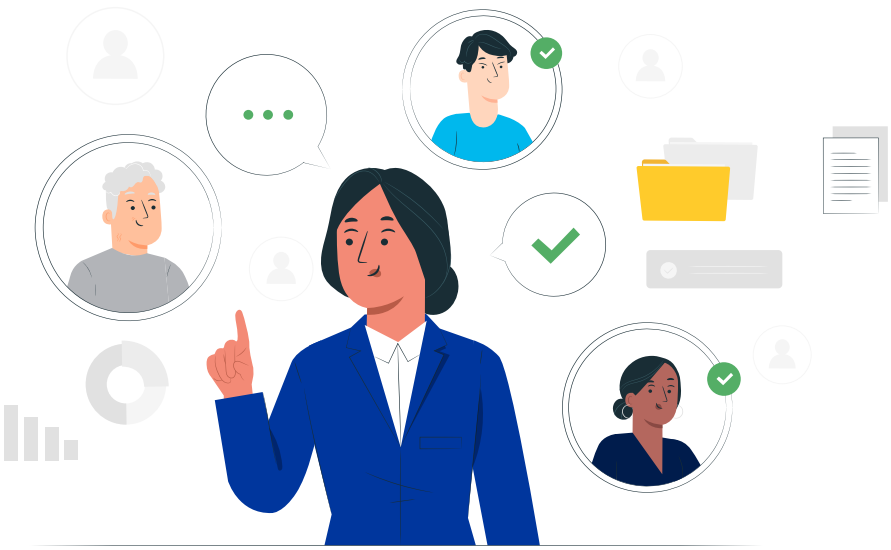
The coordination process will depend on the project and programme management methodologies used in the organization.

It is good practice to:

1. Have a top management member as a sponsor for the programme or project that coordinates activities. One of the key challenges of establishing an effective BCMS is buy-in across the organization. Having a top management sponsor will minimise this challenge.
2. Establish a multi-disciplinary steering group of subject matter experts to oversee, advise, and make recommendations as the BCMS is developed.
3. Establish communication channels for consulting stakeholders. These may be face-to-face or virtual, and synchronous or asynchronous.

Methods and Techniques

- Project and programme management methods for coordinating activities.
- Stakeholder identification, mapping, and engagement.
- Identification of external suppliers.
- Facilitation and communication methods for working with stakeholders.
- Specialist software can be used to manage data, documents, and projects.



Defining the scope of the BCMS

General Principles

The following principles should be considered when defining the scope of the BCMS:

- Defining the scope ensures clear understanding of which areas of the organization are covered by the BCMS and which areas are not.
- A well-defined scope focuses the BCMS on organizational priorities and ensures the BCMS makes best use of available resources, such as funding and time.

  Although an initial scope needs to be defined, it is subject to change as the BCMS is developed, for example if the organization identifies gaps in the initial scope when it conducts a BIA (PP3).
- The initial scope of the BCMS may be limited to specific areas of the organization with high value, as identified with the relevant stakeholders. This would make it easier to manage risk, complexity, and cost across the organization. Further development and reviews of the BCMS could then provide a better understanding of BCM across the organization and create opportunities to expand the scope and enhance resilience.
- Once the BCMS is established, its scope should be reviewed at pre-agreed intervals to ensure the BCMS continues to focus on the high value areas of the organization. The scope should also be reviewed if there is a change to the internal or external operating context, **for example:**
  - » Acquisition, merger, or divestiture.
  - » Changes to products or services (including those that are outsourced).
  - » Changes to the way products and services are delivered.
  - » Geographic relocation of the organization.
  - » Changes to legal or regulatory requirements.
  - » Major disruption that highlights the need to change the scope of the policy.
- The BCMS scope should be available as documented information.
- The scope of the BCMS is independent of the BC policy, so it may be defined before or after the policy is written.

Concepts and Considerations

- The scope of the BCMS needs to be defined before proceeding with the activities described in other PPs.
- Scope is usually defined in relation to high-value products and services. Alternatively, locations may be used to define the scope, allowing the BCMS to include and exclude locations or sites.
- There may be occasions when an organization must build its initial implementation of the BCMS based on a regulatory requirement, a customer demand, certification against a standard, or an audit finding. In this case, the organization will need to include all the activities associated with the relevant requirement in the BCMS scope.
- When an external supplier is involved in delivering a product or service that is within the BCMS scope, this supplier and their supply chains should also be in scope. This extends to supporting information communication technology (ICT) and resources, facilities services, or on-site health service providers.
- There might be occasions when an organization's priorities change during the establishment of a BCMS after the scope has been defined – for example if an unexpected regulatory requirement is imposed. If this happens, the organization should consider revising the BCMS scope.

Methods and Techniques

Methods and techniques for defining the initial scope of the BCMS include:

- Stakeholder consultation.
- Cost-benefit analysis.
- Consulting existing information, such as BIAs and risk assessments. Information might be held in parts of the organization such as risk management and internal audit teams.
- Consulting people who might have relevant knowledge that has not been documented.
- Horizon scanning to identify known and emerging risks (the horizon scanning process is further explained in (PP3).

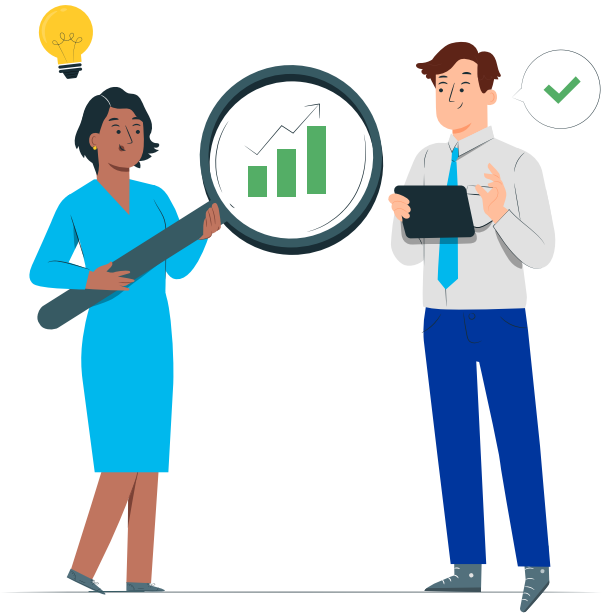
Outcomes and Review

The outcome is a documented scope statement which is reviewed at an agreed cadence.

The BCMS documentation may include the following:

- A defined BCMS scope.
- A BC policy.
- High-level governance structure.
- Objectives for the BCMS.
- How the objectives will be met.
- Detailed operational processes and associated roles and responsibilities.
- Ways in which the BCMS will be validated.
- How organizational culture will support the BCMS.
- How the BCMS will be monitored, reviewed, and continually improved over time.

It is important to note that some of these will only be available if the organization has already previously engaged in BC.



Establishing the BC Policy

The BC policy sets out the: "Intentions and direction of an organization as formally expressed by its top management," (ISO 22301:2019).

General Principles

- **The BC policy is a statement from top management that:**
  - » Explains the meaning and importance of BCM to the organization.
  - » Demonstrates top management commitment to the BCMS and its continual improvement.
  - » Sets expectations for how the BCMS will be used by all workers.
  - » Defines the guiding principles for setting, reviewing, and meeting BCMS requirements (objectives).
  - » The BC policy should be written at a level that is independent of the scope of the BCMS and does not include any specific information such as BCMS requirements, processes, or operational roles.
  - » The BC policy should be available as documented information that is communicated and understood by the whole organization.

Concepts and Considerations

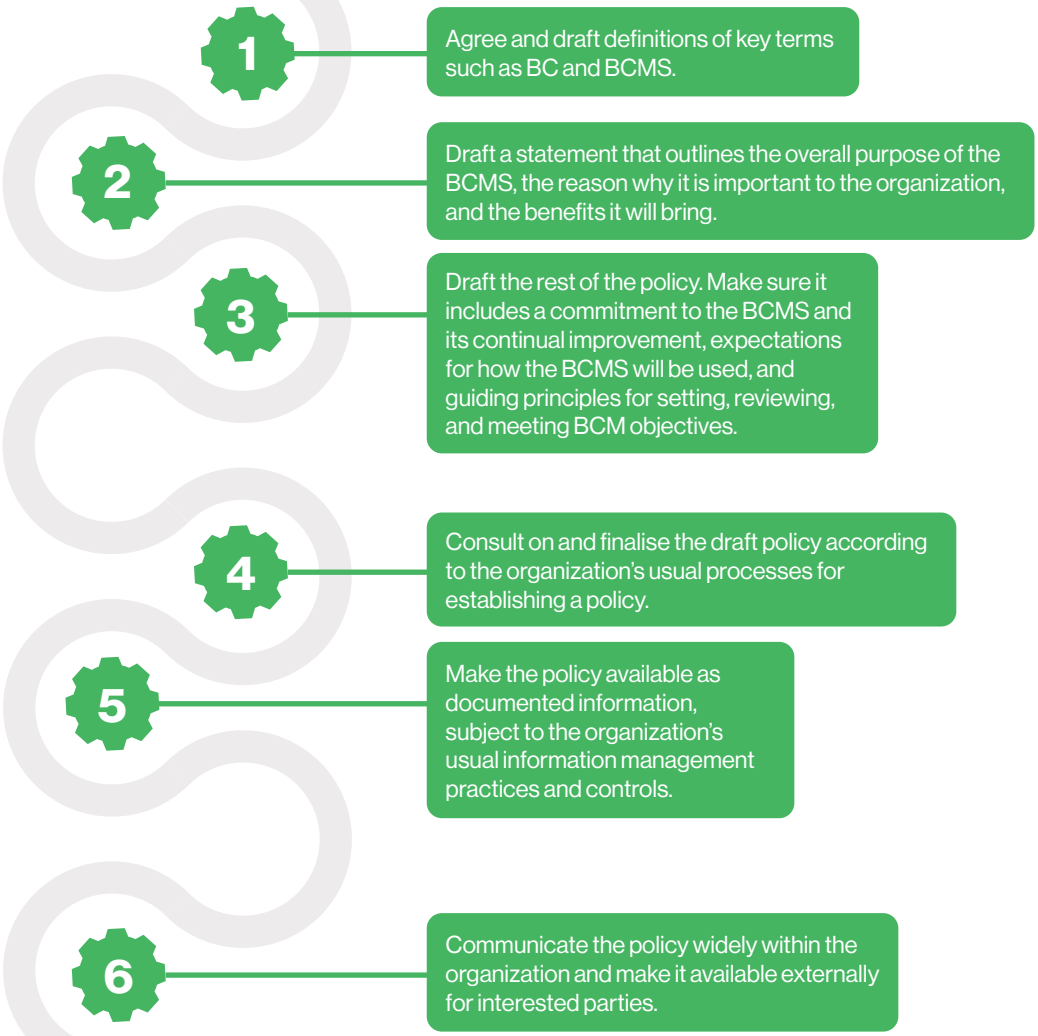
- The policy should be appropriate to the size, complexity, and type of the organization, and aligned with the organizational culture and operating environment.

  Global organizations may need to issue multiple policies to take account of different cultures in different locations.
- A long and complicated policy could be a barrier to effective communication and Embracing BC. The policy should focus on 'what' the organization will do, not 'how' it will be done. This will facilitate the swift establishment of the BCMS.
- **The policy may also include details such as:**
  - » The roles or people with overall responsibility and accountability for the BCMS
  - » A commitment to meeting the requirements of any relevant regulations, standards, and guidelines.

Process

The BC policy should be written by top management with support from BC professionals.

The steps required to develop an effective BC policy are:



Methods and Techniques

Methods and techniques for establishing the BC policy include:

- Using an organizational policy template that is accepted and recognisable by readers.
- Working with communication specialists to ensure the policy is easy to understand.
- Publishing the policy on the organization's website.

Outcomes and Review

The outcomes of an effectively communicated BC policy are:

- Shared understanding of the importance of a BCMS and its relevance to the organization.
- Clear expectations from the employees on how they will use the BCMS.
- Demonstration of top management commitment to the BCMS and a supportive organizational culture.

The policy should be reviewed at agreed intervals or following significant changes to the operating context, for example if there is a change in the approach to risk.

An effective policy, written at a high level, should not contain details that are likely to change frequently.

Establishing Governance

Establishing governance early in the development of a BCMS provides the foundation for its further development, effective operation, support, and continual improvement.

The early identification of clearly defined roles and associated responsibilities is a key element of governance and it is essential for an effective BCMS. Having top management sponsor the programme to establish the BCMS is necessary to ensure commitment across all organizational levels and functions.

Top management commitment and support are preconditions for an effective BCMS.

General Principles

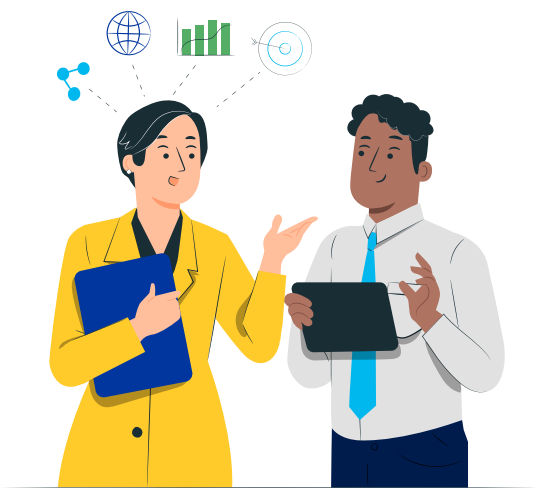
Top management should ensure that responsibilities and authorities for roles in the BCMS are assigned and clearly communicated.

Assigned responsibilities and authorities should cover the following activities:

- Monitoring and evaluating the performance of the BCMS and reporting the results to top management.
- As the BCMS becomes established, this includes reviewing the performance of the BCMS to ensure the requirements are being met.
- Ensuring that people are engaged and using the BCMS effectively, for example by following required processes.
- Ensuring that the BCMS remains aligned with organizational objectives and strategy.
- Ensuring the BCMS is aligned with the BC policy and meets any related legal and regulatory requirements.
- Supporting continual improvement.

Top management should ensure that the support and resources needed to establish and operate the BCMS are available. Resources include funding, time, technology, and competent people.

Top management should also ensure that people with accountable roles in the BCMS are competent and receive any necessary education and training.



Concepts and Considerations

- Assigning overall accountability for the BCMS and its effectiveness to a member of top management ensures that the BCMS is recognised as a key part of the organization.
- Senior accountability for the BCMS makes it visible across the organization, which may encourage collaboration across organizational boundaries.
- BCMS responsibilities should be included in job descriptions and communicated to all interested parties.

Process

Establishing governance for a new BCMS is an iterative process. It will depend on the size and complexity of the organization and on the organization's existing practices for introducing new management systems.

Early in the establishment of the BCMS, it is likely that the organization will not understand all the roles, responsibilities, and authorities required to operate the BCMS. The initial focus should be on establishing a governance structure that enables the programme, or whatever mechanism is used, to coordinate the activities needed to establish the BCMS. The essential roles at the outset might be, for example, a top management sponsor, a programme manager, a BCM professional, and a steering group.

Methods and Techniques

The following table describes generic roles and responsibilities in a BCMS. In some organizations, people might take on more than one role.

Some roles, for example top management roles, are needed to establish a BCMS. The need for other ones will emerge as the BCMS becomes operational.

Table 2 : roles involved in establishing, managing, and using a BCMS.

Role	Responsibilities
Top management	• Providing leadership, commitment, support, and resources to the BCMS. • Assign responsibilities and authorities for other BCMS roles. • Establishing and communicating the BC policy. • Ensuring the performance of the BCMS is monitored, reviewed, and continually improved. • Promoting and contributing to the BC culture, including leading by example.
Steering group/ committee	• Overseeing, supporting, and advising on the establishment and operation of the BCMS. • Making recommendations, removing roadblocks, and reporting to top management.
BC professional	• Developing, coordinating, and facilitating the BCMS. This includes developing analysis and BC plan templates. • Facilitating and coordinating the BIA, risk and threat assessment (related to prioritised activities), strategy and solutions planning, BC plans and testing throughout the organization. • Ensuring maintenance of the BCMS on a periodic basis as well as whenever it is appropriate.
BC plan owner	• Ensuring that the BC plan (or plans) adequately delivers the organization's BC capability and meets the BC requirements.
Incident response team	• Responding to an incident or crisis, delivering the BC solutions, and following the BC plans.
Departmental representative	• Communicating the implications of departmental changes that may impact the BCMS. • Collecting information for and completing the BIA. • Identifying and acknowledging supply chain priorities. • Developing, implementing, and maintaining departmental procedures on behalf of the plan owner. • Conducting and participating in exercises. • Maintaining the departmental BC documentation. Liaising with the BC professional.
Workforce/personnel/ staff	• Understanding and acknowledging the relevance of the BCMS. Acknowledging roles and responsibilities during an incident to ensure effectiveness by understanding the BCMS. • Recognising an incident or crisis. • Alerting incident or crisis responders (including emergency responders) as appropriate. • Escalating action to the incident or crisis management team. • Responding appropriately to specific threats. • Responding appropriately when evacuated from the site. • Understanding relevant plans and associated roles and responsibilities.

It is recommended to have deputies assigned for all the roles listed above. The deputies must also be subject matter experts that may deputise for the primary role holder, in the event there is an unavailability of the primary role holder due, for example, to annual leave or illness.

Succession plans should also be considered for individuals with key roles and responsibilities within the BCMS, such as incident response personnel, plan owners, and departmental representatives.

Those responsible for BC should already have or be working towards a professional credential from an appropriate professional body (such as the BCI) to maintain and continue their professional development.

Outcomes and Review

Establishing governance at an early point in the development of a BCMS demonstrates top management's commitment, involvement in, and accountability for the BCMS from the outset.

The outcomes of assigning responsibilities and authorities for the BCMS are:

- Clearly defined, communicated, and understood roles and responsibilities, assigned to competent individuals and teams.
- Appropriate authority assigned as relevant to the role.

The governance of the BCMS should be reviewed at pre-agreed intervals or following a significant change in the organization's context.

A strategic checklist upon successful completion of PP1 should confirm the organization has:

- An initial definition of the scope of the BCMS.
- A BC policy.
- Assigned roles, responsibilities, and authorities.
- A programme (or another mechanism) for continuing the establishment of the BCMS.

The iterative journey has begun. The next step is to work through the activities in the remaining PP sections of the GPG.

BCI Professional Practices

PP2: Embracing Business Continuity

Embracing Business Continuity is the PP that enables the organization to improve the BC culture underpinning the BCMS over time.

Embracing BC is a paradigm shift from mandating and enforcing compliance (for example, to a policy) by embedding BC into the organization. Embracing supports the requirements present in policies and audit requirements and it is an outcome of education, awareness, and a greater understanding of the reason why the organization needs protection from operational disruptions. Embracing also elaborates and provides clarity on those nuances and grey areas that are often missing from compliance and statutory requirements. This level of pragmatism is specifically designed to help persuade all members of an organization to adopt a BCMS. Time demands and overall commitment from personnel will only be met once the workforce truly believes that BC must be up-to-date and operational to protect the organization and its interested parties. This results in an improved BC culture that delivers fit-for-purpose capability and competency.

Introduction

The most common drivers for BC derive from regulations, statutory demands, audits, compliance requirements, risks, client expectations, and shareholder pressure. In response, top management normally mandate BC via a policy to protect the organization from disruptions and embed BC.

The term 'embedding' is used to describe a process that defines how to integrate BC practice into BAU activities and organizational culture. Embedding includes allocating roles and responsibilities across the organization's hierarchy, providing training, scheduling BCMS-related activities over the calendar and confirming adherence to the policy. The BC professional then facilitates the organization through the BCMS.

However, what commonly emerges over time is a realisation that the policy and embedding activities alone do not guarantee fit-for-purpose BC. This becomes evident when organizations find it challenging to keep their documentation up-to-date or when incidents occur and BC plans prove to be inadequate.

A fit-for-purpose BCMS is not a point-in-time position or capability. Fit-for-purpose means that BC must always meet the operational requirements of the organization, regardless of organizational or operational change.

This requires beliefs and behaviours beyond the systematic process of operating a BCMS.

A key attribute of a fit-for-purpose BCMS is quality. For example, nominating personnel to participate in a BIA as part of the embedding does not guarantee a quality of outcome.

The following examples highlight reasons why quality suffers despite BC being embedded:

Table 3: examples of why embedding does not always result in BCMS quality.

Reason	Example
Insufficient priority	Other tasks are more important and delay BC to next year.
Lack of interest/commitment	Required personnel do not attend BC meetings or workshops.
No ownership	Consultants are engaged to run BC as a project.
Low attention to detail	Plans describe what to do, but not how to do it.
Corners are cut	Plans are created from BIA without the consideration of strategies and solutions. Plans are maintained without BIA refresh. Exercises are not undertaken.
Reviews and learning are limited	Exercises do not include debriefs or formal reports.
Not understanding the true benefit of BC	Changes to business operations, structure, technology, supplier, and the workforce are not recognised as drivers for BC reassessment.

As introduced in **PP1** and detailed further in this chapter, a fit-for-purpose BCMS derives from a corporate culture that has embraced BC. This is where personnel demand and do what is necessary to protect the organization and all interested parties. This type of commitment requires a journey over time. It starts with greater awareness, which leads to stronger beliefs and more constructive attitudes, eventually resulting in improved behaviours.

PP2 provides a structured approach for measuring and improving the BC culture of the organization so that, through Embracing BC, the organization truly does produce and maintain fit-for-purpose BC. The guidance presented in **PP2** for Embracing BC may equally apply to other management disciplines (for example, cyber security and health and safety) that collectively contribute to resilience.

Only then can BC move:

From – head (rational): A corporate mandate driven by policy.

To – heart (emotional): A cultural mandate driven by personal beliefs and corporate behaviours.

Understanding the Organization's Culture

General Principles

Fit-for-purpose BC requires the development of a management system that is consistent with the culture of the organization, so that the organization embraces the programme across all management levels. Therefore, individuals tasked with creating or enhancing a BCMS need to understand such a culture.

This requires an understanding of the beliefs, values, and assumptions that underpin how the organization operates and how personnel behave and interact.

Every organization has its own culture. It is the outcome of the interplay among several factors, including:

- The sector in which an organization operates,
- The tone set by the executive leadership,
- The mission and values of the organization, and
- The wider role the organization plays in the community.

Concepts and Considerations

According to ISO, organizational culture is a set of: "Collective beliefs, values, attitudes, and behaviours of an organization that contribute to the unique social and psychological environment in which it operates," (ISO 22316:2017).

It is important to understand the cultural attributes that the organization exhibits. The BCMS may then be designed to leverage the potential opportunities that the organization's culture provides while being aware of, and managing, the potential pitfalls. Understanding the organization's culture may also help identify whether the culture might need to be influenced to encourage personnel to better embrace BC.

Process

The following steps assist in understanding organizational culture:

1. Identifying parties interested in BC within the organization. These could be risk or governance leads, individuals who are part of the risk or audit committee, internal auditors, senior leaders for priority business units, existing BC champions or advocates.

2. Determining the most effective way to engage with interested parties through emotional intelligence. This will lead to understanding their key interests, priorities, and communication styles.

3. Identifying key sources of information on core values, purposes, beliefs, and communication styles. These may include reading the mission statement, annual reports, corporate social media accounts or newsletters.

   In this regard, the following questions might provide further help in understanding organizational culture:

   - How does the organization present itself? What does it stand for?
   - What is the organization's mission?
   - Do they have an active presence on social media?
   - What methods of communication do they use for internal messaging? Some examples may include social media channels, collaboration platforms, posts, and newsletters.

4. Analysing how the organization has responded to incidents, including crises and disruption.

   The following questions might help better understand the quality of the response:

   - What was the tone and frequency of the messaging?
   - What was the communication style (both spoken and written)?
   - To what extent and how did the organization assist those impacted?
   - How transparent (within the boundaries of privacy and confidentiality) was the organization in providing explanations of the incident?
   - Did the organization take responsibility for the incident?
   - What was the timing of the response? Could it be described as 'prompt"?
   - Was the response in the best interest of the organization and its interested parties?
   - How dedicated/collegiate were the teams that responded to the incident?

   It should be noted that analysing the response to previous incidents helps understand the general culture of the organization as a whole as well as providing specific insights on the internal BC and resilience culture.

Methods and Techniques

Having identified interested parties, communications channels, and initial sources of information, the BC professional can proceed to further analyse organizational culture.

The following steps will assist in understanding organizational culture:

Study the operating context and environment. This includes looking at external factors such as the organization's sector, regulators, and legal obligations; and internal factors such as corporate structures, governance, and sub-cultures.

Dialogue with the network of people and stakeholders who have an influence on BC. This will help BC professionals understand similarities and differences in culture, behaviours, values, and beliefs.

Assess communication styles across the organization, looking at how people communicate. This will highlight areas such as the quality of the relationship between personnel and top management, how easy it is to feedback across different organizational levels, and how open management is to challenge.

Evaluate how decision-making takes place at various levels of management. Is input from across the organization welcomed and how are decisions actioned?

Consider top management's approach to prioritisation and conflict resolution.

Analyse employees' working preferences: do they prefer working in groups or individually? Look at organizational groups and networks to understand levels and robustness of cross-functional collaboration. Look for signs of problematic behaviours: such as a blame culture, bullying, or discrimination.

These methods and techniques may assist in understanding the culture model existing in the organization. This should highlight some of the potential advantages and challenges that could be faced when implementing a BCMS. Being aware of the organizational culture will help you develop an approach to BC that complements the elements of corporate culture. It will also allow for changes that would support the organization to better embrace BC.

The internal network of key figures, facilitators, and champions may provide a significant contribution to the successful embracing of BC. Organizations that have champions in related management disciplines (e.g. risk management, information security management, etc.) offer the opportunity for champions to collaborate.

Champions may also provide ongoing feedback as the BCMS is progressing, identifying where the programme is clashing with organizational culture and suggesting revisions. Champions may contribute to organizational change and to influencing culture, which leads to fit-for-purpose BC and greater support for the BCMS.

Understanding BC Culture

General Principles

Understanding the internal BC culture is an essential part of ensuring that prioritised activities become resilient in the event of a disruption. BC culture means that continuity forms part of the operational fabric of the organization. It requires a collaborative approach embraced by all and demonstrated by top management and other key figures.

Concepts and Considerations

BC culture means a shared understanding of why BC is a priority for the organization. It should involve everyone in the organization, not only BC professionals.

The behaviour, attitudes, and beliefs of personnel are indicators of the level to which the organization is Embracing BC. An organization that embraces BC will operate a more sustainable BCMS.

Conversely, a lack of commitment, especially from top management, will ultimately result in poor execution, lack of corporate involvement, and an ineffective BCMS. In achieving full commitment from personnel, top management must demonstrate clear support towards the BCMS and its related activities.

The following represent indicators of an executive management Embracing BC:

- **Commitment:** top management address BC as a priority, setting the tone for the rest of the workforce.
- **Communication:** top management enable personnel to feel comfortable engaging with management about concerns that may impact the organization's BC.
- **Support:** top management promotes BC learning and awareness initiatives where personnel routinely look for and implement ways to improve BC. When incidents occur, organizations ensure that they learn from them and that appropriate measures are in place to prevent reoccurrence (PP6).
- **Engagement:** top management ensure that the workforce is actively engaged in BC activities by setting an appropriate level of priority.
- **Alignment:** BC underpins the organization's objectives.
- **Strategic planning:** BC is part of the organization's strategic planning and is integrated into business decisions. For example, BC requirements are considered as part of supply chain management and the procurement process, or new products and services include BC considerations during the planning stage (e.g. analysing the impact of opening a new facility in an area subject to natural disasters).

Methods and Techniques

The following indicators will assist in understanding the organization's BC culture.

This will contribute to understanding the extent to which personnel are Embracing BC:

1. The BC policy is approved by top management, setting out why BC is essential. The policy sets out organizational aims, principles, and approach to protecting the organization from disruption and for meeting the needs and expectations of its communities of interested parties (PP1).
2. There is BC accountability within the organization, for example, by setting BC objectives for personnel and ensuring sufficiently trained resources are allocated to accomplish those objectives.
3. BC awareness activities refer to material containing previous disruption cases, statistics on disruptive events, and thought leadership pieces on the subject, thereby reminding personnel of the importance of BC. Such knowledge may be shared through awareness campaigns, policies, posters, industry publications, and industry initiatives such as the BCI Business Continuity Awareness Week (BCAW).
4. BC is included in the induction processes while regular training is provided to existing personnel to gain and further develop their understanding of BC through a series of techniques, including class training, policy refreshers, and e-learning.
5. Training courses, such as the CBCI, are available to BC professionals and individuals with BC roles and responsibilities.
6. The organization's BC maturity is subject to periodical assessments, with the identification of areas for improvement through annual assurance plans, maturity reports, and surveys.

If the extent to which the organization embraces BC is not considered sufficient, the role of the BC professional is to find ways to promote and influence the organization to embrace a BC culture.

Improving the Organization's BC Culture

Introduction

Insights regarding the organization's BC culture will enable the BC professional to estimate the gap between the existing and desired level of Embracing BC. Based on this, the BC professional may set an achievable timeframe to implement initiatives for influencing personnel to better embrace BC.

The progressive growth of commitment will depend on the style, messaging, and delivery channels, which should suit the culture of the organization. As with other stages of the BCMS, Embracing BC will need to be monitored over time to confirm that it is evolving. For organizations with a large BC culture gap, the approach is to start with the basics. Initial messaging should focus on the purpose of BC and who or what needs protection from operational disruption. This should then evolve to more advanced tips and topics over time.

General Principles

Understand the Context and Culture of the Organization

Successful awareness strategies in a large enterprise might not work in a small to medium-sized organization. Similarly, strategies that work for one sector might not resonate in another one. Therefore, understanding your organization's culture and appropriately building your awareness strategy is critical.

This operates at two levels:

- **Organizational:** identify what drives the organization (for example, the mission or the external stakeholders).
- **Individual:** identify leaders.

Focus on What Adds Value

It is essential to focus on what matters to the organization's interested parties, including personnel, or they will struggle to see the value in Embracing BC and the culture will remain stagnant. It is also important to highlight the importance of not losing valuable processes and missing key objectives due to disruptive events, leveraging this not only as a risk but also an opportunity to gain a competitive advantage by increasing the ability to remain operational in the face of a disruption.

Identify the Channels for Delivery

People have different learning styles and preferred ways of receiving information. Therefore, it is important to offer education and awareness via appropriate channels using the various methods and techniques. BC professionals should be mindful of different learning needs, time constraints, and working arrangements when delivering education and raising awareness. For instance, if a part of the workforce operates remotely, these activities will have to be performed through online channels.

Methods and Techniques

There are a variety of methods that may be undertaken to achieve commitment, articulate value, and improve culture. Therefore, the BC professional should consider implementing more than one method to maximise coverage across the organization. The following five methods offer various techniques to provide a blend of approaches to influencing personnel to better embrace BC.

Executive Sponsorship and Support

The BC professional should establish a good working relationship with senior and top management. Ideally, the BC professional should regularly meet (for example, quarterly) with the leadership team. This provides a forum for reporting on BCMS progress, benefits derived over the previous period, and indicators where requested leadership support would improve BC and cultural change or resolve roadblocks limiting such improvements.

Build Relationships and Gain Allies

As the organization's BC culture matures, its values and objectives should progressively align with what matters most to interested parties. This helps create and strengthen relationships and raise awareness. Interested parties will recognise and appreciate everyone working towards a common goal and, in response, they will be more likely to become allies. The implications of disruption and the inability to meet the needs of interested parties provide tangible proof of the importance of BC. This perspective can be included in various discussions and awareness sessions to help personnel better understand the need for BC.

Collaboration with Other Disciplines

Collaboration with other disciplines is at the heart of organizational resilience. According to international standards, such as ISO 22316:2017, different management disciplines should provide their contribution and work in a harmonised way. One such example would be to consult and collaborate with the risk management function regarding the risk register. This will help the BC professional gain a better understanding of the threat landscape and of those events that could interrupt prioritised activities and hinder organizational goals and objectives, thereby affecting all interested parties. The BC professional might also collaborate with other related functions such as information and cyber security, corporate security, health and safety, crisis management, and logistics.

Programme Marketing

This is often overlooked but it may be the most beneficial action to add value and improve culture. The key is to regularly provide the organization with meaningful content on BC in an easy-to-digest format, with tips, techniques, and tools to enhance resilience.

Some examples include writing a resilience blog, posting short videos on the organization's intranet, posting messages on electronic video boards, running competitions, and leveraging BCI material (especially during industry events, such as BCAW). Coordinating with the people and culture department can also be beneficial to raise awareness and use well-established communication channels. Most of all, it is important to be consistent. Even if positive feedback is not immediate, BC professionals should keep working on raising awareness, as change will happen over time.

It is also useful to leverage new or existing industry material such as research reports, white papers, webinars, and case studies to show the threat landscape and the value that BC brings in allowing the organization to stay operational in the face of a disruptive event.

Establishing Targeted Training and Awareness Initiatives

Raising awareness within the organization to embrace a lasting BC culture requires personnel to be aware of the BCMS and their role. Where a strong BC culture is not present, the effectiveness of embracing initiatives will be measured by how personnel change their behaviour and attitude towards BC and commit to implementing a BCMS.

Examples of how to improve BC culture include:

- Induction awareness for new personnel. Helping beginners understand BC is vital and it can be achieved through awareness sessions that may take the form of short briefing documents or e-learning courses with core BC principles and values.
- Ongoing training for those who have a role in BC. Personnel need to stay engaged and aware of new initiatives through continual education, based on fresh content that can keep people engaged and interested.
- Include a short educational and awareness section at the beginning of each BC activity. For example, prior to the BIA workshop explain the context of the BIA and its importance in defining BC requirements. Similar educational inclusion may be introduced in other activities such as strategies, plans, exercises, and management reviews.

Table 4: changes that Embracing BC can bring about.

Before (when BC is not well embraced)	**After** (when BC is embraced)
Insufficient priority	Activities are given appropriate priority across the organization, resulting in regular updates to all documents.
Lack of interest/ commitment	Tasks are completed on time and those involved willingly produce a reasonable product.
No ownership	There is executive sponsorship of the programme with an adequate budget. Adequately trained resources are dedicated to the tasks at hand.
Low attention to detail	Plans are thorough and complete, with regular updates and improvements made.
Corners are cut	The entire programme is fit for purpose and is adequately sized for the organization.
Reviews and learning are limited	Lessons-learned meetings are conducted and areas requiring improvement are identified with owners. Resources are committed to improvements.
Not understanding the true benefit of BC	Key interested parties recognise areas where BC adds value to their operation and the sustainability of critical functions.

Measuring the Organization's BC Culture

General Principles

It is essential to understand and measure the personnel's values, beliefs, and attitudes towards BC. A strong BC culture delivers fit-for-purpose BC capabilities. This positively influences the response behaviour during incidents and crises and helps limit the consequences of disruptive events. Establishing a strong BC culture also supports a better alignment to expected outcomes, improved decision-making, and recovery performance.

Since understanding culture helps shape organizational behaviour, any measurement of BC culture can be considered a lead indicator for improvement.

Measuring BC culture should be approached through appropriate methods. Too often, measures are subjective, intangible, and not easy to quantify.

Concept and Considerations

Measurements of BC culture provide insights into how well personnel have embraced BC. When an organization embraces BC, personnel tend to be more engaged in BC activities such as recovery, setting priorities, and following BC plans and procedures to deliver fit-for-purpose BC outcomes.

The methods for measuring BC culture should be easy to perform, non-judgmental, and not intimidating to the participants. It is suggested to design these methods into day-to-day operations, as well as dedicated BC activities, such as workplace recovery tests and exercises, BC reviews, and audits.

For example, while performing workplace recovery exercises, one of the measures could focus on priority assignments by various teams. This measure may help assess behavioural consistency (or variations) among response team members while assigning recovery priorities among personnel.

It is best to plan for multiple measurement methods and aggregate them. Such aggregation may help analyse the overall BC culture, reducing bias or errors from isolated methods.

Process

BC professionals should establish a formal process to measure BC culture, inclusive of the following factors:

- **Who** is the target audience for the final output or for whom are we doing this? (e.g. leadership teams, functional teams, BC participants, etc.).
- **What** are we going to measure?
- **When** are we going to do the measurement? This could include both timing (e.g. when during the year) and frequency (e.g. annually, quarterly, etc.).
- **Where** are we going to do the measurement? This could include all of the organization vs selected parts, and it should be determined whether this will be collected directly from individual employees (e.g. surveys) or indirectly (e.g. extracted from data that has been previously collected at other times).
- **How** are we going to do the measurement? This should include both how the information will be collected (e.g. surveys) and how it will be assessed (e.g. simple data points, pivot tables, pareto charts, etc.).

Methods and Techniques

Designing the appropriate methods to measure BC culture is highly contextual to the organization. One or more of the methods provided below or similar proven methods could be selected. The measurement activities may be carried out independently or they may be integrated into other BC or regular organizational tasks, such as tests, exercises, simulations, and training. For example, when planning for an organizational or operational change, it might be useful to document alternate plans for meeting the desired outcome in the case of unexpected developments. This would help integrate BC thoughts into day-to-day tasks.

The BC professional should periodically engage with top management to share the results of the BC culture assessment. This serves as a basis to discuss initiatives for pursuing the desired level of BC culture. In addition, the organization might perform 'before' and 'after' assessments to review the initiatives employed to establish a BC culture. Finally, periodic assessment may help understand the progressive improvement of Embracing BC over time.

The following methods measure BC culture. While considering a method, it is essential to consider the organization's readiness and operating context. Some methods could be specific to a context or targeted at a particular audience, such as senior and top management. Some methods might require a certain level of BC maturity and culture as a prerequisite.

Behavioural Consistency

This method seeks to strengthen specific continuity behaviours when subject to similar scenarios. For example, people safety must be given utmost priority in emergency incidents. This idea may be reinforced to improve behavioural consistency by facilitating simulation exercises across the organization that includes the potential for physical or emotional challenges. The objective is to confirm consistent behaviour in the same or similar situation across the breadth and depth of an organization.

Training Hours

The organization may offer a set number of hours for BC training, encouraging personnel to participate. Training could be in the form of external courses, conferences, and seminars. These types of activities benefit both BC knowledge in those participating and the overall organizational BC culture.

BC Awareness

This method may measure outcomes or just the frequency of initiatives. Metrics could include the percentage of personnel that has completed a set activity and the number of engaging events like competitions, games, and simulations.

Culture Index

A periodic measure to check what percentage of the organization is covered by various BC culture initiatives. However, the coverage is not a complete measure and may be combined with other measures like the BC pledge.

Unstructured Observations

BC teams may participate in day-to-day meetings, team reviews, and planning meetings to check if continuity risks are being considered and responded to in the form of alternate plans. For example, in a project planning meeting, the project manager can ask, "If key team members are not available for 30 days, what is the plan?" Or, "If a supplier is not able to supply in time, what would we do?" As with all other methodologies, this cannot work as standalone measure; rather, it can complement the data gathered through a range of techniques.

Pre-mortem Checks

The method may apply specifically to the continuity planning stage. The method explores the possibility of failed outcomes during the plan writing stage. For example, the facilitator can pose the scenario: "The plan currently describes the steps for engaging an alternate freight logistics company to deliver raw material by road to our manufacturing plant, when our contracted freight supplier is disrupted. However, consider the scenario of a fuel contamination crisis that has impacted the whole road transport sector, which makes the current strategy ineffective. Can we include other strategies and solutions in the plan, such as freight by rail?"

BC Pledge

The organization may urge personnel to commit themselves to the continuity objective. A measure can then be implemented to periodically check the percentage of people that have committed themselves to BC efforts. The BC pledge can be part of an induction programme for new personnel, suppliers, partners, etc. For example, an organization may ask personnel to sign off their commitment to BC as part of periodic declarations and measure compliance. This approach will help build awareness and familiarity with the BCMS.

Document Integrity

An organization may insist that personnel include continuity briefings as part of every decision regarding high-value areas or functions. The measurement may be based on a percentage of corporate documentation to include a continuity component.

BC Idea Count

Organizations should encourage personnel to generate continuity ideas to overcome common, recurring issues. Ideas can be gathered in a suggestion box or digital portal. For example, an organization may request personnel to email a near-miss for all physical and cyber security related incidents and how they were avoided. The resulting database will create a diverse library of ideas to incorporate into the BCMS and will also show a rate of suggestion flow which can be measured against corporate penetration testing showing engagement. The measurement can be around the number of ideas generated, analysed, and implemented.

Supply Chain Alignment

This targets critical suppliers and can use one or more of the methods listed here. Note: this may only be feasible where there is a strong, trusting, and mutually beneficial relationship between the organization and the supplier.

Outcome and Benefits of Embracing BC

Embracing BC is about strengthening the relationship between the organization and its internal and external stakeholders. It is important that everyone understands the importance of staying operational in the face of disruptions, so that they work for the collective good.

This is a powerful and important relationship that demands protection from disruption.

Only when employees believe in the benefits of BC can the organization be supported by sound response and recovery capabilities, underpinned by procedures executed by competent response and recovery team members. The level of quality and the extent to which BC is fit for purpose is directly related to how much the organization has embraced BC. The BC call to action requires everyone across the organization to proactively monitor and support the BCMS.

The BCMS, as described in the GPG, provides many opportunities for increasing awareness. Each PP includes opportunities to raise awareness with participants at all levels of the organization. For example, the first few minutes of every BC workshop and presentation are an opportunity to reconnect each participant to the organization. It is also an opportunity to support interested parties to move towards BC. Those with no BC responsibility or who have no participation in the BCMS also need to be reminded of why the organization requires protection from disruption and what benefits their contribution to the BCMS will deliver.

This is not an easy endeavour because it requires cultural change, time, and patience.

However, when there is an effective and balanced BCMS, the outcomes will be:

- A programme that is bespoke for every organization, taking into account its organizational culture.
- A policy engaging emotional intelligence and empathy to not lose sight of the pragmatism required for a holistic BCMS.
- Complimentary processes in place to embrace the scope and policies across the entire organization, not because they are mandatory but because it is universally agreed to be the correct and proper course of action for the benefit of the organization.

Remember to ask: who are our stakeholders and why do they need us to have BC?

BCI Professional Practices

PP3: Analysis

Analysis is the PP that contains the two techniques used for analysing BC requirements: the business impact analysis (BIA) and the risk assessment (RA).

The BIA defines the impacts of disruption over time to determine the organization's response, recovery priorities, and resource requirements, namely the BC requirements. The RA identifies the disruption risks to the organization's prioritised activities and required resources. The BIA is the foundation for designing effective recovery strategies and plans. The outcome of the BIA and the RA is an input to the strategy design stage of the BCMS. Therefore, the quality and results of the BIA and RA process and its outcomes are extremely important.

Introduction

The BCMS uses two organizational analysis techniques, the BIA and RA. The BIA estimates the impacts of disruption over time to determine the organization's response, recovery priorities, and resource requirements, namely the BC requirements. The RA identifies the disruption risks to the organization's prioritised activities and required resources. The BIA is the foundation for designing effective recovery strategies and plans. The outcome of the BIA and the RA is an input to the Solutions Design (**PP4**) stage of the BCMS. Therefore, the quality and results of the BIA and RA process and its outcomes are extremely important.

The outcomes of the BIA and RA process are dependent on the organization's understanding of the following:

- The external environment, inclusive of the priority suppliers and the statutory and regulatory bodies in which it operates.
- The internal operating environment, inclusive of business processes, activities, and resources, as well as the potential impacts caused by disruptions to the delivery of products and services. In organizations operating within a non-commercial environment, the customer can be the public or an overseeing authority, such as the government (ISO 22317:2021).

The outcomes of the BIA and RA also highlight inefficiencies and risks, as well as gaps for top management to address or accept. Outcomes provide opportunities for collaboration between related management disciplines to contribute to and strengthen the resilience of the organization.

Business Impact Analysis (BIA)

General Principles

The BIA is the technique used to define the impact of a disruption over time.

By performing the BIA, the BC professional determines the following:

- The prioritised activities, and
- The recovery timeframes and resource requirements.

As described in PP1, the organization aims to meet the requirements of the predetermined and documented BCMS scope that takes into consideration products and services.

There are three types of BIA:

1. **Product and service BIA**: identifies and prioritises products and services.
2. **Process BIA:** determines the process or processes required to deliver the organization's prioritised products and services. Process-driven organizations, such as manufacturing, will typically perform the process BIA. Less process-focused businesses can omit it and move on to the activity BIA.
3. **Activity BIA:** identifies and prioritises the activities that deliver the most urgent products and services and determines the resources and dependencies required for the continuity of these activities.

Many approaches can be followed to conduct a BIA. Organizations do not have to undertake all three BIA types. They can choose to use them individually or in combination to find the most appropriate BIA approach, according to the size, complexity, and type of the organization and the scope of the BCMS. While the process BIA is applicable for process-driven organizations (as explained above), it is optional for others. Large organizations can do an activity BIA separately, while small organizations can combine it with a product and service BIA.

The BIA considers the products and services of an organization as well as those processes and activities, including resources and dependencies, that ensure the delivery of said products and services. The different types of BIA provide greater levels of detail and understanding about the organization and cover the entire BCMS scope.

The BIA is not a one-time or single-stage activity. Initially, it can help clarify the scope of the BCMS, after which it becomes an integral part of the ongoing BCMS, typically reviewed periodically (for example, annually) or in the event of significant organizational changes in the operating context or environment. The technical specification ISO TS 22317:2021 is a good reference guide for further details on conducting the BIA.

The BIA process aims to:

- Identify legal, regulatory, and contractual requirements.
- Assess the impact over time of a disruption on the organization.
- Identify the timeframes for the maximum tolerable period of disruption (MTPD).
- Set the recovery time objective (RTO) for the prioritised activities.
- Identify resources needed to perform prioritised activities following a disruption.
- Set the timeframes for the recovery point objective (RPO) regarding data and information.
- Set the minimum business continuity objective (MBCO) for the minimum level of products and services that is acceptable to the organization.
- Identify dependencies, including suppliers, partners, and other interested parties.
- Identify the interdependencies of prioritised activities.
- Reassess and validate the scope of the BCMS.

Process

The BIA process involves the following steps:

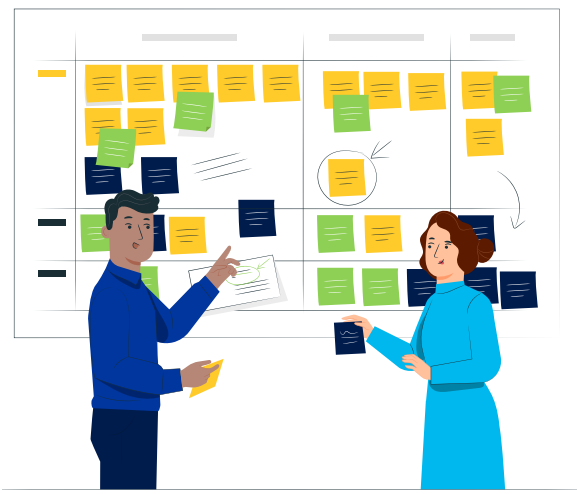
1. Reviewing the context and scope of BIA – strategic in nature and approved by top management.
2. Assigning BIA roles and responsibilities within the organization to enable the process to operate smoothly.
3. Creating a BIA implementation plan, including the approach and methodology for conducting the BIA. A consistent approach to performing the BIA should be used throughout the organization. The process can be scaled to suit each organization and might be reviewed after the BIA stage is completed or as part of the management review at the end of the current BCMS cycle. The method used should be robust enough to ensure that the information collected is consistent and impartial.
4. Determining priorities of products and services and the associated activities of the prioritised products and services. The priority of prioritised processes will only need to be determined for process-driven organizations, where a process BIA is done. The types of impact considerations to determine these priorities could be financial, reputational, legal, customer, health and safety, operational, regulatory and any other impact depending on the nature and type of the organization. It must be considered that the impact from disruptions can come from within the supply chain or other external sources. For consistency in approach, the BC professional might define impact thresholds or use an impact type matrix to determine the RTO and MTPD.
5. Determining the resources required for continuity of activities following an incident, as well as all other dependencies and interdependencies.
6. Performing a final analysis to consolidate BIA results.
7. Obtaining top management approval for BIA results. Determining impacts over time should demonstrate to top management how urgently the organization needs to respond to a disruption.
8. Including a periodic review of the BIA as part of a continual improvement strategy.

The terminology used in the BIA by an organization is not as important as understanding when the disruption will result in unacceptable impacts. The words 'priority', critical', and 'key' are often used interchangeably to describe the products and services, processes, activities, and resources required following a disruption. These words are often understood as meaning 'important'. However, this can lead to misunderstandings and exaggerations when collecting information for the BIA. Therefore, it is recommended that these terms are replaced with 'prioritised activities'. These are defined as an: "Activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption," (ISO 22301:2019).

Roles and Responsibilities

Various personnel and teams must play their part to ensure that the BIA process meets its purpose.

- **Top management:** for ensuring commitment to the process, allocating competent resources, providing financial approval for costs, and communication within the organization.
- **BC professional:** for preparing, planning, managing, delivering, and ensuring consistency throughout the BIA process. The BC professional plays the key role and co-ordinates across teams and levels.
- **Activity owner:** for providing all the necessary information for the BIA, including the resources required, any workarounds, known dependencies, etc.



Methods and Techniques

The methodology and the information collection methods used for conducting the BIA should be agreed in the planning stage and reviewed regularly. Methods used to conduct the BIA vary from one industry sector to another and from one organization to another.

Depending on its size, complexity, and type, an organization may choose to combine the different types of BIAs. For example, an organization may conduct one BIA, combining the product and services, process, and activity BIAs, while others may conduct individual BIA categories or combine results as required.

Whichever approach is taken, the information must be recorded in the same way.

Methods and techniques used to collect the BIA information include:

- **Workshops:** collecting information from individuals and teams in person or virtually. This also provides an opportunity to raise awareness and improve the BC culture (PP2). Interdependencies can be identified, issues can be raised, and solutions explored. This method delivers higher quality results because it provides a forum for discussion. Workshops will require some preparation time prior to the event.
- **Surveys/questionnaires:** collecting information from individuals or teams by paper or electronically. They can be designed to gather detailed information and generate a large amount of information if the questions are well written and easily interpreted. Using software to collect and analyse this information electronically is helpful for medium and large organizations. This method can create increased awareness in all personnel and support an enhanced BC culture which can facilitate quality results.
- **Interviews:** collecting information from individuals or teams through interview-based conversations. The BC professional may perform interviews to facilitate discussion regarding BAU operations, resource needs, obligations, and possible impacts if a disruption were to affect the team's capability to deliver prioritised activities and products or services. Interviews often identify risks which need to be captured in the RA. However, this method requires quality execution and adequate time to complete so that people do not impact the results by interpreting the concepts and definitions incorrectly.

Combining the different types of analysis can be a more efficient way to achieve an organization-wide view, provided the combined approach does not make the BIA process complex and challenging.

To prepare effective workshops, surveys, questionnaires or interviews, the BC professional should review all relevant documents to help assess the appropriate parameters and factors required for performing the BIA. Examples of documents to review as part of the BIA may include existing BC information, necessary excerpts from the organization's annual reports, existing department, or business unit plans, legal or regulatory requirements, service level agreements, etc.

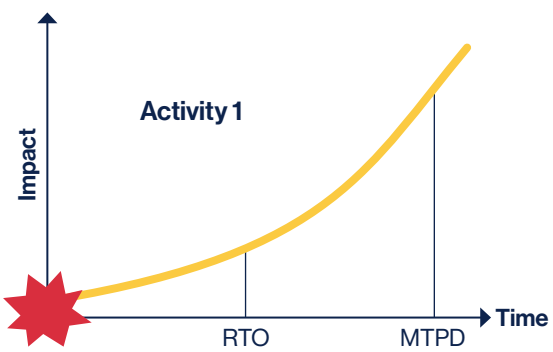
The BIA process can be automated through an internally developed tool or by adopting an external supplier tool, which could ease the collation and assessment process, store the BIA results for reference, and automate reports and analyses. However, using software does not remove the need for workshops, questionnaires, and interviews with relevant personnel.

Also, it is important to consider the following points:

1. For organizations that conduct the BIA for the first time, an initial assessment may be done at a high level that can then be used to develop a system for more detailed BIAs and to clarify the scope of the BCMS. The minimum objective of an initial assessment is to identify the products and services within the organizational structure.
2. There are generic processes which run across the whole organization, such as people management and business management, which have common requirements and dependencies. Capturing these centrally can save time in multiple BIA workshops and can ensure consistency when identifying RTOs and MTPDs.
3. It is important to identify processes that operate only during a crises or business disruption, such as 'crisis management support' or 'regulatory reporting'.

Evaluating Impacts to Determine the MTPD and RTO

The BIA information collected should include all in-scope products and services, processes (if included in the BCMS Scope), and activities which are to be prioritised by determining the MTPD and RTO.



Some factors (e.g. impact types) that should be considered when estimating the MTPD and RTO of a disruption to a product or service delivery include, **but are not limited to:**

- Loss of financial value or viability (e.g. in the short or long term).
- Damage to reputation or interested-party confidence.
- Breach of legal or regulatory obligations.
- Failure to meet the business objectives of the organization.
- Loss or impact to people/personnel or management efforts.

The timeframe of the MTPD and RTO varies across industries and sectors, depending on the nature of the business and the magnitude of impact over time and can be estimated in minutes, hours, days, weeks or even months.

When assessing an impact over time, a worst-case scenario should be considered (i.e. the disruption happens at the worst possible time for the business). For example, a systems outage for a bank's payment processing department during the regulatory cut-off time, which could potentially lead to regulatory impact and financial loss. When considering the impact over time, the timeframes can be grouped into ranges to simplify the analysis (e.g. 1-4 hours, 4-12 hours). In some organizations, impacts may reach unacceptable levels within minutes, whereas in others an organization may not experience unacceptable consequences for several days following a disruption. For example, a hospital may have a timeframe range of minutes, while a government policy department may have a timeframe range of a week. It is not advisable to break the time ranges down too finely, as that can mislead the estimation of impacts and generate excessively detailed data.

Examples of the type of impacts over time include:

- Breaches of legal or regulatory requirements, such as fines and reputational damage resulting from a failure to settle share trades within the required time frames.
- Financial impacts, for example, loss of sales income or cash-flow problems caused by delayed payments, resulting in penalties from contractual breaches.

The duration or lead time of the activity delivering the product or service may be a significant consideration in the MTPD estimate. For processes or activities that take significant time to deliver their output, assumptions may have to be made when setting the MTPD. The organization should consider at what point during the activity the disruption occurs and how much of the activity needs to be repeated.

The following table is an example of MTPD thresholds for certain impact types. **The MTPD describes the unacceptable outcome of a disruption – one that places the organization at the point of failure:**

Table 5: MTPD thresholds for certain impact types.

Impact type	Description	MTPD threshold
Financial	Financial losses due to fines, penalties, low profits, etc.	Loss greater than [x]* value in fines, costs, and revenue.
Reputational	Negative news causing damage to brand.	A viral negative news story on social media.
Regulatory	Regulatory censure, fines, criticism.	Regulatory breach threatening revocation of operating license.

***[x] Refers to the financial value that the organization can define based on its risk appetite or industry practice.**

The aim of BC is to ensure that the organization's products and services are restored before the MTPD is reached. The BIA identifies and sets the RTO for prioritised products, services, activities, and resources so that the organization can develop and implement BC strategies and solutions supported by plans, used by competent teams of people, that avoid reaching the MTPD. The RTO should always be less than the MTPD. Where activities and resources support multiple products and services, the shortest time requirement of these products and services is the RTO.

The development of BC requirements should consider more than just the RTO. The BIA should also determine a minimum capability level at defined points of time. One common term used to describe this capability is the MBCO. The MBCO should be achieved at a specific time, either at or after the RTO. Setting several MBCOs for different times after a disruption and for each product group may be appropriate. Where MBCOs rely on outsourced service providers, the objectives should consider service level agreements and any legal or regulatory requirements.

The Product and Services BIA

General Principles

Products and services are defined as the: "Output or outcome provided by an organization to interested parties, e.g., manufactured items, car insurance, community nursing," (ISO 22301:2019).

It is top management's responsibility to ensure that priorities are assigned for products and services.

This is because top management have the following duties:

- Setting the objectives of the organization.
- Holding the ultimate responsibility for ensuring continuity of the organization and the fulfilment of its objectives.
- Adopting the broadest view of the entire organization from which to assess priorities.
- Choosing to override contractual and other obligations when setting priorities in exceptional circumstances.
- Being aware of planned future changes and other factors which can affect the BC priorities and requirements.

This type of BIA prioritises products and services and can also be used to confirm or modify the scope of the BCMS. A product and services BIA can be used to determine the impact of a disruption pertaining to significant changes or developments within the organization, **such as:**

- Introduction of a new product or service.
- Retirement of an existing product or service.
- Relocation or a change to the geographical positioning of a product or service.
- A significant change in business operations, structure, or personnel levels.
- A significant new supplier or outsourcing contract changes.

The product and services BIA should enable the organization to take advantage of any changes to improve its BC capability and build organizational resilience. An organization may decide to restrict the scope of the product and services BIA to the higher priority products and services.

This focus on higher priority products and services can be used to make changes manageable and more cost-effective.

Process

The product and services BIA process involves the following steps:

1. Collecting the information necessary to perform the product and services BIA from interested parties, such as top management or product owners.

   Such information may include:

   - Mission, objectives, and strategic direction of the organization.
   - The BCMS scope.
   - Legal and regulatory requirements to which the organization or specific products and services are subject, as well as an assessment of the impact of breaching each requirement.
   - Contractual requirements, including penalties for failure to deliver products and services.
   - Expectations of customers and other interested parties.
   - An assessment of the impacts of failure to deliver.
   - Lessons learnt from past disruptions and exercises.
   - The potential impact of significant developments within the organization or its operating environment.

2. Defining timeframes based on impact types, criteria, and the agreed methodology, estimate the MTPD and RTO for each product or service group.

3. Listing the products and services sorted by priority and their continuity requirements, which are then used for process/activity BIA.

4. Obtaining top management approval and sign-off on the list of prioritised products and services.

The Process BIA (optional)

General Principles

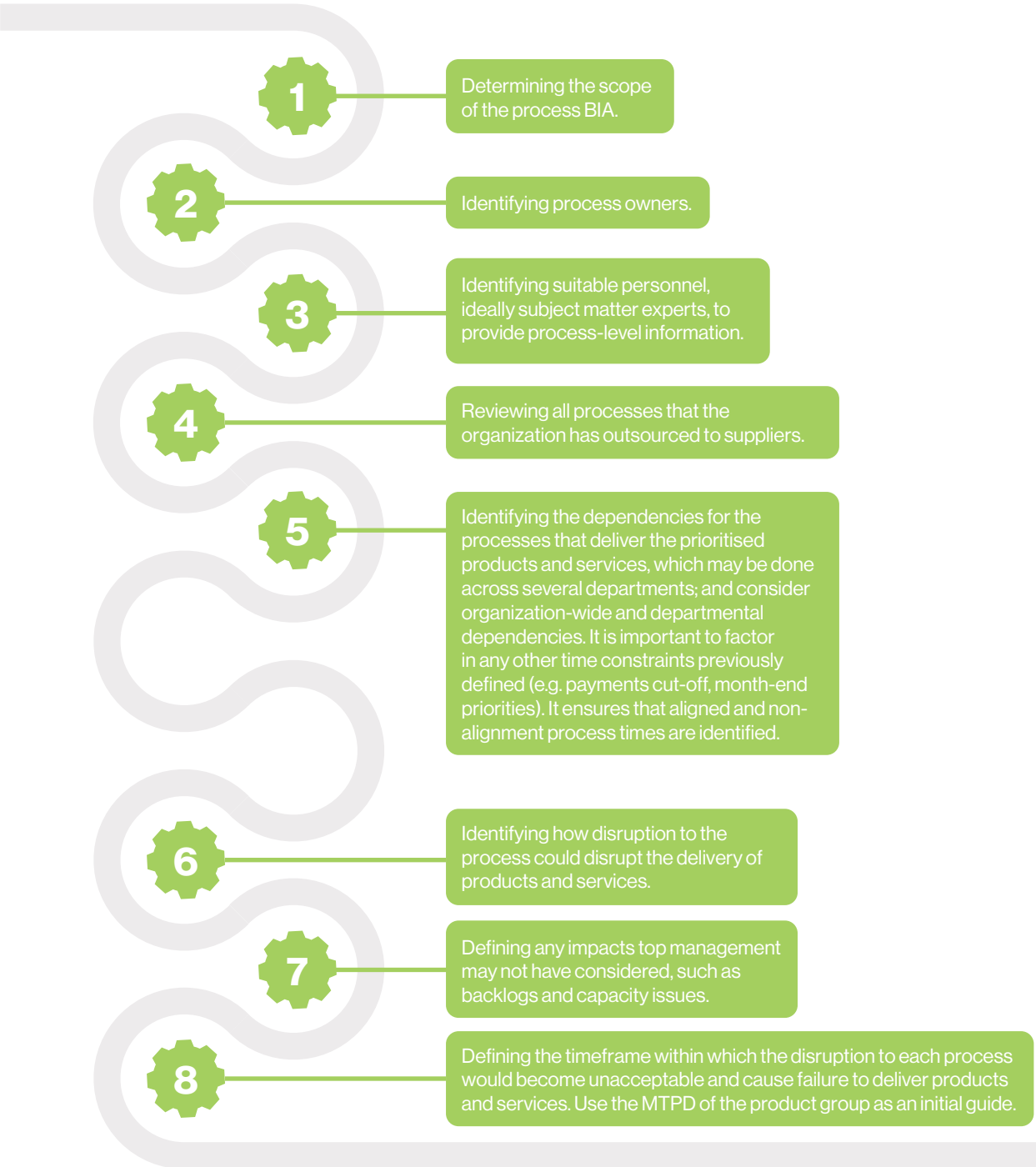
A process is described as: "A set of interrelated or interacting activities which transforms inputs to outputs," (ISO 22301:2019). A process may be divided into several activities. For example, a process could be manufacturing (from raw materials to finished product), managing investments, or collecting waste. The process BIA is optional since it is generally performed by process-driven organizations, for example, manufacturing. Less process-driven organizations may decide to skip the process BIA and move directly onto the assessment of the activity BIA.

An organization may decide to restrict the scope of the process BIA to processes relating to higher priority products and services, using impact criteria (e.g. impact types) to estimate the magnitude of impact over time to determine the recovery timing of each process. The scope of the process BIA is linked to the product and services BIA scope, which examines the impacts of disruption to one or more product and service groups. It is important to recognise processes which support multiple products and services and to understand the interdependencies between them to ensure the overall BIA does not miss any important elements.

The process BIA will build on the results of the product and services BIA and should also help to verify the outcomes of the product and service BIA.

Process

The process BIA involves the following steps:



9 Ascertaining the process MTPD and RTO.

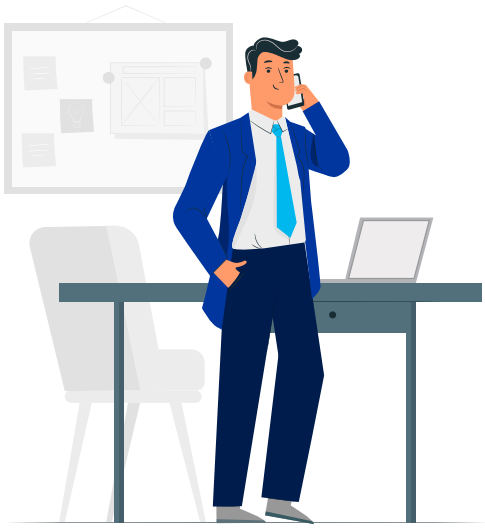
10 Obtaining confirmation from the process owners validating the accuracy of the information.

11 Publishing the results of the process BIA.

Outcomes and Review

The outcomes of the process BIA are:

- A list of processes that contribute to the delivery of the organization's prioritised products and services within the scope of the BCMS.
- The MTPD and RTO for each process.
- Identification of any processes that have been outsourced by the organization and therefore present an increased risk. Service level agreements and more frequent reviews should be considered for these processes. This is an important step in the process BIA and will be of value to the overall programme when considering supply chain resilience.



Activity BIA

General Principles

An activity is defined as a: "Set of one or more tasks with a defined output," (ISO 22301:2019). For example, performing quality control, undertaking home care visits, raising invoices, or answering calls by a service desk.

The activity BIA determines prioritised activities that enable product and service delivery to be resumed at a predetermined timeframe and capacity following a disruption. The activity BIA starts with the activity owners identifying the activities that contribute to each in-scope product and service or process. The objective of the activity BIA is to determine the RTO and MTPD for each activity.

Process

The activity BIA process involves the following steps:

1. Determining the scope of the activity BIA.
2. Identifying the relevant activity owners.
3. **Collecting and analysing the data regarding:**
   - Priorities of the products and/or services that the activity supports.
   - Operational methods or scope of the activity.
   - Fluctuations in demand or peak operating times that could adversely impact the activity.
   - Factors not already discovered that may affect the determination of BC requirements, such as backlogs, legal and regulatory requirements or obligations, and the interdependencies on other activities (internal or external).
   - Legal and regulatory requirements.
   - The activity details and its interdependencies, both internal and external.
   - The duration or lead time of the activity.
4. Breaking down the resources required to maintain the activities at an agreed level and within the MTPD and RTO.
5. Obtaining approval from the activity owner on the accuracy of the data collected. Based on the impact types and criteria, the defined timeframes, and the agreed methodology, activity owners should assess the impacts over time resulting from a disruption, identify the MTPD, and set the RTO for each activity. This capacity can be represented as a metric such as the percentage or ratio of a level of service or quantity of product.
6. Identifying and prioritising the activities, in ascending RTO order, which contribute to the process/es or products and services.

Outcomes and Review

The outcomes of the activity BIA are:

- An approved list of prioritised activities that contribute to the processes needed to deliver products and services.
- Detailed MTPD and RTO and the justification for them, which should determine the timeframe of the solutions for each activity.
- A breakdown of internal and external dependencies, which may include priority suppliers that deliver goods and services.
- Documentation of the internal and external interdependencies for the prioritised activities.

Once the activity owners approve the list of prioritised activities, the strategies and solutions for prioritised activities are determined.

Resources and Dependencies

The activity BIA stage is also where the organization collects detailed information about the resources and other dependencies required to continue activities which support the organization's strategic objectives. Dependencies on external suppliers and outsourced service providers can be further detailed at this level when defining resource requirements. It is usual to identify common dependencies at the activity level that affect most processes, such as utilities.

To identify the resources and dependencies required for the prioritised activities, organizations need a minimum understanding of the **requirements for:**

- **People:** the number of resources needed over time. The activity owners should have an understanding of resource requirements under various scenarios (e.g. the number of resources required for an activity to achieve the MBCO during a crisis).
- **Information and data (vital records):** the RPO of such vital records must also be determined at this stage. "The recovery point objective (RPO) is the point to which information used by an activity must be restored to enable the activity to operate on resumption. RPO can also be referred to as maximum data loss," (ISO 22300:2021). Where some activities cannot tolerate any loss of data, others may be able to operate adequately with some data loss. Very few activities can operate adequately with no data or with data that is not current. It should be recognised that different data users may require different RPO timeframes. The RPO for specific information or data set is the shortest RPO required by all users.
- Buildings, work environment, and associated utilities (physical infrastructure).
- Facilities, equipment, raw materials, consumables, etc.
- Information, IT systems, and applications.
- Transportation and logistics.
- Finance.
- Suppliers and outsourcing partners.

Resources and dependencies also need to consider:

- The location of resources and potential challenges to the provision of recovery strategies and solutions.
- Dependencies on the workforce including, but not limited to, their knowledge of the activity, training, qualifications, authority, transportation, and other logistical concerns.
- Any known single points of failure.

Consolidated Analysis

On completion of the BIAs, a final consolidation of all analysis is conducted to help with the identification and implementation of recovery strategies and solutions. Organizations can choose the appropriate quantitative and qualitative analytical approach, which can be influenced by the type, size, or nature of the organization, as well as resource and other dependency constraints. While the organization may be flexible on the methodology for the analysis, it is imperative that they challenge and ensure that the data collection is credible, complete, reasonable, sufficiently accurate, and justifiable.

The final approval from top management is sought at this stage by sharing the results of the prioritised products and services, including the priority of their related processes (if a process BIA was completed) and related activities. It would be best to document the results in a report or a presentation to top management that **clearly details:**

- The purpose of the BIA and the methodology used.
- The product and services, by order of priority.
- Priority of related activities (and processes if a process BIA was completed).
- The MTPD, RTO, and MBCO for the activities; and RPO for data and records.
- Any specific risks, concerns, or issues identified.

Top management approval should be obtained and retained as per the organization's data retention policy.

The BIAs should be regularly reviewed at pre-defined intervals or following a significant change within the organization or in the external environment in which it operates. The BIA process and methodology should also be reviewed to continually improve its quality and ensure it continues to meet the organization's purpose.

Risk Assessment

General Principles

In the Analysis stage, the BIA is often conducted before the RA so that the organization can just focus on the prioritised activities. This can maximise the benefit of any investment in risk treatments.

The BC professional then uses RA techniques to identify unacceptable risk, single points of failure, and opportunities for continual improvement. Risks are collated by using a scoring system based on the likelihood and consequence of the risk occurring. A risk is defined as: "An effect of uncertainty on objectives," (ISO 31000:2018).

Concepts and Considerations

RAs involve methods to identify, analyse, and evaluate a range of risks relevant to the organization. They use a formula based on likelihood and consequence to calculate a risk score. RA is defined as the overall process of risk identification, risk analysis, and risk evaluation: and it should be conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiries as necessary (ISO 31000:2018).

If the organization has an established risk management function, risk information relating to prioritised activities and their resources may already exist. Hence, BC professionals should collaborate with the organization's risk professionals and have access to the information contained in the organization's risk register. However, having an existing risk management function is not required for a successful RA as part of an effective BCMS.

RA methods can be effective when analysing known and anticipated risks. However, the BC professional should be aware of the limitations to RA techniques when they are being used to evaluate complex and emerging risks and the cause of future disruptions. Estimations based on the likelihood and consequence of a risk occurring are often based on limited or incomplete data sets and historical information.

RA methods typically consider timeframes relevant to the organizational planning process and its business objectives. For example, if an organization uses a five-year planning cycle, the BC professional may want to estimate the likelihood of a risk materialising within that planning cycle.

RAs as part of the BCMS consider the risk of disruption to activities on the organization. The BC professional will benefit from a general understanding of risk management and should use their knowledge of the organization and its operating environment to decide how much time and resources to invest in the RA and the appropriate level of detail for the organization.

Many organizations carry out horizon scanning at pre-defined intervals. Horizon scanning is an activity used to monitor and identify potential risks to an organization and considers current, emerging, and over-the-horizon risks. Information provided by horizon scanning is useful when undertaking an RA as part of the BCMS. In addition, the organization can consider using recognised industry-specific and global risk reports, monitoring services or systems, news websites and social media as part of its horizon scanning activities. The BCI publishes a Horizon Scan Report annually.

RA Process

The key steps when undertaking an RA as part of the BCMS are as follows:

1. **Listing risk sources:** these are the known and anticipated internal and external risk sources for each of the prioritised activities (e.g. regulation, economic, seasonality, competition), which should include the supply chain.

   Organizations may find the following sources useful when performing a RA:

   - Risk sources as identified during the BIA process.
   - Risk sources as identified during previous exercises.
   - Previous incidents experienced by the organization and captured in the risk register or other incident reports.
   - Previous incidents recorded within the industry sector or geographical region.
   - Information or reports relating to threats and past disruptions.
   - Risk sources drawn from horizon scanning activities.
   - Publicly available records about known local, regional, national, and global risks.

2. **Performing a risk source analysis:** organizations must determine the likelihood of each risk occurring and estimate the consequence of each risk source on the organization. Together these may indicate how

fast a risk could affect an organization. Then the score of each risk must be calculated by combining the scores for consequence and likelihood. A risk matrix may be available where impact ratings are grouped into consequence categories that relate to the organization (e.g. financial, environmental, legal, safety, and reputational). Care should be taken to ensure that the consequence ratings appropriately describe the consequences of disruptions.

3. **Evaluating risk:** this step consists in prioritising the risks based on the risk score for the prioritised activities and it comprises the **following activities:**
   - **Identification:** identifying which risks are deemed unacceptable.
   - **Risk treatment:** using the information from the RA process to identify opportunities to mitigate each risk identified by seeking to reduce the likelihood of the risk materialising or lowering the impact of the disruption to the organization. Options for risk treatments will be developed in the Solutions Design stage (**PP4**) of the BCMS.
   - **Risk reporting:** sharing the outcomes with the relevant interested parties.

Tables 6 and 7 are examples of a RA matrix and present a priority thresholds table to assist with developing a risk matrix. In most cases, the organization's risk management framework already has the assessment matrix defined, which is also applicable for BC.

Outcomes and Review

The outcomes from the RA as part of the BCMS are:

- An awareness of the range of risks that could disrupt the organization's activities.
- A prioritised list of risks based on the risk rating.
- Identification of any unacceptable risks and single points of failure.

The RA process can be ongoing, depending on the size, complexity, and type of organization. However, the methods used should be regularly reviewed at pre-defined intervals or following significant change as defined within the BC policy.

Table 6: an example of a RA matrix for impact of disruption.

Impact of disruption	Duration	Financial	Reputation	Health and safety
Note: the impact categories and examples should be specific and relevant to the organization.				
3 - Major	More than 5 days	Over $1m cost/lost revenue	National damage to reputation/customer or community support	Potential for irreversible injuries/fatalities
2 - Moderate	2 to 5 days	$100k to $1m cost/lost revenue	Regional damage to reputation/customer or community support	Potential for serious injuries (hospitalisation)
1 - Minor	Up to 1 day	Less than $100k cost/lost revenue	Local damage to reputation/customer or community	Potential for minor injuries (time-off work)

Table 7: an example of a RA matrix for probability of disruption.

Probability of disruption	3-Likely	2-Possible	1-Unlikely
	Frequent occurence/at least once in 3-year period	Infrequent occurence/ once in 10-year period	Exceptional occurence/once in 30-year period
Combining the probability and impact scores for each threat produces a risk score (high/medium/low).			
3 - Major	High	High	Medium
2 - Moderate impact	High	Medium	Low
1 - Minor impact	Medium	Low	Low

BCI Professional Practices

PP4: Solutions Design

Solutions Design is the PP that specifies how the organization will meet its BC requirements.

The Solutions Design PP identifies strategies and solutions that enable an organization to resume business operations within the approved continuity requirements and identifies capabilities to mitigate unacceptable risks and single points of failure. Strategies outline the high-level approach for meeting the organization's BC requirements. Solutions detail how the strategy will be delivered. BC recovery solutions include approaches, arrangements, methods, procedures, treatments, and actions that can be put in place to implement business strategies with due consideration to the associated costs.

Introduction

Solutions Design is the PP that specifies how the organization will meet its BC requirements.

The outputs are strategies and solutions that:

- Enable the organization to resume business operations within the approved continuity requirements (i.e. MTPD, RTO, MBCO for activities and RPO for data records).
- Identify capabilities to mitigate unacceptable risks and single points of failure.

These requirements are based on the approved outcomes of PP3 (Analysis) and collectively describe how the organization can:

- Protect, continue, resume, and recover prioritised activities.
- Mitigate, respond to, and manage impacts of disruptive events.

Strategies outline the high-level approach for meeting the organization's BC requirements. Solutions detail how the strategy will be delivered. BC recovery solutions include approaches, arrangements, methods, procedures, treatments, and actions that can be put in place to implement business strategies with due consideration to the associated costs.

A strategy should consist of at least one solution and a solution can be used for more than one strategy.

Strategies to Resume Business Operations

The strategies to resume business operations are based on the outcomes of the Analysis stage, which identifies the following:

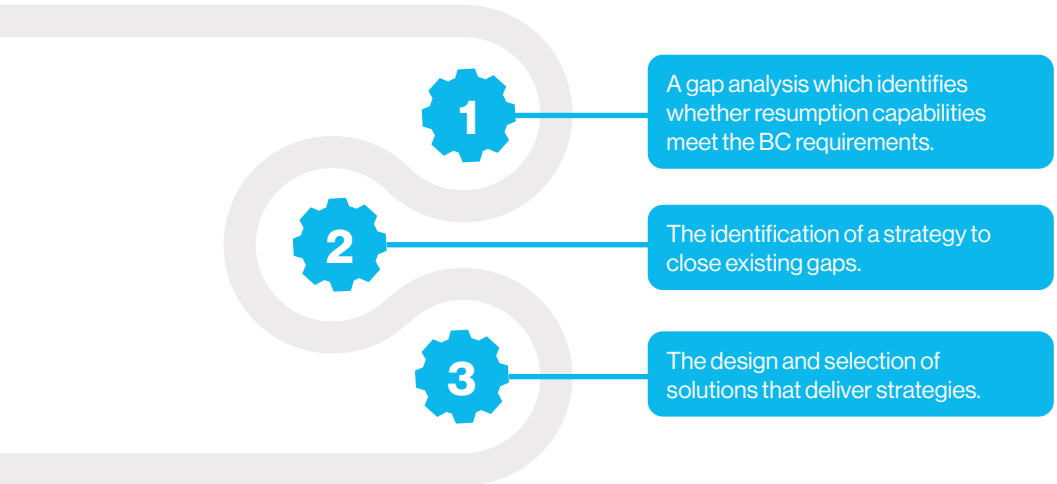
- Prioritised products and services,
- Prioritised activities, and
- The MTPD, RTO, MBCO, and RPO.

Principles and Considerations

Strategies and solutions describe how the organization can resume business operations when disrupted. The identification of solutions must always include a series of considerations that are relevant to the BCMS and the organization as a whole. Solutions must meet the BC requirements but at the same time they need to be considerate of costs and benefits. For instance, the cost of mitigating the impact of a disruption should not exceed the cost of the disruption itself or introduce a secondary risk that negatively affects the organization.

Process

Developing strategies and solutions for the resumption of business operations is **a three-step process which includes:**



The following sections elaborate on the main points included in the **three-step process.**

1. Gap Analysis

The gap analysis aims to establish whether new strategies and solutions are required.

The BC professional will achieve this by meeting with the owners of the relevant products, services, activities, and resources and assessing their levels of preparedness for disruptive events. Relevant information for this activity could be sourced from the documentation obtained in PP3, such as the identification of the owners of products, services, activities, and resources. This can be sequenced by RTO, before proceeding to schedule the meetings.

The owners will then be presented with the BC requirements, including the description of the resources needed and the RTO. It is likely that the BC professional will have already met with some or most of the owners in question during PP3 (e.g. during BIA interviews); however, for those not familiar with the BCMS and its related activities, it will be best to provide some education and awareness.

In evaluating possible gaps, the BC professional should seek confirmation of whether the existing recovery capabilities meet the RTO. This can happen through a review of past exercises, tests, or responses to real disruptive events.

The final evaluation might have three possible outcomes:

- BC capabilities are inadequate and require more investment,
- BC capabilities meet the BC requirements and do not need further investments, or
- BC capabilities exceed requirements and resources could be redistributed to other areas.

The results of the gap analysis should be presented to top management who will provide direction for determining strategies and selecting solutions. In some cases, top management might decide not to pursue specific gaps even though the BC professional recommends new strategies and solutions.

This could occur for a variety of reasons such as:

- Costs being prohibitive.
- Gaps fall within the risk appetite of the organization.
- Impending business changes require caution with investments.

In response, the BC professional may recommend the business pursues adjusted strategies and solutions that partially close the gaps identified in the Analysis phase. Although BC requirements may not be fully met at this time, due to cost or resources availability, a partial implementation may provide an acceptable compromise for the business. In circumstances where gap items are not closed, the corresponding entries in the organization's risk register should indicate the acceptance of an operational risk.

2. Strategy Determination

Based on the requirements from senior management, the BC professional will:

- Group products, services, processes, activities, and resources requiring strategies by owner and prioritising them by RTO.
- Schedule sessions to meet the owners.
- Present the results of the gap analysis to the owner.
- Discuss activities and resources to develop new, enhanced, or alternate strategies and solutions.
- For each strategy option, the owner will consider and document parameters for various solutions to be **defined with:**
  - » A specification (i.e. sufficient detail such that the solution can be implemented),
  - » Advantages and disadvantages,
  - » Implementation time, and
  - » Estimated costs to prepare, implement, operate, and maintain.
- The owner will select the most appropriate solution(s) for each strategy.

3. Solutions Design

Solutions Design requires the involvement of a broader range of personnel than during PP3. As the BC professional reaches out to those who own the resources needed to implement the identified solutions, there will be also an opportunity to raise awareness about BC and strengthen the practice of Embracing BC. Specifically, each meeting on strategy and solutions should start with an overview of BC and why it matters to the organization, for those who are not yet familiar with the BCMS.

Methods and Techniques

Ideally, the pursuit of strategies and solutions should include the objective of providing additional benefit to the organization during BAU, which will be more appealing to top management.

Combining and consolidating strategies will also help maximise investment, as one strategy could support multiple activities or resources; however, this process might be challenging at times and require lateral thinking. It provides greater return on investment when one strategy supports more than one activity or resource. This naturally occurs when considering resource strategies since it is usual for a resource to be required by more than one activity. For example, a strategy to provide software application redundancy by replicating the system at a geographically separate site has an improved cost/benefit when considering that the system supports more than one application, as well as many activities across the organization. Consolidated strategies for activities might not be as obvious and may require some lateral thinking. For example, the strategy of stockpiling equipment for an activity might require the creation of a new storage facility. In such a case, it will be best to use the new facility for stockpiling key items needed for more than one activity, which will improve the cost/benefit ratio of this action.

The BC professional should recognise that, broadly speaking, there are two groups of strategy developers:

- **Activity owners:** have deep knowledge of the process (including both products and services) and are responsible for resuming activities.
- **Resource owners:** ensure the delivery of products and services, are responsible for the repair and replacement of resources, and consider factors such as RTOs, quantity over time, and alternate delivery locations.

It is usual for activity strategies to guide resource strategies and solutions. For example, consider an activity that operates in two cities. Choosing between transferring an activity to a different team or relocating one will have an impact on different aspects, such as people, facilities, logistics, etc.

The BC professional can agree with the activity owner to resort to temporary workarounds. Adopting a workaround consists of a change to the way of operating that provides acceptable outcomes for a limited time. Workarounds are usually not ideal because they tend to be labour intensive, require more time to undertake, or are expensive. However, there are two key benefits.

They:

1. Enable an activity to recover from disruption before reaching the RTO.
2. Can extend the RTO of a resource.

The BC professional should lead a conversation where each resource required by the activity is discussed to identify workarounds. It is important to note that not every resource can be replaced by a workaround. Workarounds might also have prerequisites that need to be in place prior to the loss of the resource. This might be the case, for example, with an application that is used to capture online orders. The workaround is to direct customers to call instead. Staff can then capture orders via a spreadsheet, which will be uploaded or imported every four hours to the system connected to the application. In this case, two key prerequisites need to be developed and tested: a spreadsheet and an upload and import process. Estimating how long this workaround can operate before it becomes impractical provides the opportunity to adjust the RTO of the application.

Segmenting strategies over time can improve the efficiency of recovery. **For example, the unavailability of a team leader could be supported by the following approach:**

- **Week 1:** transfer a team leader from a different team or location.
- **Week 2:** release the transferred team leader and have the department manager step in.
- **Week 3 and beyond:** go to market for a contractor.

A technique to be considered by the BC professional is to categorise or group BC strategies based on defined RTO ranges.

Categorisation examples include:

- A, B, C, D.
- Platinum, Gold, Silver, Bronze.
- Tier 1, 2, 3, 4.
- < 2 hours, < 12 hours, < 1 day, < 3 days, < 1 week, < 3 weeks, >= 3 weeks.

If categorisation is to be used, the BC professional should nominate a timeframe for each category taking into consideration the range of RTOs approved by top management.

The category reflecting the most urgent recovery capability (e.g. Category A) will require the most advanced, sophisticated, and expensive solutions compared to, for example, Category E.

Resources should be grouped together and categorised to facilitate the identification process for strategies and solutions. For consistency, the BC professional should use the same resource types used during the BIA, **such as:**

- People,
- Information and data (vital records),
- Facilities, equipment, raw materials, consumables, etc
- IT systems and applications,
- Transportation and logistics,
- Finance,
- Suppliers and outsourcing partners.

Figure 1: strategy catergories over time.

Solution Design and Selection

The following tables provide examples of strategies and solutions by resource type segmented by RTO category (Figure 1) and include prerequisites to be implemented prior to disruption. Depending on the nature of the strategy, there might be aspects that need consideration, such as corporate security (both physical and digital), financial constraints, legal and regulatory compliance, and implementation times.

Recovery solutions to deliver a strategy will likely have different parameters of cost and risk. For example, the IT strategy to spread an IT service over two or more geographic locations will include options to retain systems internal to the organization or outsource them to a cloud service provider. Both solutions will meet the business requirements (i.e. application RTOs), but each solution offers different advantages, disadvantages, risks, and costs.

These solution parameters should be presented to top management for selection and approval. Approved solutions, including their parameters, form the solution specification (i.e., the information set required by **PP5**, Enabling Solutions, for implementation).

People Strategies

Sample strategies	Category	Sample solutions	Prerequisite
Staff step in	A	Assign staff with suitable competency at the same site/ location.	Cross-train on-site staff.
		Assign staff with suitable competency from non-impacted site/location.	Cross-train staff at alternate locations.
		Promote staff to higher duties with delegated authority.	Identify suitable staff and document delegation of authority triggers.
Staff take over	B	Select general staff to take over.	BAU documentation.
		Training material.	Cross-train on-site staff.
Relocate staff	C	Suspend activities with longer RTOs and assign their staff to the disrupted activities.	Training material and selection criteria.
Employ external resources		Engage external people.	List of third parties able to supply competent people.
	D	Go to market for contract staff.	Training material expanded to include induction and corporate overview.
		Contact former employees and contractors.	Refresher training material.
	E	Go to market for replacement staff.	N/A

When considering various solutions for people strategies, the BC professional should include references to the MBCO, since the minimum capacity or level of service requirements could be an attribute of the number of people needed.

Additional information regarding people can be sourced from ISO/TS 22330:2018.

Information and Data (Vital Records) Strategies

Sample strategies	Category	Sample solutions	Prerequisite
Replicate	A	Data accessible via available technology across geographically separate locations.	Available infrastructure over at least two geographically separate locations.
		Paper records accessible via digital storage.	Scanning facilities and electronic storage infrastructure.
Restore	B	Data accessible after being restored from back-up.	Establish back-up and restoration facility or engage provider under contract.
Recreate		Recreate paper records from various sources including email and the originator of the document.	Authorisation process for requesting external parties to resend paper records.
	C	Re-key data from source documentation.	Source documentation to be stored in a safe and secure off-site location.

When considering various solutions for information and data strategies, the BC professional should include reference to the RPO since the frequency and retention period of back-ups could be an attribute of the type of service or technology required.

Buildings, Work Environment and Associated Utilities (Physical Infrastructure)

Sample strategies	Category	Sample solutions	Prerequisite
Continuous operation	A	Split the activity across two or more sites/locations.	Increase in funding to operate more than one facility.
		Activate on-site power generation, water storage, and gas storage utilities.	Generator rated to support activities with short RTOs.
Alternate location	B	Work from home.	Staff have suitable home office/ equipment.
		Utilise space/facility at another site/ location.	Confirm space is available and can be made ready within activities RTO.
Relocate to another work area	C	Suspend activities with longer RTOs at a location not affected by the incident to receive relocated staff from activities with shorter RTOs.	Management agreement on which activities will be suspended based on RTOs and physical environment needs.
		Repurpose work areas and facilities (e.g. meeting rooms, lunch areas, etc.).	Management agreement on facilities to be repurposed.
Purchase when needed		Order, deliver, and install temporary/ rented replacement utilities (e.g. power generator, etc.).	Identification of service providers and clarity of their delivery time capabilities.

Continued ...

Sample strategies	Category	Sample solutions	Prerequisite
Relocate to another facility		Transfer activity to staff performing the same activities at non-impacted site/ location.	Confirm capacity loading at receiving site supports MBCO.
		Transfer staff to a non-impacted facility where the same activities are being performed.	Split the activities to operate at more than one location.
		Transfer staff to a third-party facility (e.g. commercial service office).	Ability to establish a contract and configure IT connectivity and other services to meet activities RTO.
Repurpose	D	Repurpose building areas (e.g. storerooms, office spaces, etc.).	Management agreement on building areas to be repurposed.
Replace and rebuild	E	Rebuild facilities.	N/A
		Purchase, deliver and install replacement utilities.	N/A
		Rebuild and reconnect utility feeds.	N/A

When considering various solutions for physical environments, the BC professional should include reference to the MBCO since the minimum capacity or level of service could be an attribute of the size or capacity requirements of where people or equipment need to operate from.

Transportation and Logistics

Sample strategies	Category	Sample solutions	Prerequisite
Redeploy	A, B	Staff use their personal vehicle.	Confirm insurance requirements for staff using personal and company vehicles for business.
		Staff use company vehicle.	
Go to market		Engage an alternate transport and logistics company (ad-hoc service request).	Identification of alternate companies providing the required services.
Leverage customer relationship		Request customers pick-up or arrange their own courier.	Consider whether this will damage the customer relationship.
Outsource	C-E	Contract an alternate transport and logistics company (contractual agreement).	Identification of alternate companies providing the required services. Ability to establish a contract and provide the service to meet the activities RTO.

IT Systems and Applications

Sample strategies	Category	Sample solutions	Prerequisite
Hot continuity	A	Applications and data stores are replicated in real time across two (or more) geographically separate locations under an active/active arrangement (also referred to as hot).	Establishment of replicated IT infrastructures (either in-house or outsourced).
		Access to a copy of the data that meets the RPO.	Cross-train staff at alternate locations.
		Data communication paths have diverse routing which can switch automatically.	Installation of diverse routing and redundant equipment.
Redeploy	B, C	Redeploy workstations, printers, and other office IT equipment.	Management agreement of which devices are to be redeployed (typically aligned to activities with long RTOs).
		Staff use personal equipment (i.e. BYOD).	Process to approve personal equipment for business operations.
Warm recovery		Alternate infrastructure is available and preloaded, ready to receive the latest restore (referred to as warm standby).	Alternate infrastructure and process to maintain suitable version control (either in-house or outsourced).
		Replace office data communication paths with Wi-fi infrastructure via off-the-shelf or spare equipment.	Management and storage of spare equipment.
	C	Purchase replacement workstations, printers, and other office IT equipment when needed.	Availability of funding.
Cold recovery	D	Alternate infrastructure supporting systems with long RTOs that can be rebuilt to receive the latest restore (referred to as cold recovery).	Management agreement on which infrastructure to redeploy (typically aligned to systems with long RTOs).
Purchase when needed	E	Purchase, install, and restore new infrastructure ready to receive the latest restore.	Availability of funding.
		Outsource to third party service provider.	Ability to establish a contract and configure IT connectivity and other services to meet activities RTO.

Finance

Sample strategies	Category	Sample solutions	Prerequisite
Immediate available funding	A, B	Use corporate credit card.	Identify managers with cards and set their spend limit.
		Create/extend letter of credit with the bank.	Establish an agreement with protocols than can be activated even out of banking hours.
		Define emergency or delegated spend authorities.	Establish an agreement with protocols than can be activated under defined criteria.
	C	Access funds from cash reserves.	Establish an agreement with protocols than can be activated under defined criteria.
Parent assistance		Request support from parent company.	Establish an agreement with protocols than can be activated under defined criteria.
		Request funds from parent company.	Establish an agreement with protocols than can be activated under defined criteria.
Insurance	D	Use funds provided by insurance claims.	Ensure adequate cover with consideration given to various types of insurance, such as business interruption, damage, cost of increased working, loss of revenue, cyber, etc.

Suppliers and Outsourcing Partners

Sample strategies	Category	Sample solutions	Prerequisite
Continuous operation	A, B	Operate with more than one supplier for each product and service to be delivered.	Identify and engage alternate companies providing the same products and services.
		Increase stock levels within the organization or at the supplier.	Establish and maintain the process for excess stock levels.
Go to market	C	Engage an alternate supplier on a temporary basis.	Identify and engage alternate companies. Verify their ability/capacity to supply.
Step in		Offer support to supplier with equipment, logistics, personnel, funding, and facilities to allow the supplier to recover from their disruption.	Assess the nature of the service provider and identify the areas of support, the mechanisms, and limits of provision.
		Take over operations from the supplier or business partner.	Establish contractual arrangements and triggers. Ensure staff are suitably trained.
	D	Purchase the supplier or business partner and continue to operate.	Establish contractual arrangements and triggers. Ensure staff are suitably trained.
Go to market		Engage suppliers previously contracted.	Identification of previous suppliers still able to supply.
Replace	E	Engage a new supplier or partner on a permanent basis.	Identify and engage alternate companies.

When considering various solutions for supplier strategies, the BC professional should include references to the MBCO, understanding that the minimum capacity or level of service could be an attribute of the supplier's startup (ramp up process), and that capacity requirements may increase over time. Additional information can be sourced from ISO/TS 22318:2021.

The BC professional should also meet with those in charge of procurement and legal units to investigate and, where required, remediate, contractual arrangements with suppliers and partners. This should also flow into new tender and contract criteria. The objective is to ensure suppliers and partners have regularly tested BC plans and capabilities aligned to the activities RTOs that rely on them. Suppliers and partners with shorter RTOs should be prioritised in this assessment, while those with long RTOs might not necessarily have to be included.

For suppliers and partners with short RTOs, the BC professional should encourage contractual obligations that allow the organization to:

- Attend/participate in exercises,
- Review plans and exercise reports, and
- Be advised of any material change the supplier or partner are planning related to the delivery of the service.

People Management Strategies

The BC professional should meet with the people and culture manager to identify and document strategies for responding to people needs during an incident. The meeting should commence with some education and awareness regarding the purpose of the meeting, why it is important, and how their participation will contribute to better protecting the organization from unacceptable disruptions. It is important to note that the BC professional might have met with the people and culture manager during the activities of PP2 and therefore could have already established a working relationship with this professional figure.

The following are conversation prompts for the BC professional that might be useful in starting a conversation:

- What structures do we have in place to protect and keep people safe during a disruptive event?
- How do we account for the people on site in the case of an emergency?
- Are these structures inclusive of people with different needs? Do they include people other than staff, such as visitors or customers?
- Do we have the right channels to liaise with interested parties, such as emergency services or families?
- Do we have adequate training and equipment to manage injuries or possible fatalities?
- Do we have procedures for managing issues such as payments, funding, transport, and accommodation during and in the aftermath of an emergency?
- Would we be able to furlough staff or modify their work arrangements?
- Are we able to provide physical and mental health services?

Other similar discussions might take place with other managers, such as those responsible for properties and facilities.

Outcomes and Review

The outcomes in this section consist of a set of strategies and solutions to resume business operations that:

- Allow disrupted activities to continue according to their respective RTOs,
- Can limit the impacts of disruptive events to prioritised activities,
- Are cost effective,
- Address different areas of the organization, including suppliers, business partners or contractors that support prioritised activities, and
- Provide several choices to BC professionals, so that they may choose the one(s) that are most suitable to their organization.

Mitigating Unacceptable Risks and Single Points of Failure

The outcomes from the RA undertaken during PP3 are:

- An awareness of the range of risks that could disrupt the organization's activities.
- A prioritised list of risks based on the risk rating.
- Identification of any unacceptable risks and single points of failure.

Concepts and Considerations

Within the context of the RA, strategies and solutions are concerned with the mitigation of unacceptable risks and single points of failure.

The identification of solutions is influenced by a variety of business relevant considerations, including:

- **Regulatory obligations:** these must not be breached,
- **Initial and ongoing cost-benefit:** these must not outweigh the cost of disruption,
- **Intangible benefits:** must not be ignored,
- **Contractual requirements:** must not be breached,
- **BC requirements:** must not be breached, and
- **Secondary risk:** a solution must not introduce additional risk.

Process

The BC professional must identify and collaborate with those across the organization that have a deep understanding of items with unacceptable risk, or the single point dependency, to identify mitigation strategies.

These people are activity and resource owners and have a vested interest in protecting the organization from disruption.

The BC professional will:

1. Review each unacceptable risk and single point of failure.
2. Identify or nominate a knowledgeable person within the organization.
3. Group unacceptable risks and single points of failure by owner.
4. Schedule sessions to meet each owner.
5. Present details of the unacceptable risks and single points of failure to the owner. The meeting should include some education and awareness regarding the purpose of the meeting, why it is important and how their participation will contribute to better protecting the organization from unacceptable disruptions.
6. Convey the concerns of top management (e.g. their risk appetite).
7. Discuss strategy options that will mitigate the risk or remove the single point of failure.
8. **For each strategy option, the owner will consider and document parameters for various solutions where each solution will be defined with:**
   - A specification (i.e. sufficient detail such that the solution can be implemented),
   - Advantages and disadvantages,
   - Implementation time, and
   - Estimated costs to prepare, implement, operate, and maintain.
9. The owner then will select the most appropriate solution(s) for each strategy.

Methods and Techniques

Strategy and solutions development is best undertaken via a workshop or meeting with the activity and resource owners. This enables the BC professional to direct the conversation while learning the nuances of the risk item. This provides another opportunity to improve the BC culture of the organization, by including elements of education, awareness, and the purpose of BC.

The meetings could be divided into two main sections:

1. **An introduction to strategy and solutions, where the BC professional will:**

- Present the list of risks and single points of failure,
- Explain how to think about strategies and solutions by discussing the philosophies of risk mitigation (ISO 31000:2018), and
- Offer a timeframe by which the work will be completed by the risk owner, noting whether they indicate their need for some time to undertake research for the solution.

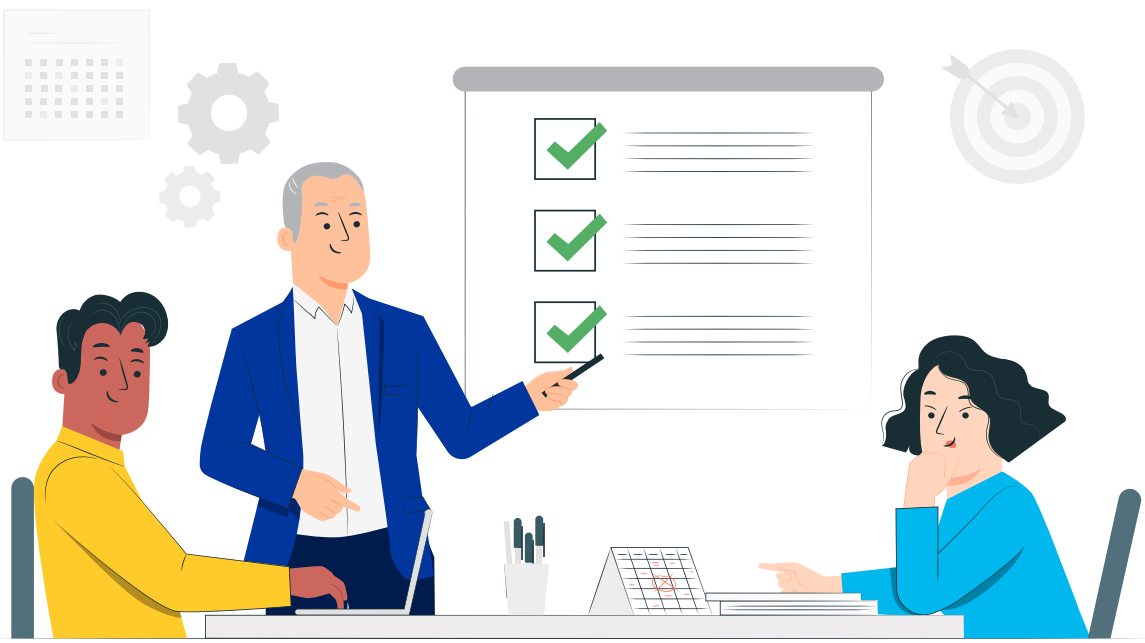
2. **A review of the strategy and solutions, where the BC professional will:**

- Walk through each solution,
- Consider the solution parameters, and
- Nominate at least one preferred solution for each strategy, in consultation with the resource owner.

Outcomes and Review

The outcomes and review in this section consist of a set of approved strategies and solutions to mitigate unacceptable risks and single points of failure to:

- Protect activities from disruption with respect to their RTOs.
- Limit the impacts of disruptive events to prioritised activities.
- Remain cost effective in terms of implementation and operational investments.



BCI Professional Practices

PP5: Enabling Solutions

Enabling Solutions is the PP that outlines the methodology to implement the agreed solutions, develops the response structure and BC plans to ensure that the solutions can be deployed when required.

Enabling Solutions implements the agreed BC solutions, designs a response structure to mobilise resources and deploy during an incident, together with developing BC plans that detail the response activities and procedures that response teams need to follow. The resulting plans and processes are designed to be scalable and therefore able to be deployed in response to any incident type.

Introduction

Once the solutions have been designed and specified, the next step is to operationalise them so they can be utilised when required in response to an incident.

This consists of three activities:

- **Implementing BC solutions:** operationalising solutions that have been agreed in PP4.
- **Designing the response structure:** designating the response teams required to mobilise and deploy the plans during an incident.
- **Developing BC plans:** creating guidance documents that detail the response activities and procedures that specific response teams need to follow.

Implementing BC Solutions

Once the solutions to resume business operations and the solutions to mitigate unacceptable risks and single points of failure, collectively known as the solutions, have been specified and approved (**PP4**), they need to be implemented. Solutions must be implemented before they can be deployed to respond to disruption and recover affected resources. They must also be supported with a response structure and BC plans. Solutions to mitigate unacceptable risks and single points of failure are implemented to reduce the likelihood of a disruption to an activity (prevention). Finally, solutions and BC plans need to be validated (**PP6**).

General Principles

To implement the solutions, the BC professional should adhere to the following principles:

- The solutions have been specified and approved as part of the Solutions Design stage (**PP4**).
- The Solutions Design stage must specify the solutions with sufficient detail – the more complex the solution or the shorter the recovery time, the more detail is required in its specification.
- The BC professional is accountable for ensuring that the solutions are implemented.

  It is important to understand that:

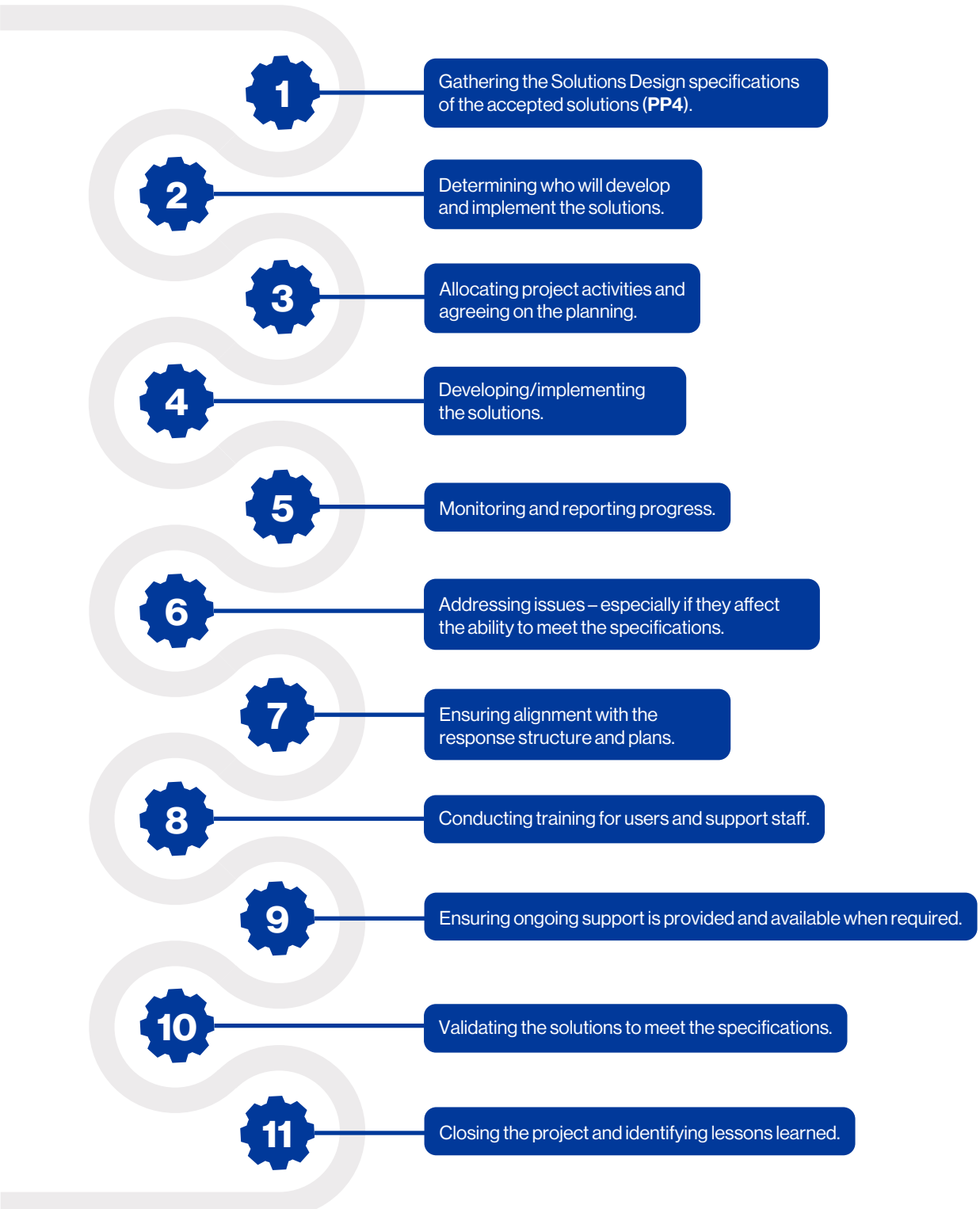
  - The solutions to resume business operations will often be developed and implemented by other teams within the organization or by third parties.
  - The risk department will typically oversee the implementation of the solutions to mitigate unacceptable risks and single points of failure.
- The implementation of the solutions may require the development of systems or tools.
- The implementation of the solutions should be carried out as a project. This may be a single project or several projects under a programme. The project should follow the organization's project management processes.
- Each implementation should include Validation (**PP6**) – without this, it cannot be confirmed to have met the specifications.
- Validation may be performed as part of the implementation and change process or routinely scheduled validation activities.

Concepts and Considerations

- Consider utilising a competent project manager for the implementation, especially for larger or complex implementations.
- Ensure that the appropriate competencies are available in the project team.
- Work with the organization's procurement and legal departments when purchasing external solutions.

Process

The BC professional needs to ensure that the implementation of the solutions meet the agreed specifications. **Therefore, the following steps should be carried out (note: it is expected that some steps will be carried out in parallel):**



Methods and Techniques

The implementation should be managed as a project in compliance with the organization's project management procedures and practices.

Outcomes and Review

The outcome of the implementation of solutions is that the solutions are implemented and handed over to the business. The implemented solutions should be regularly reviewed and validated through exercises.

Designing the Response Structure

The purpose of establishing a response structure is to ensure that the organization has a documented and well-understood hierarchy of teams for responding to an incident, regardless of its cause. This goes further than just the ability to recover the business processes. The response structure establishes command, control, and communication to help the organization manage the incident and minimise its impact.

An effective organizational response capability can be achieved if BC professionals collaborate with other professionals accountable for managing the response in their respective management disciplines. This has the added advantage of contributing to an improved BC culture, encouraging those collaborating to embrace better BC (PP2). It is therefore essential that these teams can work together when required. This should be taken into account when designing the response structure.

General Principles

The response structure identifies:

- The roles, responsibilities, and authority of the teams responsible for response activities.
- The leadership of each team.
- The documented procedures to support the teams.

Each organization should develop a response structure that meets its own needs. The response structure should be closely aligned with the existing management and organizational structure as this will help align with existing chains of command and responsibilities. The result is clearly defined roles and responsibilities when responding to an incident.

A response structure that is appropriate to the size and complexity of the organization should be established.

While the focus of BC is the resumption of prioritised business activities, this is only one type of incident that the response structure must be able to manage. Therefore, when developing the response structure, include all teams that may be required to respond to incidents. For example, teams from the areas of emergency or environmental response, ICT DR, supply chain continuity management (SCCM), health and safety, or cyber incident response teams.

All members of the response structure must be trained and must participate in exercises.

Concepts and Considerations

An organization's response structure should be agile and capable of dealing with many incident types.

Incidents may have an immediate impact but, in other situations, the impact could develop slowly over time. Therefore, incidents need to be monitored and early action taken to prevent them from escalating further.

The critical requirements for an effective response structure include:

- The ability to recognise and assess threats when they occur.
- Clear procedures for escalation when an incident has occurred or may occur soon.
- Individuals and teams with the authority and capability to develop and select an appropriate response to an incident.
- Clearly understood procedures in place to activate and control the response to an incident.
- Responsible personnel with the authority and competency to invoke the agreed response, which may include implemented solutions.
- A plan to communicate effectively with internal and external interested parties.
- Access to sufficient resources to support the response.
- Knowledge of when key external suppliers and regulators should be notified and included in the response.
- An agreed budget for supporting the response structure, including training.

Some organizations build their response structure using existing levels in a hierarchy (for example, strategic, tactical, and operational). The strategic, tactical, and operational teams in the response structure undertake different levels of activity.

The strategic team focuses on issues threatening the organization's reputation and viability. This includes impacts on the organization's core objectives or products and services. The strategic team is always led by top management.

At the strategic level, it is important to keep in mind the following considerations:

- Crises are abnormal situations that threaten the organization's viability and integrity. They require a flexible and creative response by experienced managers with the authority to apply the organization's complete resources to the response.
- The strategic team is often called the crisis management team. It is primarily responsible for addressing incidents impacting the organization at a strategic level, which may be formally declared as a crisis.
- While crisis management is a separate discipline, it is often established and coordinated by the BC professional – particularly in smaller organizations.
- The strategic team may also provide guidance and decision-making during less severe incidents and support tactical and operational teams.
- Complex organizations may have local, regional, and global strategic teams. In smaller organizations, the strategic team may also perform the tasks of the tactical team.

Attributes of strategic team members should include:

- Ability to listen actively and accept input from various sources.
- Excellent communication skills.
- Strategic thinking.
- Respect from colleagues and top management.
- A wide reach across the organization that can inspire others to accomplish goals.
- Decisiveness and the ability to make decisions quickly and, if needed, with partial information.
- Ability to manage stress within themselves and with others.
- Strong situational awareness.

Tactical teams enable the coordination of response activities when several operational teams are involved.

They are responsible for several tasks:

- Providing support for the strategic team.
- Passing on directives from the strategic team to the operational teams.
- Consolidating information from the operational teams and relaying this to the strategic team.

Attributes of tactical team members should include the ability to:

- Coordinate operational teams.
- Escalate information to the strategic team.
- Communicate on behalf of the strategic team.

Operational teams focus on the continuity of business activities and the availability of resources that deliver the prioritised products and services. Operational teams also deal with the immediate effects of an incident by containing it where possible and managing the direct consequences. Operational teams may also manage the recovery of the resources and business activities.

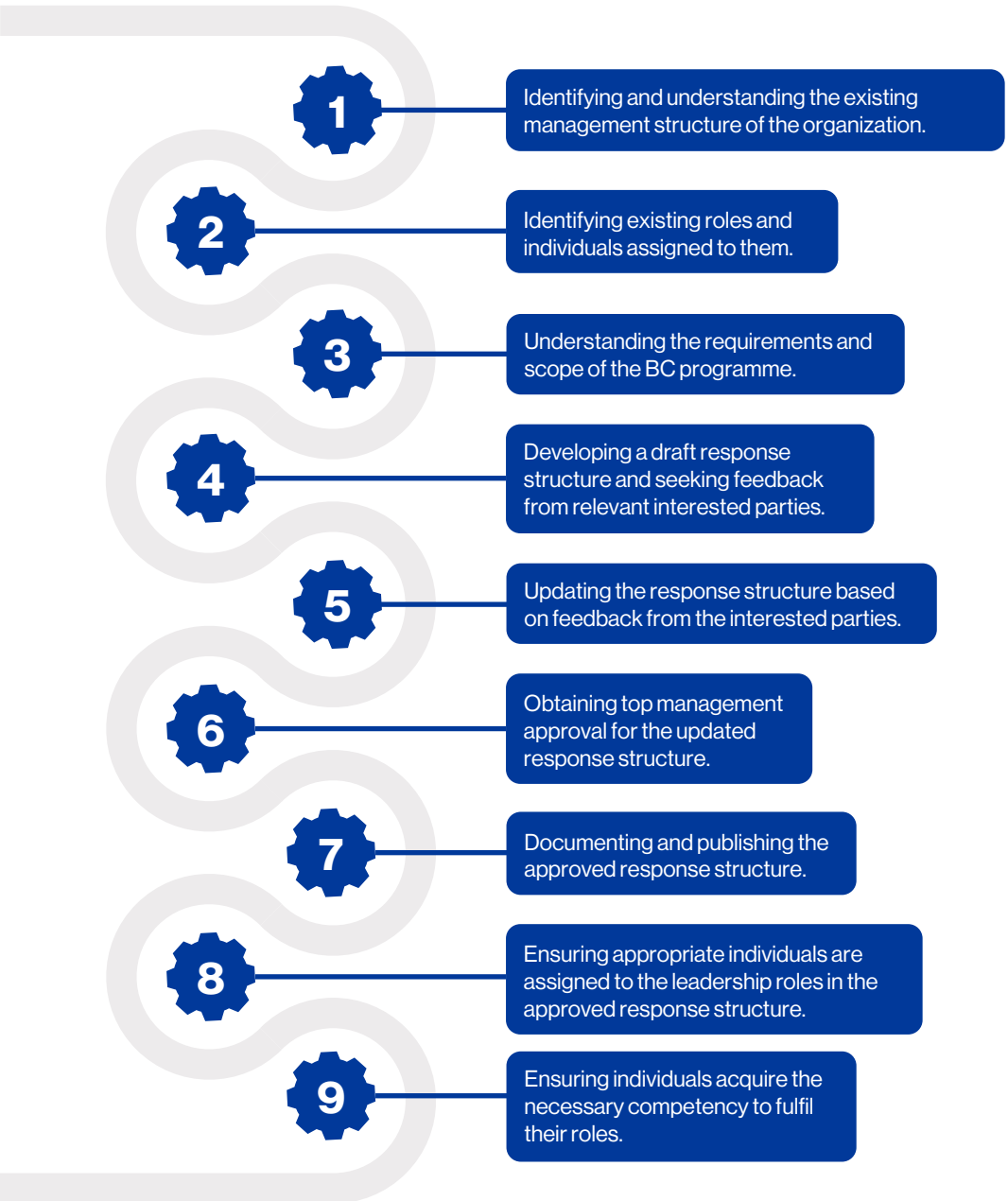
Attributes of operational team members should include:

- An understanding of the business processes to be recovered and their relationship with other processes.
- Familiarity with their BC plan.
- Appropriate knowledge and skills as required to execute the BC plan.

Process

The BC professional should develop a response structure capable of responding to incidents.

The key steps should include:



In some organizations response plans may already exist. In this case, the teams and roles responsible for developing the existing plans should be assessed and, where appropriate, aligned and incorporated into the response structure. As a result, changes may need to be made to the existing response structure.

Methods and Techniques

- The strategic, tactical, and operational response structure provides a possible model for an organization.
- The table below shows how this model could be implemented in different types of organizations:

Table 8: how response structures may differ depending on organizational size.

Strategic	Tactical	Operational
Small, single-site organization		
The entire response structure may consist of only one team.		
Medium-sized organization		
Due to limited personnel, it may be appropriate to configure the strategic and tactical teams as one team.		An operational response team should exist for each business unit with prioritised activities. There are separate teams for emergency response, IT recovery, production, etc.
Large organization		
There should be a dedicated strategic team.	**The tactical team(s) will:** • Provide support to the strategic team, • Coordinate when several operational teams are involved, • Pass on directives from the strategic team to the operational teams, • Consolidate information from the operational teams, and • Relay this to the strategic team.	An operational response team should exist for each business unit with prioritised activities. There are separate teams for emergency response, IT recovery, production, etc.
Large multinational organization		
A large multinational organization should have a global strategic team and possibly separate strategic teams for each country or region.	**The tactical team(s) will:** • Provide support for the strategic team, • Coordinate when several operational teams are involved, • Pass on directives from the strategic team to the operational teams, • Consolidate information from the operational teams, and • Relay this to the strategic team.	An operational response team should exist for each business unit with prioritised activities. There are separate teams for emergency response, IT recovery, production, etc.

Outcomes and Review

The outcome of developing and implementing a response structure is that the organization can respond effectively to incidents.

The response structure defines:

- The required number and type of teams needed in an organization.
- The relationships between the teams.
- The roles, responsibilities, and authority of the teams and their members.

The response structure should be regularly reviewed and validated through exercises.

Communications

When responding to incidents, both internal and external communications are critical elements of an effective response. How interested parties perceive the response to the incident is a key factor in determining how successfully it is being managed. Poor messaging, slow response, lack of empathy for those impacted, and failure to acknowledge the incident can worsen an already bad situation. The purpose of communications is to position the organization as the central source of information, demonstrate its control of the situation, and reassure interested parties.

During an incident, sending out warning notifications may be of vital importance to those who may be impacted and could be a matter of life or death. This could be, for example, warning people to evacuate an area in response to a fire, the release of hazardous gas, or a chemical spill.

Having a comprehensive framework in place for coordinating warnings and communications, trained spokespersons, and validated communication plans will contribute to the organization successfully managing an incident. This should also include leveraging available local, regional, national, and global warning systems.

General Principles

To implement effective communications, the organization should adhere to the following principles:

- Internal and external communication during an incident can occur at all organizational levels, as long as they are centrally approved first. The level at which communications occur, whether at the strategic, tactical, or operational level, may be based on the level at which communications occur during normal day-to-day operations. Communication procedures must be developed and documented, detailing how communication will be carried out and coordinated throughout the organization.
- Top management usually sets the messaging, the media strategy to be followed, and the tone of the communications. Communications must be coordinated within the organization and the messages should be adapted to the channel used to communicate and the requirements of the targeted interested parties. Inconsistent messaging or contradictory information will negatively impact the organization, especially its response and reputation, and will confuse the people receiving it.
- All plans should contain or reference documented communications procedures, including required authorisations and responsibilities.
- Communications with the media, social media, and the appointment and briefing of spokespersons are usually coordinated centrally by a communications team. In addition, the communications team will work with and advise the strategic team on the organization's communication strategy.
- The communications procedures should cover all forms of impact on the organization, including reputational impact.
- Communications should be consistent with the organization's beliefs, culture, values, and value proposition. The media may extract information from the organization's website at any time, particularly during an incident. It is therefore essential to keep it up to date and it should not contradict any incident communications.

- Since images of incidents can be live streamed or uploaded to social media instantaneously, the organization must be ready to issue communications regarding incidents at very short notice.
- Social media can be a channel for communicating directly with interested parties. It is a platform that can contribute to the organization's objective of positioning itself as the central source of information, demonstrating its control of the situation and reassuring interested parties. It can bypass the filter of traditional media and can be used to state the organization's views and provide an opportunity to listen to and engage with interested parties. Unfortunately, it can also be the platform where untruths, rumours, personal attacks, and misinformation flourish. Therefore, organizations must be prepared and know how to respond to an incident playing out on social media, even if they do not regularly use or have a presence on these channel(s).

Concepts and Considerations

Documented Communications Procedures

The BC professional should facilitate discussions to ensure that the organization has procedures which document how communications are coordinated across the organization.

These procedures should:

- Detail how communications are developed and authorised.
- Address how internal and external communications should be coordinated and tracked across the organization.
- Include responsibilities for alerting interested parties impacted potentially by an actual or impending disruption.
- Identify, list, and then rank internal and external interested parties, record their contact details and, where possible, define each party's communication requirements or expectations.
- Define the available methods and channels for communicating with each interested party, for example, social media, phone, email, text, radio, and newspapers.
- Describe how to escalate an incident which has or is likely to attract media attention.
- Provide instructions regarding interacting with the media or handling media enquiries.
- Include a selection of communication methods and channels so the team can guarantee the availability of at least one method or channel. This should include the ability to respond if internal systems are unavailable, for example, due to an IT failure or cyber attack.
- Allow for developing questions and answers for placement on the organization's website, which may also be referenced by staff when communicating with interested parties.
- Provide guidelines to staff for the use of social media during incidents.
- Procedures for logging and securely storing communications received and sent to interested parties.
- **Remind those developing communications that messages:**
  - » Should not contain complex or technical language,
  - » Should be in the appropriate language for the target audience, and
  - » Should be honest and transparent within the boundaries of confidentiality and privacy.
- Identify the organization's team, group, or individual with the responsibility, authority, and technical knowledge to deliver communications via each available method and channel.
- The usual channels and methods should be used to communicate with interested parties where possible.
- Assign responsibility for monitoring and reviewing the effectiveness of messaging and interested party response to communications and then assess and adjust as required.

Engaging with Media and Social Media

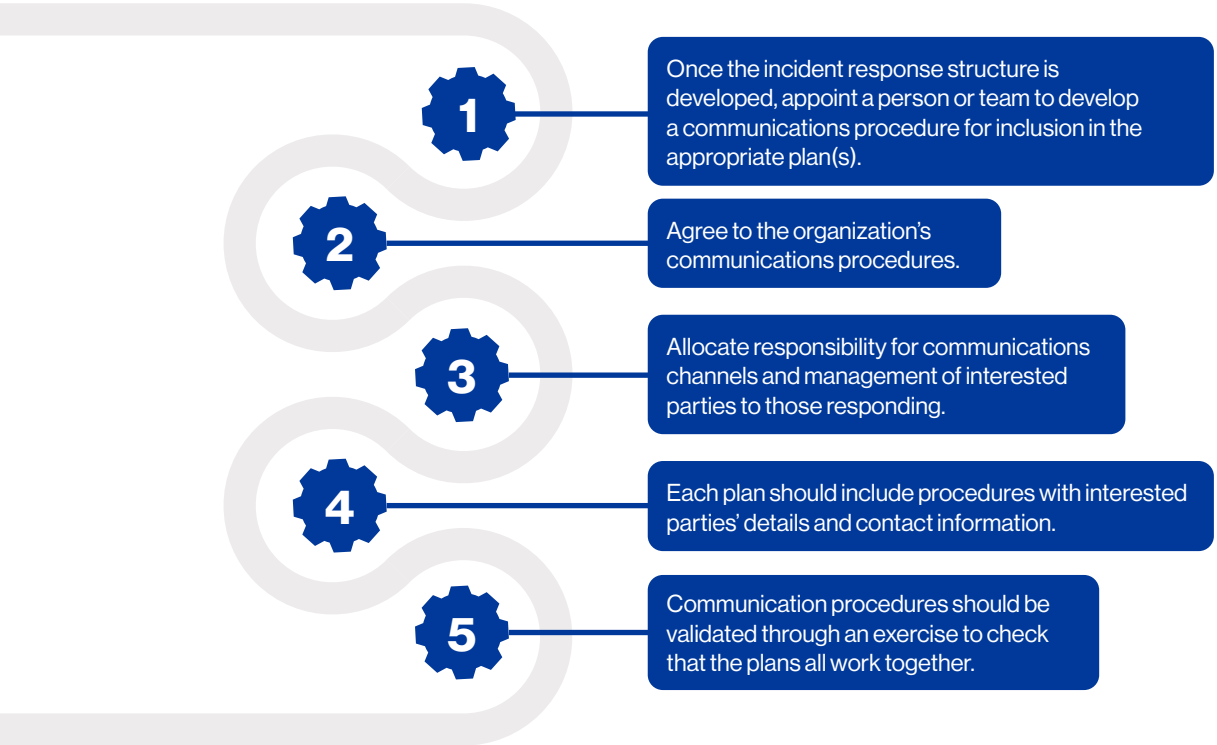
Communication procedures should address how the organization manages communications with the media and on the organization's social media channels. The plan should ensure that only appropriately trained and authorised personnel liaise with the media and communicate using social media channels. They should also participate in exercises (PP6).

Communications with the media should be via written statements, information placed on the organization's website, or through the provision of a spokesperson for live interviews.

When communicating using social media channels, communications should be two-way. This can provide insight into how interested parties react to the organization's response to the incident.

If social media is a key element in the organization's communications response strategy, then an appropriate preparation strategy is required. For example, build up followers and establish its social media channel(s) presence as the organization's authentic voice before an incident occurs.

Process



Methods and Techniques

Warning Plans

As part of emergency response, there may be instructions on how to notify people of an actual or possible incident. This may be a separate warning plan or part of an emergency response plan. The instructions should enable the recipients to take action to protect themselves, carry out an action, or involve themselves in responding to an incident.

A warning plan should:

- Identify the recipients, **including:**
  - » Those on-site or in the surrounding area of an on-site hazard, such as a hazardous gas or material release.
  - » Staff not on site, in order to instruct them, for example, not to go to work due to a transportation incident or an incident affecting their place of work.
  - » Interested parties with sensitive data stored by the organization, in case a breach occurs.
  - » Response team members.
  - » Those in a location that may be affected by severe physical disruption, such as extreme weather. This will help with warnings and follow-up actions (e.g. evacuations).
  - » Interested parties in case of a product recall.
- Consider the warning timing (e.g. out of office hours versus during office hours).
- Consider privacy and data protection regulations.
- Determine the organization's response to an alert, including any special assistance it would need to provide to those affected, such as vulnerable individuals.
- Include the method and system for informing the recipients, **such as:**
  - » Use of an onsite public address system, flashing lights, alarms, or sirens.
  - » Direct communications by telephone, radio, satellite phone, or email.
  - » Call lists: a list containing contact numbers and alternative contact numbers.

  - » Call trees: a predetermined list where each person calls several others.
  - » Use of a 'chain of command', where more senior employees notify more junior ones.
  - » Notification software tools. This can be a very powerful way to connect large numbers of people and has the advantage of multiple contact channels. They can be used to confirm reception of key messages.
- Make sure those who react to an alert know what actions to carry out and when the alert is over.
- Exercise warnings regularly, at least once a year.

The BC professional should facilitate discussions to ensure that the organization has procedures for receiving, documenting, and responding to external warnings, alerts, or communications, including those from national, regional, or global risk advisories.

Spokespersons

A spokesperson represents the organization and positions it as the central source of truth, demonstrating its control of the situation.

Spokespersons should respond according to the communications strategy, which conveys information to interested parties. Part of the duties of a spokesperson will include attending press conferences, presenting the organization's view of an incident, and offering apologies when appropriate.

Failing to perform all of these activities due to poor information, inconsistency of language and contradictions, lack of sincerity (e.g. in an apology), and not having a designated spokesperson can all have a detrimental impact on the organization and those impacted by an incident.

The BC professional should consider that the spokesperson must:

- Be appropriate to the audience and relevant to the type and impact of the incident (e.g. executive, communications professional, local manager, or technical expert).
- Have familiarity with the language and jargon of the audience (translation services or technical experts' assistance could be used if needed to achieve this).
- Undergo media training and exercising.
- Be able to get to the location of an incident, or other agreed locations, at short notice.
- Receive briefings and updates.
- Have the availability of venues to liaise with the media, emergency services, or other interested parties.

Identification of Interested Parties

Within all plans there should be a comprehensive list of interested parties who might need to be contacted during an incident.

The following information should be recorded for all interested parties:

- **Who** is the interested party? For example, personnel, suppliers, customers, community, and the media.
- **How** should they be contacted? For example, by telephone, email, social media, text, or letter. This section should include a selection of several communication channels.
- **When** should they be contacted? For example, immediately after becoming aware of the incident, the next working day, within the first week, etc. If there are regulatory timeframes for reporting incidents, these should be documented.
- **What** are their identified information requirements during an incident? For example, facts of the incident, actions they should take, impact on service delivery, and timescales for restoration.

Criteria and responsibilities for identifying relevant interested parties and prioritising them during an incident should be documented.

Interested parties may be segmented into smaller groups to allow for tailored communications. Examples of groups could be the top 10% of vulnerable customers, as the organization may need to respond to them differently than other customers.

Logging Information and Decisions

All organizations should have procedures for logging and securely storing actions, events, communications, and decisions. After an incident, there should be a review. This could vary from an internal review or debrief to an external review, investigation, or inquiry.

It is good practice to record decisions and actions. In some cases this is a legal requirement. A process should be in place for collating and securely storing all pertinent information about an incident.

Outcomes and Review

The outcomes of developing warning and communications procedures include:

- A warning capability where required.
- A documented framework for managing communications across the organization and ensuring consistency of messaging.
- A list of interested parties for each plan or document.

Developing and Managing Plans

A BC plan is defined as: "Documented information that guides an organization to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives," (ISO 22301:2019). The term BC plan suggests a single document; however, it may comprise several documents for use by different teams. In addition, the plan or plans are likely to be structured according to the organization's size, complexity, type, infrastructure, products and services, and locations.

While BC plans focus on business recovery, plans must also be developed to address other responses to an incident. The response structure should determine the number and types of plans to be put in place.

The BC plan is not intended to cover every eventuality as all incidents are different. Also, it is not possible to envisage every impact. Therefore, the plans need to be flexible enough to adapt to the specific incident and the opportunities that may arise. However, in some circumstances, scenario-specific plans are appropriate to address a particular threat or risk, for example, a pandemic plan.

General Principles

Plans are intended to be used in high-pressure, time-limited situations. Therefore, a user-friendly plan should be concise and easy to read. Plans are guidance documents, not reports, and should not contain information that is not needed during a response.

To make plans fit for purpose, plans should be:

- **Direct:** provide clear, action-orientated, time-based instructions, as well as quick access to vital information. The instructions and information in the plans should be presented according to the order in which they are required.
- **Unambiguous:** not be open to multiple interpretations and avoiding jargon and abbreviations.
- **Verifiable:** include information to determine that the instructions have been carried out correctly and have the desired effect.
- **Adaptable:** enable the organization to respond to a wide range of incidents, including those that the organization may not have anticipated.
- **Concise:** include clear instructions and not unnecessary, vague/unclear words, or language.
- **Relevant:** provide only guidance, information, and tools that are current and useful to the team using the plan.
- **Ordered:** contain information in the plans that is laid out to avoid a search for information, especially when teams are under pressure to respond at the beginning of an incident.

Plans should be kept up to date and they should be documented to enable personnel to access the information relevant to them quickly.

It is vital that plans can be relied upon to deliver the agreed outcome. Therefore, before a plan is deemed operational, it should first be validated (PP6).

Concepts and Considerations

Plans should support the teams as defined in the response structure. Often, this results in strategic, tactical, and operational plans.

Tactical and operational plans may contain information about procedures which can only be developed after the solutions have been agreed upon in the Solutions Design stage (PP4) or after their implementation in PP5. The strategic plan does not usually contain such detailed procedural information and may be developed earlier in the BCMS to provide an initial response capability.

The relationship between the strategic, tactical, and operational plans should be documented.

Plans at all levels (strategic, tactical, and operational) should contain the following:

- Purpose, scope, assumptions, and objectives of the plan.
- The team responsible for executing the plan.
- Plan activation criteria.
- The individuals authorised to activate the plan and mobilise the team.
- **Plan activation and team mobilisation procedures:**
  - » Details of meeting locations (physical or virtual).
  - » Response team roles and responsibilities (with alternates as appropriate).
- Individual responsibilities and authorities of team members within each plan (with alternates as appropriate).
- Prompts for immediate action and any specific decisions the team(s) may need to make, such as activating an alternate site.
- Communication requirements and procedures.

- **Guidance for escalation:**
  - » A list of relevant interested parties who might have to be contacted during a disruption.
  - » Internal and external dependencies, including contact details.
  - » Third parties who may form part of the response, their contact details, and any applicable support contracts.
- Plan approval.
- Guidance and templates for logging information and recording decisions, actions, and outcomes.
- Procedures for standing down once objectives have been achieved and/or the incident has been resolved.

Regardless of the type of plan being developed, it should not be carried out in isolation. It is essential to be mindful of the organization's overall BC requirements and involve users of the plans, including top management, in the development process to achieve a successful outcome.

Process

The BC professional should:

Each plan should be Validated (PP6); without this, the plan cannot be relied upon to meet the BC requirements defined in PP3 in combination with modifications as agreed in PP4.

1. Appoint an owner or sponsor of the plan.
2. Define the purpose, scope, assumptions, and objectives of the plan.
3. Create a project team (if appropriate).
4. Socialise the rational and objective of the task to improve awareness as part of Embracing BC (**PP2**).
5. Determine the response team responsible for the execution of the plan and define roles, relevant authorities, and competencies within the plan.
6. Gather information from the Analysis (**PP3**), Solutions Design (**PP4**), and Enabling Solutions (**PP5**) stages and other sources to populate the plan.
7. Draft the plan according to the agreed template and assign individuals to defined roles.
8. Circulate the draft plan to those required to execute it for consultation and review.
9. Gather feedback from the consultation and review and finalise the plan taking this into account.
10. Seek approval of the plan from the plan owner or sponsor.
11. Ensure that the organization is aware of the existence of the plan.

Methods and Techniques

The following methods and techniques should be adopted to develop strategic, tactical, and operational plans.

Plan Management

Although a specific business unit may own some BC plans, they are part of the organization's overall BC programme. In addition, other departments within the organization may own other incident response plans.

All plans should be held in secure locations and the most up-to-date version of each plan must be available for all team members. Depending on the solutions implemented, physical copies of the plans may also be required or desirable. Plans stored electronically must be secured and available when needed. Consider storing plans in an independent online repository, such as the cloud, and synchronise to smartphones where a local copy can be stored. Ensure that updates are pushed to mobile devices.

Roles and Responsibilities

In the plan, the personnel nominated to be members of the response team should have the appropriate authority and competency to respond to an incident. Alternates should be identified for each role to ensure cover when the primary team member is unavailable or when extended hours are required during the response. Alternates must be trained to the same level as the primary team member. Plans should clearly state which team members have responsibility or authority for key decisions or actions when a team member or members are absent.

Specific team roles, each with nominated responsibilities, might include:

- The team leader, who ensures that the response team is mobilised, briefed, and properly staffed. They can nominate additional team members if necessary.
- People-welfare personnel, who have responsibility for safeguarding the health, safety, and welfare of their workforce, contractors, visitors, and customers (in some industries).
- **Communications:**
  - » Internal communication establishes and maintains contact with personnel and other response teams and keeps them informed.
  - » External communication establishes and maintains contact with interested parties outside the organization, including the media.
- Operations, including finance.
- Administrative support, including a record keeper for incoming information, decisions, and actions.

Activation and Mobilisation

The plan should document the conditions or circumstances of the activation and mobilisation of the teams. For example, a disruption estimated to exceed the RTO of prioritised activities is a trigger for plan activation.

The plan should contain a process for continually assessing the situation to determine if it is still applicable or if escalation is required.

Not all incidents happen suddenly or have an immediate impact. Some develop at a slower pace before they are recognised as an incident. Consequently, the plan should include information about incidents that could later develop and trigger activation criteria.

The activation criteria should be implemented in the strategic, tactical, and operational plans so that the organization has a consistent approach to identifying, assessing, and escalating risks and incidents. The strategic, tactical, and operational teams may not always activate their plans simultaneously. For example, activation may start with the operational team, escalate to the tactical team, and then on to the strategic team. Alternatively, activation may begin with the strategic team and cascade down to the operational teams. Authority to declare a crisis should be documented in the strategic plan.

It is better to mobilise a team promptly and stand down if not required, than it is to mobilise too late or not at all. Therefore, each plan should include criteria for standing down the team.

Team Meeting Facilities

Based on its operating model and environment, the organization should ensure that appropriate team meeting facilities are available to manage the response to an incident. To save time and avoid confusion during an incident, each team should know in advance where and how they should meet. At least two meeting options should be predefined. The location could be physical or virtual.

The team leader can decide on the most suitable meeting location based on the situation.

The availability of the following resources should also be considered when setting up a meeting facility for physical meetings:

- Transport to and from the location.
- 24-hour access.
- Physical security.
- Work and meeting facilities, such as desks and tables.
- Lighting, heating, and/or cooling.

- Personal hygiene items.
- A continuously available and stable power supply.
- An appropriate number of telephones (mobile, landline, and satellite).
- Video conferencing equipment.
- Access to corporate systems and printers.
- Mobile chargers.
- Sim cards from alternate telecom providers.
- A robust Internet connection (preferably independent of the organization's normal Internet service provider).
- Computers/laptops, television, radio, and satellite telecommunications as required.
- Electronic or physical versions of relevant plans and documents, including log sheets and urgently required information.
- Whiteboard/flip charts, templates, and pens (or collaborative electronic equivalent) for recording incident details, actions taken, and decisions made by the team.

For incidents requiring involvement for a longer period, the following should also be available:

- Refreshments.
- Sleeping facilities on-site or nearby.

Overview of Plan Types

The table below describes various types of strategic, tactical, and operational plans:

*Examples of possible owners are provided but there should only be one owner (role or department) of each plan.

Table 9: various types of strategic, tactical, and operational plans.

Plan type	Plan name	Definition	Typical owner*	Response team
Strategic plan	Crisis management plan	Defines the framework for managing strategic issues resulting from an incident.	Crisis management team leader	Crisis management team
Strategic plan	Crisis communications plan	Sets out how communications to key stakeholders (internal and external) will be managed at the time of the incident.	Public relations manager, external affairs manager, communications manager	Crisis communications team
Tactical plan	Alternate work area plan	Describes how to coordinate the preparation of one or more facilities in anticipation of relocating multiple business units, including remote work capability.	Facilities manager	Facilities team, ICT team
Tactical plan	Transportation plan	Describes how the transportation of personnel and products from multiple business units to one or more alternate facilities will be coordinated.	Facilities manager	Facilities team, corporate security
Tactical plan	Procurement plan	Describes how resources will be sourced and allocated when a supplier disruption affects multiple business units.	Procurement manager	Procurement team

Plan type	Plan name	Definition	Typical owner*	Response team
Operational plan	Business unit recovery plan	Provides direction on continuing business activities (and processes) to deliver products and services when a facility, technology, people, or suppliers are unavailable.	Business unit manager	Individual business units
Operational plan	Emergency response plan	Describe the steps to be taken to protect life and safety and to secure the facility.	Facilities manager	Emergency response team
Operational plan	Technology recovery plan	Identifies the steps to be taken in response to the loss and for the subsequent recovery of the technology infrastructure, such as network, systems, applications, data, and telecommunications to support business activities.	ICT manager	ICT disaster recovery team
Operational plan	Warning plan	Describes how to notify people of an incident, or the possibility of an incident, so that they can take action to protect themselves and/or participate in the response to an incident.	Facilities manager, HR Manager, or ICT manager	Facilities team, HR team, or ICT team
Recovery return to BAU plans	Recovery plan	Describes how to return the business processes to a normal state from the temporary measures deployed during the response to the disruption.	BC business unit manager	Crisis management team
Scenario specific plan	Pandemic plan	Describes how to manage a disease outbreak.	Pandemic response manager	Pandemic team (comprises BC, HR, facilities, health and safety)
Scenario specific plan	Product recall plan	Sets out the procedures to be followed when there is a health or environmental issue with the product.	Managers of: quality, regulatory, operations, or production department	Product recall team
Scenario specific plan	Hazardous material spill	Describes the procedures for managing a spill that may impact health, safety, and environment safety.	Health and safety manager	Health and safety team
Scenario specific plan	Cyber incident response plan	Describes how to manage compromised systems or data at the technical level.	Information security manager	Information security team

Outcomes and Review

The outcomes of developing and managing plans include:

- An overview of the plans required for the organization.
- An overview of the structure and content of each plan.
- A process for developing plans.

A review of the development and management of plans should also be performed following a crisis and whenever the organization undergoes significant change.

Strategic Plan

A strategic plan defines how strategic issues (for example, those threatening the organization, its integrity, and viability) resulting from an incident should be addressed and managed by the strategic team.

A strategic plan is often referred to as a crisis management plan and might be supported by other strategic plans such as a crisis communication plan. The BC professional is usually tasked with developing the strategic plan in consultation with a variety of other senior managers. Depending on the response structure, there may be more than one strategic plan. For example, country, regional, and corporate crisis management plans may exist.

Some incidents do not involve physical disruption to the organization and may not require the activation of an operational or a tactical plan. Examples could include fraud, malpractice, or negative media exposure that threatens the organization's reputation.

There may also be incidents that result in the mobilisation of one or more operational teams which do not require the mobilisation of the strategic team. However, it is good practice, especially where there is the potential for reputational damage, to make the strategic team aware of the situation in case it escalates.

The strategic plan should describe the process for handling all types of crises stemming from an incident (anticipated and unanticipated) that require a strategic response. It may also contain checklists, actions, decisions, and communications needed in response to specific scenarios appropriate to the organization.

General Principles

To develop effective strategic plans, the organization should adhere to the following principles:

- A strategic plan should be concise but contain sufficient guidance to help those responsible for executing it. The plan should allow flexibility in responding to anticipated and unanticipated situations. It should also address strategic issues impacting people, organizational integrity, core objectives, and prioritised products and services.
- The strategic plan should address the need to communicate with interested parties. It is common for organizations to develop a separate crisis communications plan which is sometimes incorporated into the strategic plan.

Concepts and Considerations

During a crisis or incident, the strategic team is accountable for the welfare of people, the organization's stability, continuity of operations, and integrity. In addition, it is responsible for implementing and adjusting response activities to achieve the best possible outcome for the organization.

Specific responsibilities of the strategic team that should be captured in the plan include:

- Evaluating the situation to determine if it is a crisis.
- Declaring the crisis, if applicable.
- Determining the need to mobilise the strategic team.
- Mobilising, guiding, and, if necessary, supporting the tactical and operational teams as required.
- Establishing the strategic response to the incident and adjusting it as required.

- Making major financial decisions and approving extraordinary expenditures during response and recovery.
- Setting overarching objectives that are communicated throughout the organization when responding to a crisis.
- Ensuring compliance with legal and regulatory requirements.
- Monitoring the overall response by operational and tactical teams to ensure that they meet the organization's requirements.
- Monitoring and adjusting the communications strategy as necessary and approving external statements before they are issued.
- Monitoring the financial health of the organization, if relevant.
- Adapting strategies based on the specific situation. These should align with the long-term objectives of the organization.
- Identifying and declaring when the crisis is over, directing response teams to stand down, and ensuring that the end of the crisis is communicated to all interested parties.
- Conducting a debrief to ascertain what went well, what can be improved upon, and following up on corrective actions captured in an after-action report.

Crisis Communications Plan

There should be a separate crisis communications plan as the communications team will often work in parallel with the strategic team. However, some smaller organizations prefer to include the crisis communications plan as part of the strategic plan because response is being guided by the same top management. A crisis communications plan may also cover communications during an incident which has not been declared a crisis.

Tasks within the crisis communications plan should be allocated to one person or a team and should include:

- Appointing a member to serve on the strategic team to advise on the communications strategy.
- Developing internal and external messaging. Ensuring these messages are cascaded throughout the organization and, when required, outside the organization to ensure consistency.
- Monitoring, liaising, and facilitating interactions with the media.
- Social media monitoring and engagement.
- Updating the website with information on the crisis. This could include the latest updates, actions pertaining to the organization and interested parties, and alternative ways of working.
- Receiving and logging incoming communications.
- Preparing and briefing the designated spokesperson(s).

The organization may work with external specialists, such as public relations organizations, to develop the communications strategy and response.

Communication volume, type, and urgency from crisis to crisis can vary significantly. Therefore, the crisis communications plan can accelerate the response process if it includes pre-formatted messages or pre-written holding statements.

The crisis communication plan should:

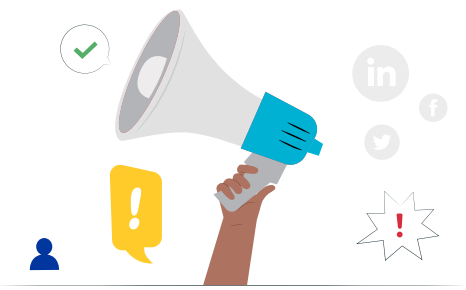
- Anticipate much of the information required by known interested parties, for example, personnel, customers, and shareholders.
- Contain pre-written statements for these anticipated communications, allowing messages to be adapted to individual requirements.
- Contain answers to general questions that are applicable in most incidents.
- Contain a general background statement about the organization, which can be distributed publicly.
- Develop a website or hidden web pages which can be activated during a crisis and be used as a focal point to communicate specific and relevant information to the workforce. Consider hosting this on a separate independent platform.

Outcomes and Review

- A plan(s) that enables the strategic team to stabilise the situation and control the response.
- Details regarding how communications are coordinated internally and externally.
- A plan that ensures the organization complies with legal and regulatory requirements.

Strategic plans should be regularly reviewed and validated through exercises. The strategic team must also participate in regular training and exercises to build and maintain the required competence.

A review of the strategic plan's effectiveness should also be performed following a crisis and whenever the organization undergoes significant change.



Tactical Plans

Tactical plans facilitate the coordination of response activities when several operational teams are involved. The tactical plan should include consolidated resource requirements and time frames defined in the operational plans so that recovery can be monitored and reported. In addition, it should identify the possible options to coordinate the response effort and any resulting needs.

The following are examples of tactical plans and their resource requirements:

- **Alternate work area plan:** coordinating the preparation of one or more facilities in anticipation of relocating multiple business units. This might include specific technology requirements for remote work and communication.
- **Transportation plan:** coordinating the transportation of personnel and products from multiple business units to one or more alternate facilities.
- **Procurement plan:** coordinating how resources will be sourced and allocated when a supplier disruption affects multiple business units.

In large organizations these tasks may be carried out by a tactical team, while in smaller organizations the strategic team may perform these tasks.

General Principles

Note that the tactical team can be mobilised even if the strategic team is not.

To develop effective tactical plans, the BC professional should adhere to the following principles:

- The tactical plan should focus on coordinating the activities of the involved operational teams to ensure they work together effectively. Tactical plans must also incorporate supplier-related solutions agreed upon in the Solutions Design stage (PP4).
- When there are multiple operational plans, one of the roles of the tactical team is to overview response activities by the operational teams to ensure that the response remains focused and coordinated. The tactical team may alter the agreed priorities and solutions if directed by the strategic team. Similarly, the tactical team should inform the strategic team when requirements have changed.

Concepts and Considerations

Tactical plans focus on coordinating the recovery of a group of interrelated activities defined in operational plans. They can be used to address the coordination of response activities in single or multiple locations.

The tactical plan should include consolidated resource requirements and timeframes defined in the operational plans so that recovery can be coordinated, monitored, and reported. The tactical plan may also contain details of services which could be deployed to support the operational plans.

Such services could include:

- Sourcing company-wide welfare services.
- Financing or leasing alternate locations.
- Rapid transitioning of technology.
- Providing transportation and logistical support.
- Approving alternate suppliers.

The responsibilities of a tactical team that should also be captured in the plan include:

- Supporting the strategic team.
- Coordinating operational teams within the scope of the tactical plan.
- Providing an interface between the strategic and operational teams.
- Requesting or receiving progress updates and other information from the operational teams.
- Reviewing and consolidating operational reports and providing updates to the strategic team.
- Allocating available resources. Resolving or escalating resource issues as appropriate.
- Identifying and then mobilising agreed specialist service providers, for example, providers of alternative premises, alternate manufacturers or providers of raw materials, damage management or salvage companies, data recovery, or counselling services, as required at the request of operational teams.
- Sourcing extra resources when required (for example, people, products, services).
- Standing down the tactical and operational teams when appropriate.

Outcomes and Review

The outcome of developing a tactical plan is a plan for coordination and reporting of response activities, as well as resource acquisition and allocation between multiple operational and strategic teams.

The tactical plan should be regularly reviewed and validated through exercises. The tactical plan's effectiveness should also be reviewed following an incident or significant organizational change.

People Welfare Aspects in Emergency Response Plans

Organizations have a duty of care to safeguard the health, safety, and welfare of their personnel, contractors, visitors, customers, and members of the public. In some countries and industry sectors, this is a legal requirement.

The issues listed below may be included in the emergency response plan or be incorporated into the body of a more general plan.

During an incident and where relevant, one or more team members should be assigned responsibility for:

- Verifying the results of site evacuation.
- Accounting for the organization's personnel and visitors.
- Communicating with personnel and others on site.
- Communicating with emergency services.
- Setting up communications systems, for example, a helpline or intranet pages.
- Ensuring next of kin are contacted per local rules and regulations.
- Arranging transport or other immediate practical assistance as required.

Subsequently, there may be additional needs to consider, including:

- Dealing with issues relating to casualties, in consultation with the emergency services and per local regulations and customs.
- Counselling and rehabilitation services (which may be provided as part of existing personnel benefits).
- Liaising with specialist services when dealing with next of kin.
- Providing family support (especially in the case of injuries or casualties).
- Providing temporary accommodation.
- Having translation services.
- Accessing emergency cash or facilities.

Operational Plans

There are various types of operational plans with differing names, scopes, and owners. The BC professional is typically not responsible for producing all these plans. However, the BC professional will need to make sure these plans are consistent in structure (for example, via a template), are available, and work together.

Operational plans may also be designed to maintain the organization's ability to function in specific situations (for example, unavailability of a critical system or key equipment failure, a localised natural hazard, or hazardous material spill).

General Principles

To develop effective operational plans the organization should adhere to the following principles:

- Operational plans protect people, property, and the environment, while supporting the recovery of the organization's prioritised activities.
- Business unit and technology recovery plans are based on the BC requirements defined in PP3 in combination with modifications as agreed in PP4.

Concepts and Considerations

Most operational plans apply to multiple locations, while others apply to a specific site, such as emergency response plans.

The level of detail contained in any operational plan is dependent upon the following:

- The complexity of the procedures to be followed.
- The RTO.
- The complexity of the processes to be recovered.
- Team member competency.

The development of operational plans should consider:

- Using a plan template. It encourages standardisation of documentation but also allows for variations where appropriate.
- Documenting interdependencies between operational, tactical, and strategic plans. For example, reliance on a tactical team for a critical decision.

Outcomes and Review

The outcomes of developing operational plans include the ability to:

- Respond to emergencies, including threats to life, property, or the environment.
- Recover disrupted activities.
- Recover technology infrastructure, systems, data, and services.

The operational plan should be regularly reviewed and validated through recurring exercises. In addition, the operational teams must participate in regular training and exercises to build and maintain the required competence.

A review of operational plan effectiveness should also be performed following an incident and whenever the organization undergoes significant change.

Process for Returning to BAU

"The organization shall have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption," (ISO 22301:2019).

The business and technology recovery plans previously focused on activating the solutions during an incident but do not describe the process for returning to the original state, also known as BAU. Producing detailed plans for returning to BAU is a challenge as the state of the primary resources during the incident cannot be predicted.

The organization should consider its increased vulnerability when its primary resources are lost during an incident.

Before any incident, a plan outlining possible options and processes for returning to BAU[1] should be developed. However, the details can only be specified when the impact of the incident is clear.

The following diagram provides an overview of situations requiring BAU plans.

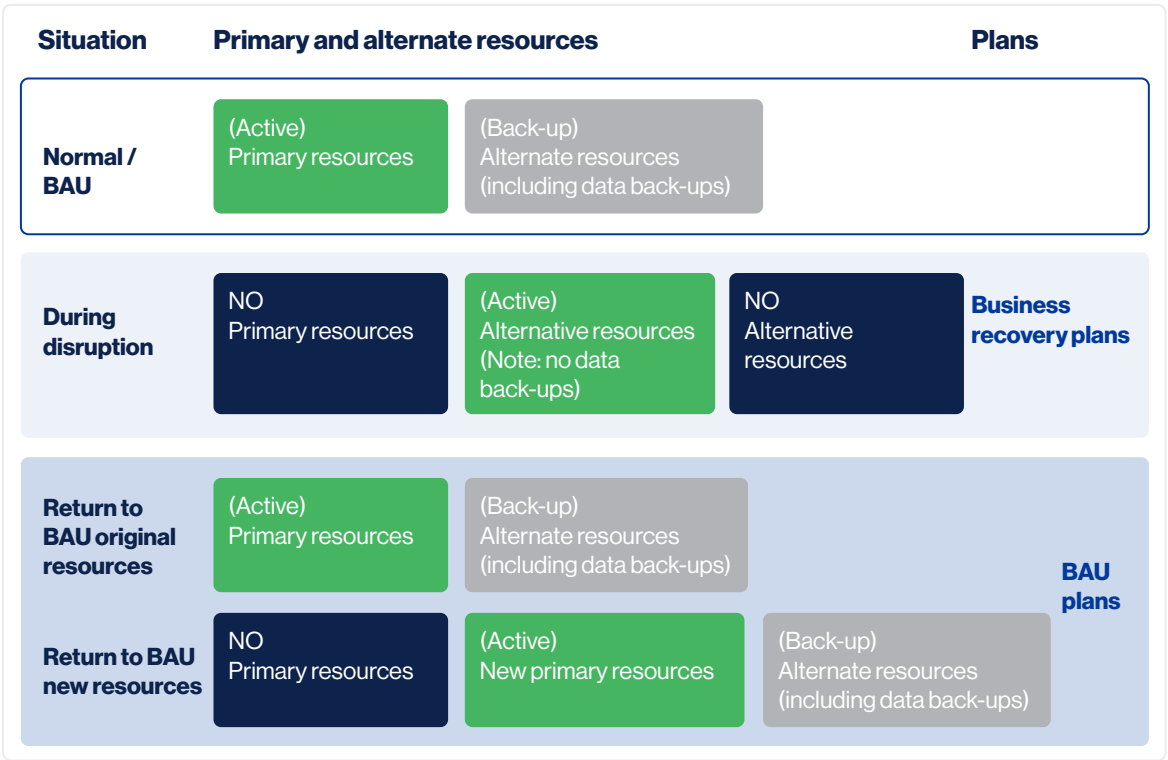


Figure 2: situations requiring BAU plans.

1 It should be noted that the definition of BAU may change to a 'new normal' as a result of the incident.

General Principles

The organization should develop an outline of the possible options and processes to support the return to BAU.

These include:

- Returning from alternate resources to primary resources.
- Dealing with long-term or permanent unavailability of primary resources.
- Resumption of activities with a lower priority or a longer RTO.
- Taking into account new vulnerabilities resulting from impacted resources.

Methods and Techniques

The following actions may support a return to BAU:

- Validating that the primary resources are available and meet BC requirements.
- Reviewing dependencies and possible phasing of returning to BAU.
- Preparing plans to deal with long-term or permanent unavailability of primary resources.
- Considering insurance policy cover and requirements.
- Reviewing those activities that have not been recovered yet.
- Examining new vulnerabilities resulting from impacted resources.

Outcomes and Review

The outcomes of developing a process for returning to BAU include:

- The organization understands the steps required to prepare for a return to BAU.
- Outline plans for returning to BAU in various situations have been prepared and can be further developed during a disruption.

The process and outline plans should be regularly reviewed and validated through recurring exercises. In addition, the teams must participate in regular training and exercises to build and maintain the required competence.

A review of the process and outline plan's effectiveness should also be performed following an incident and whenever the organization undergoes significant change.

Plans for Specific Situations

An organization may develop plans to deal with specific situations such as a cyber incident, a disease outbreak, or a product recall. In addition, in some countries or industries, there might be regulatory or customer requirements to have a specific plan.

General Principles

A specific plan should follow the guidelines for developing and managing plans.

Furthermore, a situation-specific plan should:

- Adhere to the organization's defined response structure.
- Align with the organization's strategic plan.
- Adjust to as many variations of the situation as possible.
- Utilise existing solutions where possible. The organization must design and implement new solutions if these are insufficient.

Concepts and Considerations

- A situation-specific plan may need to incorporate operational, tactical, and strategic aspects of the response efforts.
- Additional team members with subject matter expertise may be required.
- The situations described in the situation-specific plans can be used as a basis for exercises.

Methods and Techniques

Product Recall Plan

Procedures for a product recall may include:

- Determining which products are (possibly) affected.
- Determining the locations of the (possibly) affected products.
- Stopping products in transit from becoming available to the consumer.
- Removing (and returning) affected products.
- Offering refunds or replacements.
- Dealing with queries and complaints.
- Supplying alternatives.
- Gathering intelligence regarding possible impacts.
- Working with suppliers/partners (note: the supplier may be the cause of the recall).
- Having communication and reporting protocols in place.

Cyber Incident Response Plan

Details that could be included in a cyber incident response plan are:

- Indication of how the cyber response team relates to the broader response structure.
- Scenario-based, pre-arranged decisions, such as a reply to a ransom request or website defacement attack.
- In the case of data loss, communication protocols to reach out to affected or interested parties (e.g. customers whose data has been lost), or external stakeholders such as the media in the event the attack becomes public.
- Alternate communication channels in case the attack has caused a disruption to ICT systems.
- Criteria, responsibilities, authorities, and procedures for the activation of 'kill switches' for applications and networks. This could include timings for shutdowns.
- Details of regulatory reporting requirements in case of cyber incidents, including timescales.
- Details of the insurer and their requirements during a cyber incident.
- Processes to manage the liaison with law enforcement and government agencies.
- Contact details of suppliers and partners who may be either affected by the attack or the initial access point for cyber criminals. In both instances, there should be processes in place to deal with the consequences of the attack.
- Data storage and back-up procedures that might help restore data in case it is lost or stolen.
- Procedures for dealing with cyber incidents caused by or involving suppliers and partners.
- Liaison processes with cyber incident response teams to coordinate the response.
- Active monitoring of the attack, considering factors such as its extent within the organization and its operating environment (e.g. other similar organizations in the same industry).

Infectious Disease Plan

Details that may be included in an infectious disease plan are:

- Continual monitoring of the situation.
- Monitoring the development of global and local (health) rules and regulations.
- Determining, implementing, and procuring medical/ hygiene measures and supplies.
- Determining travel protocols, including cross-border travel to/from work.
- Determining criteria for being allowed to work on-site or off-site (including team-splitting).
- Dealing with security requirements to allow work to be performed off-site.
- Determine criteria and the procedure for closing sites.
- Determining protocols for visitors and suppliers who need to be on-site.
- Keeping updated on the situation regarding suppliers/partners.
- Monitoring the effect on customers and the market and determining procedures to manage the impact.
- Monitoring and managing the effects on the global supply chain and transportation.
- Ensuring availability and security of off-site facilities.
- Procedures for monitoring the well-being of staff.
- Procedures for monitoring and dealing with issues associated with the return of working on-site.

Outcomes and Review

The outcome of a plan for a specific situation is a set of instructions that help the organization deal with the agreed specific situation and variations thereof.

The outcomes of developing plans for specific situations include the ability to:

- Respond to specific situations.
- Recover disrupted activities in these specific situations.

The plans for specific situations should be regularly reviewed and validated through recurring exercises. In addition, teams must participate in regular training and exercises to build and maintain the required competence.

A review of plans for specific situations should also be performed following an incident and whenever the organization undergoes significant change.

BCI Professional Practices

PP6: Validation

Validation is the PP that confirms the established BCMS meets the objectives set out in the policy and enables the organization to embrace BC through an effective and efficient awareness, exercising, maintenance, and review programme.

Validation ensures the findings of the analysis are proportionately and reasonably reflected within BC Solutions Design and that the implemented solutions, in combination with the response structure and BC plans, work according to the agreed specifications and are commensurate with the size, complexity, and type of organization. Validation provides methodologies to measure the quality and effectiveness of the BCMS and BC capability, the competence of individuals, and team cohesiveness. A positive approach and attitude toward Validation will allow strengths to be acknowledged and areas for development to be seen as opportunities for continual improvement rather than criticism.

Introduction

Validation is achieved through a combination of the following activities:

- **Exercising:** the process to train for, assess, practice, and improve organizational performance (ISO 22300:2021).
- **Maintenance:** the process to ensure organizational BC arrangements and plans remain relevant and operationally ready to respond.
- **Review:** the process for assessing the suitability, adequacy, and effectiveness of the BCMS and identifying opportunities for improvement.

The advantages of Validation include but are not limited to:

- An organization-wide awareness of BC objectives and broader organizational strategic objectives.
- The identification of and investment into specific roles and responsibilities that support BC to become embedded within the organization.
- Comprehensive exercise and assessment programme analysis to support additional learning and training to improve competencies and behaviours. A maintenance and review programme to ensure policies, procedures, and documents are current and evaluate the continuing suitability, adequacy, and effectiveness of the BCMS.

Developing an Exercise Programme

An organization's continuity capability cannot be considered reliable or effective until exercised. No matter how well-designed a BC solution or BC plan appears, realistic exercises should be used to help identify issues and validate assumptions that may require attention. Exercises aim to continuously improve BC capabilities and competency by ensuring that lessons learned are integrated into prevention, mitigation, planning, training, and future exercises.

Planning and delivering exercises present excellent opportunities to further embrace the BC programme by engaging participants before, during, and after the activity in a comfortable learning environment.

General Principles

Exercises aim to achieve various outcomes, including:

- Evaluating the organization's capability to undertake continuity activities and achieve the expected recovery objectives (for example, RPOs and RTOs).
- Validating the BC solutions and considerations.
- Verifying the procedures documented in the BC plan are relevant, complete, and current.
- Verifying the adequacy, availability, and capability of resources that support continuity solutions.
- Identifying missing or outdated information, as well as areas for improvement.
- Validating roles and responsibilities of the response and recovery team members.
- Improving the competency of those with response and recovery roles.
- Building confidence in the recovery team members.
- Developing teamwork.
- Raising awareness of BC and the importance of exercises for personnel to improve the BC culture of the organization (PP2).

Exercises are not a one-time activity. Instead, they should be scheduled and programmed into a series of events and activities, allowing the organization to improve capability and competency gradually over time.

An exercise programme should ensure the desired capability of an organization by:

- Rehearsing all plans.
- Verifying all BC solutions.
- Verifying all information contained in plans.
- Exercising communication and coordination between teams (for example, response and recovery) to improve the effectiveness of working together.
- Exercising with all relevant personnel as outlined in the BCMS (including deputies).
- Identifying ways to evolve all elements of the BC programme over time.

The exercise programme should begin with simple activities to raise general awareness and understanding. Once sufficient awareness has been provided, the exercise schedule should mature over time into more complex and challenging activities. Exercise programmes should use a combination of methods and techniques to achieve the outcomes outlined in the PPs leading up to PP6.

The exercise programme should include suitable exercise elements, including:

- **Technical:** do all required systems and equipment work?
- **Procedures:** are tasks or steps within a plan or document correctly delivering the BC requirements?
- **Logical:** do procedures work together logically?
- **Timeliness:** can the procedures achieve the target RTO for each activity?
- **Actionable:** are the procedures practical, current, understandable, and implementable?
- **Personnel:** do the individuals involved have the required competencies and authority? Does everyone know their role and responsibility?
- **Capabilities:** is the supply of required resources known and reliable?
- **Information:** is all necessary information available to implement the plan? Can it be understood by any person that has to rely on it?
- **Workplace/location:** do the procedures consider different working arrangements, such as regular office locations (on-site), alternate locations (off-site), and work from home?
- **Participants:** do the exercises assess the roles of all teams involved (e.g. strategic, tactical, and operational teams)? Are the exercises relevant to the competencies of the participants?

The exercise frequency is defined as scheduled in the BCMS, influenced by the size, complexity, and type of organization (e.g. all plans should be exercised at least annually, while plans with an MTPD of less than 24hrs should be exercised every six months).

Prioritised products and services, processes and activities, and every member of the response teams should be involved in exercises commensurate with the exercise schedule.

Concepts and Considerations

The organizational BC policy will establish how the exercise programme should be planned and managed, as well as identifying any necessary training and resources.

Where product or service delivery is outsourced, accountability for ensuring the exercising of arrangements remains with the product or service owner. The organization should make sure, through exercises, that the outsourced company can continue to meet its obligations in the event they are disrupted. It may be appropriate to consider joint exercise arrangements with outsourced service providers and key suppliers. In addition, if other suppliers of prioritised products and services, processes, and activities have been identified in the Analysis stage (PP3), they should be asked to demonstrate their BC capability through their exercises. Evidence of BC capability may include requesting details of the BC exercise (for example: date and time it was held, participants, scenario/s used, expected outcomes) and/or copies of the latest exercise report (which documents the exercise outcomes, issues log, assigned owners, and due dates for resolution) to determine if satisfactory checks and balances are in place and that the BC capability meets organizational requirements. Organizations that may suffer from large-scale global events should consider a response that operates across different cultures and time zones. Exercises should ensure the effectiveness and consistency of the response across the entire organization.

Considering the results of the Analysis (PP3) of the supply chain, exercises involving supplier continuity arrangements should consider the **following aspects:**

- The priority level of the supplier and the required recovery time according to the BIA (PP3).
- Dependencies of the key supplier on other suppliers for respective products and services.
- Supply chain continuity risk (for example, a single supplier for the product or service).
- The documented recovery plan for the supplier's facilities.
- The location of the supplier's facilities.

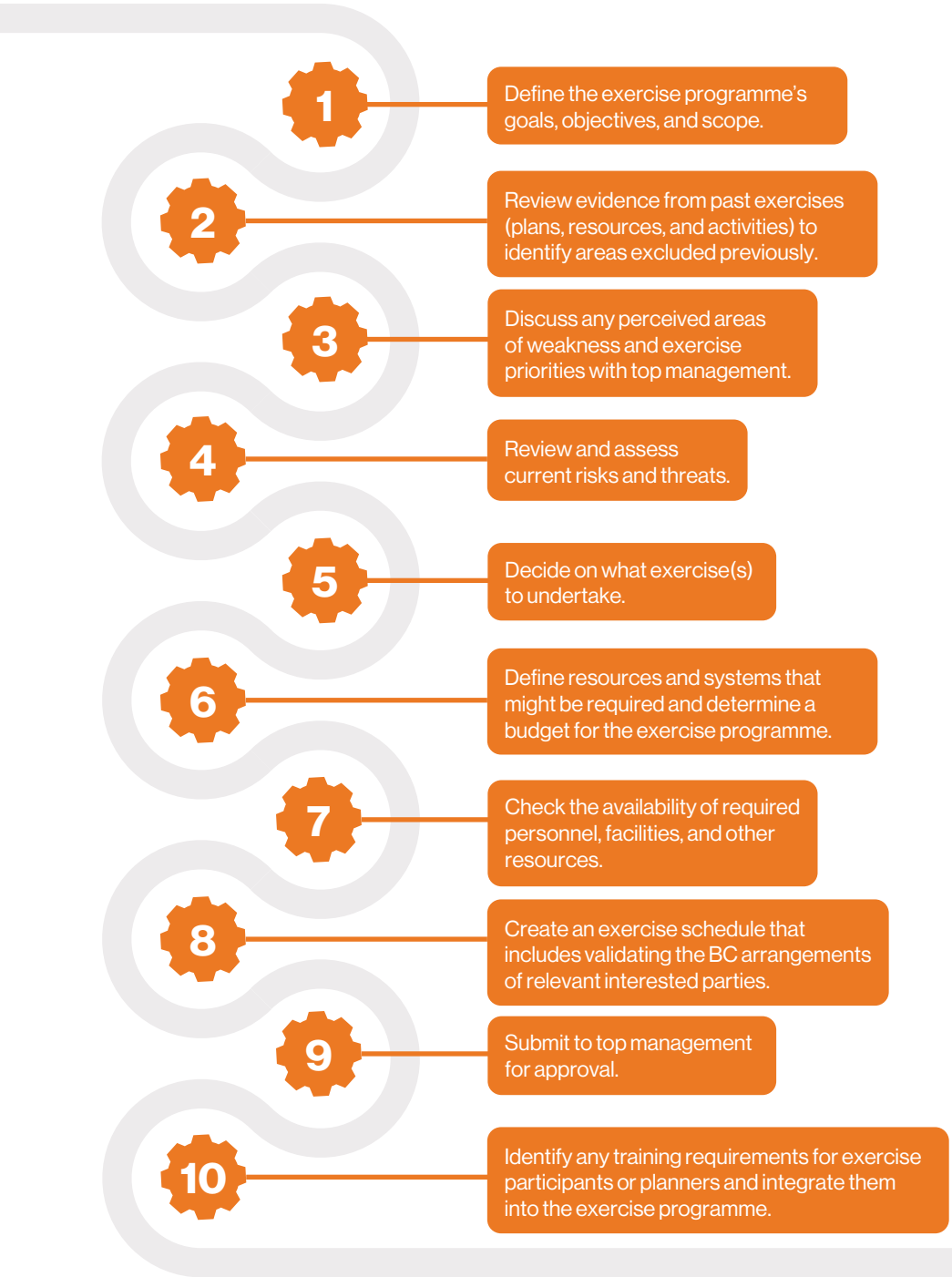
Where exercises are not performed jointly with suppliers, the following should be considered to ensure supply chain continuity:

- The recovery plan of the supplier considers exercise scenarios.
- The exercise activities are enforced through an SLA.
- Results from the recent exercise(s) conducted by the supplier are shared.
- Independent assessment/audit reports of the supplier's continuity management are conducted.

ISO TS 22318:2021 provides more detailed guidance on SCCM.

Process

The following should be considered in the exercise process:



Methods and Techniques

When developing an exercise programme, it is vital to choose exercise methods and techniques that fulfil the aim and the BC requirements (PP3) and are also approved by top management.

Exercises can be performed:

- In person at an organization's physical site, or
- In a virtual environment via conference calling technologies, which is often referred to as a 'virtual exercise'. If an exercise cannot be performed in person (for example, due to geographic, participant availability, and physical security/safety limitations), executing a virtual exercise is an acceptable alternate method. Virtual exercises can also be the preferred method if the team would not ordinarily be together in the event of a response.

The most straightforward exercise technique is a **'walk-through'**, where participants read through and check the plans/procedures. **'Table-top'** is also a typical exercise technique in which participants review and discuss the actions to take without performing them. This discussion can be over the table (for example, in a meeting room) or virtual.

Types of Exercise

This section details the methodology behind the different types of testing. Exercises can have different names, but, in principle, they fall into the **following five categories:**

- Discussion-based,
- Scenario,
- Simulation,
- Live, and
- Test.

These category types can be applied for BC and other disciplines, such as exercises by ICT disaster recovery and cyber security teams involving cyber attacks (for example, ransomware and distributed denial of service attacks). These exercise types have common features and organizations may find it appropriate to combine elements from different categories to achieve their exercise objectives.

Discussion-based

Discussion-based exercises are the simplest to organize and facilitate, as well as being the least time-consuming of all the exercise categories listed above. They are structured events where participants can explore relevant issues and walk through plans in a low-pressure environment. A low-pressure environment builds confidence and competence before escalating to a live exercise. This exercise type can focus on a specific area for improvement in order to find a preferred solution.

An example of a discussion-based exercise is a plan review. The review should be performed by the plan owner, together with those involved in the plan.

Participants should refresh themselves on the content and ensure:

- Planning assumptions do not need alterations (following any significant organizational change, event, or new BIA outcomes).
- The recovery steps within the plan continue to be valid as they collectively meet the plan's objective.
- Plan resources continue to be available.
- Names, roles and responsibilities, and contact details are up-to-date and accurate.
- Changes, if any, are highlighted and actioned.
- Appropriate sign-off for the plan is obtained.

Scenario

A scenario is: "A pre-planned storyline that drives an exercise, as well as the stimuli used to achieve exercise project performance objectives," (ISO 22300:2021). A scenario exercise is conducted using a scenario with a timeframe. The exercise may either run in real-time or include time 'jumps' to allow different scenario stages to be exercised. A scenario exercise is usually conducted in a table-top environment. Participants are expected to be familiar with the plans being exercised and must demonstrate their understanding of how the plans work as the scenario unfolds. The excercise can involve a practical rehearsal of relevant response activities, such as completing assessment checklists, using log sheets, or writing media release statements.

Realistic scenario exercises are a cost-effective and efficient method as they can be done with lower costs than simulation exercises to obtain the results. Scenario exercises can be enhanced using media and other injects to make a scenario more realistic. The response teams may produce practical outputs, such as media releases or employee communications, during the exercise. For instance, exercises involving cyber security scenarios can be documented as a dedicated document known as the cyber crisis management plan (CCMP) or cyber incident response plan (CIRP), or these exercises can be part of the information technology disaster recovery (ITDR) plan.

Simulation

Simulation is defined as an: "Imitative representation of the functioning of one system or process by means of the functioning of another," (ISO 22300:2021).

Simulation exercises are operations-based exercises designed to be more realistic and challenging. They can be carried out in the normal operational environment, alternative premises, or command centres (ISO 22313:2020) and involve key participants - not everyone is required. The exercises can be undertaken within a controlled test environment simulating a production environment, provided this does not jeopardise the integrity of the assessed objectives.

Simulation exercises are more elaborate and can involve strategic, tactical, or operational teams. During a simulation exercise, participants are given information in a way that simulates an actual incident. In addition, scenario details and questions from interested parties such as personnel, customers, and the media can be introduced into the exercise using various platforms, such as phone calls, emails, social media, and TV news.

For example, a typical scenario could be a phishing email simulation where a sample of users evaluate their response to this type of cyber attack.

The use of roleplay can bring an additional level of reality to the exercise by simulating the interaction with key interested parties, such as customers, the workforce, the media, regulators, and suppliers.

Participants manage updates or requests for information as if it were an actual incident and develop and implement a suitable response to the unfolding scenario. Simulation exercises also allow participants to rehearse relevant procedures in detail. These may include notification and escalation procedures, decision-making, communications, media response, and assessing equipment and resources.

Live

Live exercises are always carried out in the normal operational environment, alternative premises, or command centres. Live exercises are designed to include everyone likely to be involved in the response as if it were real.

Live exercises can range from a small-scale rehearsal of one part of a response, for example, an evacuation, to a full-scale rehearsal of the whole organization, potentially involving interested parties in real-time. Live exercises can also validate operations at the DR site, including the movement to the DR site.

Live exercises are beneficial where there are legal or regulatory requirements or where a high risk to an organization has been identified, and the response plans need to be thoroughly evaluated. They are the most realistic way to improve the competency of individuals and exercise the plans. However, several challenges might mean a live exercise is not the most appropriate exercise format. The BC professional should undertake a risk assessment on the proposed live exercise to determine whether it is feasible to perform. For example, the logistics planning and execution resources required can be significant and there may be financial implications. Care should be taken to avoid disrupting the organization's BAU tasks and any reputational impacts should be considered.

Test

A test is defined as: "A unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned," (ISO 22301:2019).

It is usually applied to equipment, recovery procedures, or technology rather than teams or individuals.

The following are examples of tests:

- Activating the fire alarm.
- Rebuilding a server from back-ups.
- Switching a network device to the back-up system.
- Confirming recipients receive messages from the emergency mass notification system.

Outcomes and Review

The outcomes of developing and undertaking an exercise programme includes a complete exercise programme which defines the following:

- The objectives to be achieved.
- The methods required to achieve the objectives.
- The resource requirements (including budget).
- Proposed timing and training requirements.

The organization's exercise programme should be regularly reviewed at pre-agreed intervals or following significant change, as defined within the BC policy, to ensure that it is validating the effectiveness of the overall BCMS.

Developing an Exercise

General Principles

Every exercise within the exercise programme needs to be carefully planned to justify the use of resources required when developing and delivering it.

Therefore, the exercise development process should:

- Be approached like a project,
- Use appropriate planning steps, and
- Have controls associated with good project management practices.

Concepts and Considerations

Plausibility: exercises should be as realistic and plausible as possible. They should use the same procedures and methods as in an actual event. However, albeit ideal, it may not always be practical to run exercises without considering limitations pertaining to a date, time, environment, and participants.

Setting a realistic business scenario helps ensure that participants fully engage in the exercise and benefit from the experience. Selecting a realistic scenario should also help prove the validity of the plans. The person coordinating the exercise must use credible facts to ensure participants gain the most from the exercise through the realism of the scenario and supporting material. There may also be a surprise element to the exercise by providing little or no notice beforehand.

Technology products can enhance exercises and simulations, for example, by providing audio-visual injects.

Injects can be created and could include simulated media, such as news clips, website articles, social media feeds, telephone calls, emails, and text messages.

Introducing technology or external party injects can add an air of uncertainty and generate greater interest in the exercise. However, the addition of technology or external parties should not become a distraction from the agreed objectives of the exercise.

Managing risks: exercises should focus on maximising benefits and minimising the impacts of disruption. Exercises can sometimes disrupt BAU activities.

Those responsible for planning and managing exercises should ensure:

- The disruption caused by the exercise and any associated impact is planned, agreed upon, controlled, and minimised.
- The risk of something going wrong is understood and accepted by top management.
- There is a process to end an exercise quickly if any unintended disruption occurs.

Regarding ICT DR, the testing environment should be separated from the business operating environment to avoid disrupting ongoing business activities.

Costs and benefits: the cost of planning and running an exercise depends on the type of exercise selected. A more complex exercise typically requires more resources to plan and conduct and may involve more disruption to BAU activities. However, the exercise is likely to be more realistic and provide greater confidence in the effectiveness of plans and personnel capability.

Exercise objectives: the first step in preparing an exercise is determining the objectives and outcomes. Next, criteria should be defined for measuring the effectiveness of the exercise.

Measures can be both qualitative (assessing the quality of outcomes) and quantitative (achieving a specific, measurable outcome).

Examples of measures that can be used during an exercise include:

- The designated personnel can initiate the alert, invoke, and escalate the process.
- The on-duty manager can activate the callout procedure.
- The incident manager can call an initial management meeting.
- The response team members demonstrate effective decision-making capabilities.
- Key personnel can establish and maintain an incident log.
- A priority system is recovered and restored within the expected RTO.
- Departments resume service from an alternate site using the resources available.
- The response structure is established as defined within the BC plan.
- The roles and responsibilities are allocated as per the BC plan.
- Lines of communication are established with all interested parties.

Preparation: the scope and complexity of the exercise should determine the competencies needed by the team designing and running the exercise. Team members should ideally have good project management skills, exercise design and delivery skills, and know the organization or have experience within the industry sector.

Although it is often appropriate for an organization to develop and run exercises, other options can involve the engagement of external parties. For example, the emergency services may be willing to be involved in some exercise types, such as an evacuation drill or where the exercise scenario may have broader community impacts.

Whether internally or externally facilitated, an individual or team should be designated to run the exercise. This individual or team should manage the exercise following the exercise plan and schedule, initiating, and controlling the various stages as the exercise progresses. It is recommended that the person who plans and runs the exercise is not a participant in responding to the exercise. Lessons learnt from the previous post-exercise report(s) and post-incident report(s) should be examined and considered.

If the organization plans to perform a virtual exercise, it should ensure that all participants have access and can use the same technology platform or system to connect virtually prior to the exercise.

One of the key considerations of a virtual exercise is how the exercise can progress if technical issues are encountered. These issues can be addressed by performing test runs on the platform prior to the actual exercise.

Participants: those involved in exercises can include:

- Facilitators.
- Observers.
- Safety officers.
- Role players.
- Strategic, tactical, and operational level incident response teams.
- Departmental representatives.
- Suppliers of resources and services involved in the exercise.
- Emergency services.
- Emergency managers.
- Relevant subject matter experts.
- Auditors.

External support and participation: as the organization's exercise experience and BC capability increase, it may be appropriate to consider involving a more comprehensive range of interested parties in the exercises. For example, customers, suppliers, regulators, statutory and professional bodies, agencies, emergency services, and the voluntary sector.

The continuity capability of suppliers and outsourced activities that have been prioritised should be considered an essential part of validating the organization's BC plan. Including them in the exercise programme is not only part of ongoing relationship management with interested parties, but could form part of the legal, regulatory, or contractual arrangement.

Inviting observers and external visitors to participate in an exercise requires careful consideration. The advantages and disadvantages of allowing visitors to observe the exercise should be discussed with top management. In addition, the organization should consider any operational or reputational risks involved with external participation and any health and safety implications.

Although it is sometimes necessary to conduct an unannounced exercise, for example, an 'out of hours' call-out cascade, it is more common for exercises to be pre-announced to key participants to minimise the risk of the exercise causing unintended disruption. This also creates the opportunity for the BC professional to facilitate an exercise awareness session in the week leading up to the exercise. This will help new role holders

understand their role and refresh all participants in the documentation they will likely use. Awareness sessions help participants to be better prepared and embrace BC.

The warning time and the number of pre-warned participants may reduce as the organization becomes more confident in its BC capability.

Process

Although a range of different exercises are undertaken in the Validation stage of the BCMS, the following process can be applied to any individual exercise:

1. Agree on the exercise's scope, objectives, timeline, and expected outcomes.
2. Identify the exercise planning team and team roles.
3. Plan and design the exercise, including setting a budget and time frame, as well as conducting a RA to identify the risks of impact on BAU tasks, limitations, assumptions, and contingencies where appropriate.
4. Draft an exercise plan and have it approved by the appropriate management level.
5. Conduct the exercise and consider a session structure.

   For example:
   - A briefing that includes the importance of exercises (10% of the session duration).
   - The exercise (70% of the session).
   - A hot debrief (20% of the session).
6. Assess and report the outcome and lessons learned, including a debrief with the participants immediately after the exercise.
7. Follow up to address any issues the exercise raises and take corrective action as required.

Planning the Exercise:

BC exercise plans should consider the following key elements:

- **Objectives**
  - » What is the exercise trying to achieve?
- **Timeline**
  - » How long do you have to plan the exercise?
  - » How long do you have to deliver the exercise?
  - » Do you have any lead times to consider for participants or assets you may need to utilise?
- **Storyboard**
  - » Is a storyboard used with a timeline to develop the exercise scenario over time?
- **Participants**
  - » Are all the relevant participants available (or alternates where primary players may be unavailable)?

The individuals planning the exercise should prepare a timeline demonstrating how the exercise elements come together. This should be a chronological sequence of the steps that show when and how each event, action, or procedure should occur. The timeline can also list the anticipated participant response to an event, especially if this is defined in the BC plan. The individuals coordinating or facilitating the exercise use the timeline to ensure the exercise runs as planned and to prompt participants to refer to specific BC plan content or procedures so that they can be validated.

Individual timeline events are commonly known as 'injects', which can be delivered by the facilitator or role players.

Each inject should consider the following information:

- Exercise objective.
- Designated event time frame.
- Event description.
- The delivery method of the inject.
- Participants or teams who should receive the inject.
- Where relevant, expected responses from the participants or teams that reflect the BC plan.

Prior to the exercise start: all participants should be aware of what is required of them before, during, and after the exercise. Participants can be informed via written communication in advance of the exercise and a briefing at the start of the exercise. However, the briefing must not reveal information that may adversely affect the intended aim of the exercise.

Topics for the pre-exercise briefing may include:

- Exercise aims and objectives.
- Benefits to the participants and the organization of facilitating exercises.
- Roles and responsibilities during the exercise.
- Information, communication tools, and technology to be used.
- Action in the event of unforeseen circumstances.
- Post-exercise activities, including debriefing and reporting requirements.

To prevent misunderstanding or unintended organizational disruption, participants and the wider organization must be aware of when and where an exercise is taking place and that the incident is part of an exercise.

If the exercise requires that there is no or limited notice given, participants should be briefed as soon as possible after the exercise starts.

Starting the exercise: the start of the exercise should be clearly communicated to all participants and may involve the use of an announcement or an inject.

During the exercise: exercise events and injects should occur in a predefined way as outlined in the exercise plan and schedule.

Communication injects, such as telephone calls and emails, should include an obvious warning or code word such as 'exercise only' to ensure the information is not mistaken for a real message.

Suspending the exercise: it may be necessary to pause or stop an exercise. Participants need to understand how this may occur. One way is to use a distinctive code word which should prompt an immediate suspension. This should be a word not usually used within the work environment. For example, the term 'no duff' is sometimes used and is drawn from the military. The exercise may have to be stopped if participant safety is, or could be compromised, or where an actual incident or crisis has occurred.

For complex exercises, the individual or team responsible for planning and managing the exercise should ensure that there are agreed stop and go points at key stages throughout the exercise. These points can be applied if the team makes decisions that would not be appropriate in the given scenario or to re-focus if the participants have become distracted from the main exercise objectives. Taking time out to discuss exercise decisions or concerns can also be a valuable learning opportunity or can address a significant deviation from an expected participant action which could, if not rectified, affect the progress and successful outcome of the exercise.

Following a suspension, the exercise should be restarted or terminated.

Ending the exercise: the decision to end the exercise should rest with the individual or team facilitating the exercise. Consideration should be given to whether the objectives have been achieved within the allocated time frame for the exercise.

Sufficient time should be allowed at the end of the exercise for an immediate debrief.

Debriefing: the aim of exercise debriefing is for participants to share their experiences of the exercise and the scenario used so that lessons can be identified, agreed upon, and incorporated into the BCMS. Plans, procedures, training, and awareness activities can then be modified to reflect lessons learned and improve the organization's ability to respond to future incidents. This debriefing style should not be confused with a detailed investigation that may be used following an actual incident.

As part of the debrief, the exercise should be evaluated against the objectives defined when the exercise was planned.

It is essential that all exercise participants, regardless of seniority, are encouraged to contribute during the debrief and that they understand that debriefing is about improving effectiveness and not about assigning blame for any issues identified. The debrief should be carried out to promote organizational learning and encourage open and honest feedback.

Debriefing should:

- Respect the rights of the individuals.
- Value all participants equally.
- Acknowledge identified issues but focus on opportunities for enhancement.
- Follow-up individual, group, or organizational understanding and learning.

There are several ways of obtaining information for the debrief:

- **Hot debrief:** this is held immediately after an exercise, prior to personnel leaving the exercise location. It allows the participants to highlight various issues and concerns while still fresh in their minds.
- **Formal debrief:** this should be held within one week of the exercise taking place and may address wider organizational issues rather than individual or group concerns. It should look for strengths and weaknesses and ideas for future learning.
- **Surveys:** these can be issued to obtain feedback from participants. The surveys could contain a rating system that allows respondents to score the effectiveness of the exercise. Surveys are particularly helpful for participants who prefer to respond in writing or if an exercise group is spread over many locations. It also provides opportunities for reflective responses. A scoring system, if used, can allow for future benchmarking and performance reviews.
- **Interviews:** these should be held within one week of the exercise with identified key individuals, where further discussion is required regarding their roles, responsibilities, and feedback. The interview could be conducted one-to-one or with a small group of participants.
- **Post-exercise report:** the post-exercise report should be distributed to all exercise participants, other relevant personnel, and interested parties to ensure the organization accepts and addresses any lessons. In addition, the organization should create and seek top management approval for action plans to implement the prioritised recommendations, as they may involve changes to the broader BCMS.

For those industries with specific legal, regulatory, or licensing requirements for their business operations (for example, financial services), significant issues identified in an exercise may require the organization to repeat the exercise after corrective actions have been implemented. The key emphasis is that breaching applicable legal and regulatory requirements may leave interested parties vulnerable.

Outcomes and Review

The outcomes of the exercise development and delivery process include:

- An exercise plan or brief outlining the objectives, scope, roles and responsibilities, and approach to conducting the exercise.
- Exercise delivery materials and resources required to conduct the exercise.
- One or more completed exercises.
- A post-exercise report with recommendations for corrective actions.

The outcomes that exercises should seek to achieve will include:

- Confirmation that personnel are familiar with their roles, responsibilities, and authority in response to an incident.
- Validation of the BC plan's technical, logistical, and administrative aspects.
- Validation of the suitability of the continuity infrastructure (command centres, workplaces, technology, and telecommunications resources).
- Confirmation of the availability of personnel and processes for relocation.
- Greater awareness of BC, crisis management, and emergency response procedures.
- Greater awareness of the significance of BC.
- A proactive attitude of the plan owners toward implementing the lessons.
- Ideas for further exercises and scenarios relevant to the organization.

The exercise development process should be regularly reviewed at agreed intervals or following significant change, as defined within the BC policy.

Maintenance

Maintenance of the BCMS keeps the organization's BC arrangements up to date. This ensures that the organization remains ready to respond to and manage the impacts of incidents effectively, despite a periodic organizational change or a change in the organization's context.

General Principles

Maintenance activities should be embedded within the organization's BAU processes to be effective, rather than being a separate activity that may be overlooked.

Most of the maintenance required will be the result of organizational changes. The most effective way of achieving this is to incorporate maintenance activities into the organization's change management process. However, this is not always possible as many organizations do not have such a process. If a change management process exists, a timeframe should be agreed upon to implement any changes in the BCMS, with this updated when an exercise or incident review highlights deficiencies.

The triggers for maintenance include:

- Lessons learned through exercises.
- Changes to the organization's structure, products and services, infrastructure, processes, or activities.
- Changes to the environment in which the organization operates.
- A review or audit that identifies deficiencies or opportunities for improvement.
- An actual incident where lessons learned can be incorporated.
- Changes or updates in the BCMS, for instance, through the BIA or continuity solutions.

Concepts and Considerations

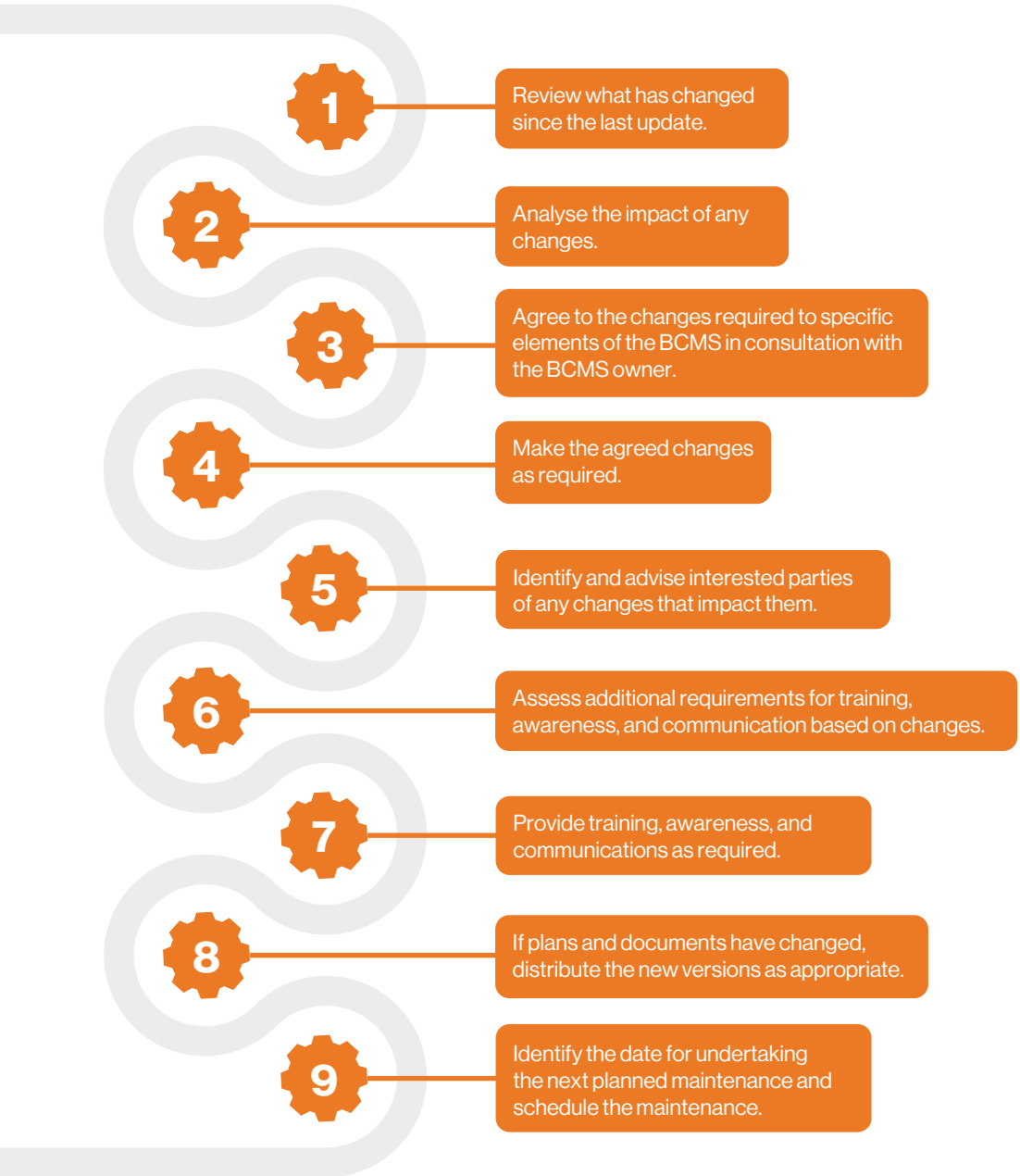
Besides these requirements, regular and planned maintenance is also necessary. The routine maintenance could consider activities like planned updates, back-up equipment checks, and a review of contracts undertaken at specified intervals over an agreed timeframe.

Process

There must be a formal process for maintaining the BCMS. The process should be undertaken at planned intervals and embedded into the organization's change management process. The frequency at which maintenance is carried out will depend on the nature and expected pace of change in the maintained activity.

For example, plans containing contact details may need to be maintained monthly or quarterly, whereas maintenance of the BC policy should be scheduled once a year.

Responsibility for undertaking the planned maintenance process should be given to an individual or team, who will:



The impact of any changes should be analysed by:

- Reviewing and challenging any assumptions that have been made.
- Determining whether any time objectives have changed, for example, MTPDs or RTOs.
- Determining the adequacy and availability of external services that might be required, such as asset restoration, recovery sites, and subcontracts.
- Reviewing the BC arrangements of key suppliers.

Methods and Techniques

Responsibility for maintenance should be given to the departmental representative for BC, although plan distribution can be handled by a central individual or team. For example, a departmental representative can be responsible for updating their plan, including personnel out-of-hours contact numbers, team tasks, notification, supplier contact details, battle box contents, and sending the updated plan to a central point for distribution.

To be effective, updated documentation should be distributed using a formal version control process.

Maintenance needs to be managed promptly to achieve its purpose. This requires regular reports that identify planned maintenance progress, highlight areas of weakness, and make recommendations for improving the process.

Proprietary software can be very effective in managing documentation by using systems with workflow processes to ensure that maintenance takes place as and when planned.

Outcomes and Review

The outcomes of maintenance of the BCMS include:

- A documented, planned maintenance schedule.
- Regular progress reports.
- Effective and up-to-date policies and procedures.
- Up-to-date documentation.
- Distribution of updated material to appropriate interested parties.

The maintenance process should be regularly reviewed at pre-agreed intervals or following significant change, as defined within the BC policy.

Review

The purpose of a review is to evaluate the BCMS for continuing suitability, adequacy, and effectiveness, as well as identifying opportunities for improvement.

General Principles

- Review activities should be embedded within the organization's BAU processes to be effective, rather than being a separate activity that may be overlooked. The review cycle of the organization's BCMS should evaluate its continued alignment to the:
  - » Policy, governance structure and strategic objectives.
  - » Culture and operating environment.
  - » Technology systems (primarily ICT-specific business applications and operating systems).

The review should also consider:

- Other prioritised resource dependencies (non-ICT specific).
- The programme's relevance and updates.
- Compliance with the applicable legal and regulatory requirements.
- The effective use of resources and procedures within the BCMS, such as systems, tools, and response and recovery procedures.

Additionally, the alignment and integration of the BCMS to other organizational response procedures should be reviewed, which may include:

- Emergency management procedures.
- Health and safety procedures.
- Security procedures.
- ICT recovery plans and processes.
- Cyber crisis response plans and procedures.
- The frequency and effectiveness of training and awareness sessions.
- An assessment of the competency of the individuals with assigned roles in the BCMS (including alternates) or recovery and response teams.
- The frequency and effectiveness of exercises and whether they validate the effectiveness of the BCMS.

The performance of the personnel who are directly accountable for the management of the BCMS.

Methods and Techniques

There are seven basic types of review. Each can be utilised independently for a specific purpose or assessed in combination during the review of the organization's BCMS to provide a holistic assessment:

- **Audit (internal and external):** a formal, impartial evaluation that measures an organization's BCMS against an agreed standard.
- **Self-assessment:** an evaluation performed by those involved in the management and implementation of the BCMS.
- **Quality assurance (QA):** an evaluation of the BCMS outputs against the requirements or expectations to determine whether BC is incorporated into every task undertaken through the BCMS.
- **Performance appraisal:** an evaluation of the performance of individuals tasked with roles and responsibilities.
- **Supplier performance:** an evaluation of a priority supplier's BCMS or recovery services against BC requirements (PP4).
- **Post-incident review:** an evaluation of the response and recovery efforts following an incident to determine the extent to which the organization's plans, capabilities, and competencies meet the BC requirements.
- **Management review:** an evaluation by top management to determine the extent to which the BCMS meets its objectives.

Audit

General Principles

Auditing is designed to provide independent assurance on a set of processes. However, it does not confirm that the solutions adopted are necessarily correct or provide assurance that the organization will be able to recover from an incident.

A BCMS audit aims to assess the extent to which the BCMS aligns to a nominated standard such as ISO 22301:2019, organizational policies, a local or national standard, or a regulatory standard/framework.

Audits should be conducted at planned intervals to confirm that the organization conforms with its BC policy, legal or regulatory requirements, or the organization's audit and governance policies where relevant.

Outcomes and Review

The outcomes of the review should be options for improving the organization's capability and competence to respond to disruption.

The effectiveness of the types of review used should be measured at pre-agreed intervals, following an incident, or following significant change as defined within the BC policy.

Concepts and Considerations

An audit assumes that, if the process of auditing a BCMS is undertaken correctly and properly applied, the outcome should provide evidence of an effective programme. It also assumes that the method adopted by the organization is effective and provides a suitable framework for audit. However, it does not verify that the BC plan, capabilities, and competencies are fit for purpose.

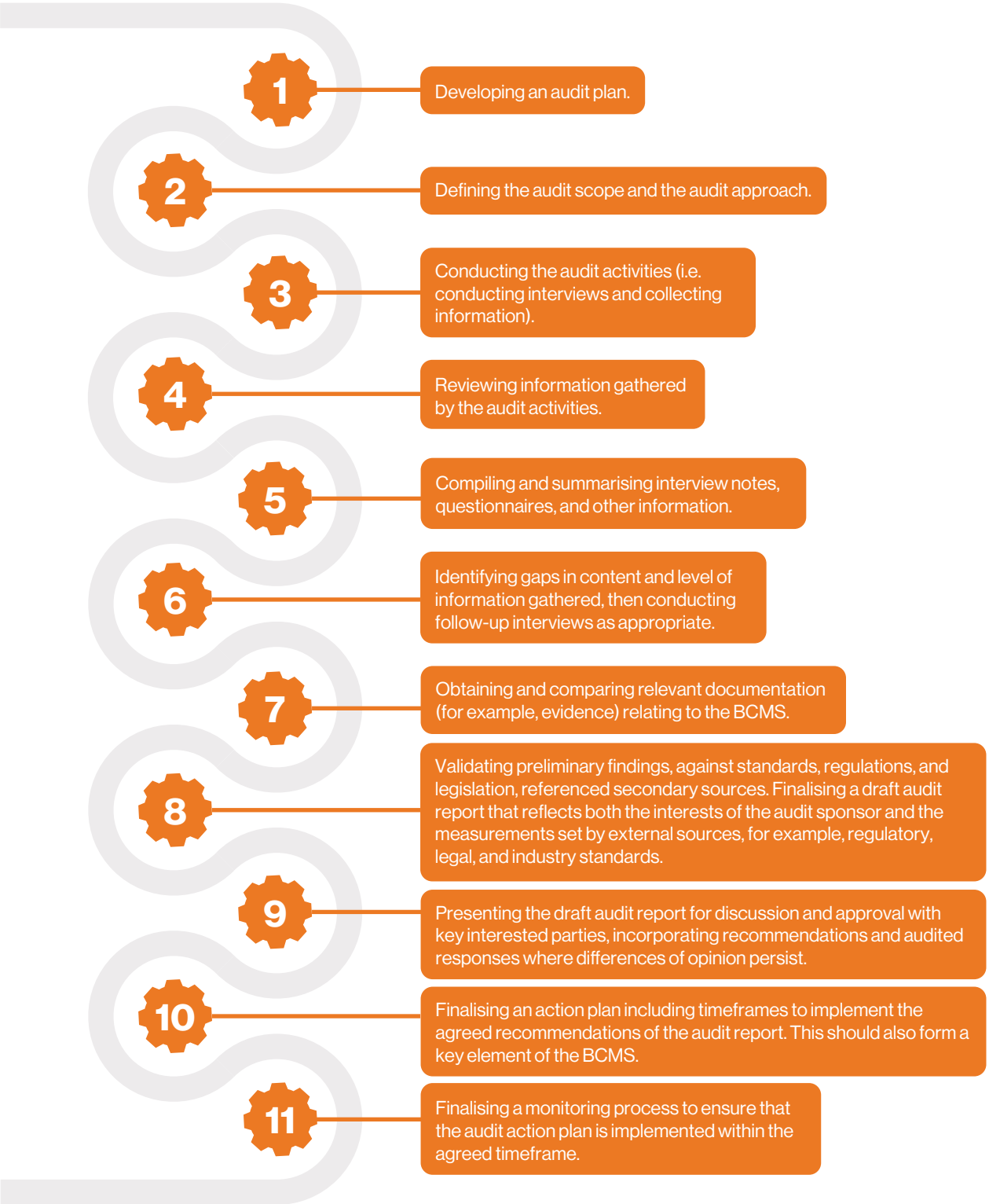
The assessment method adopted by the organization should have been defined in its BC policy (PP1).

Those performing the audit should have the relevant competencies and experience to perform this task.

Process

The BCMS audit is a detailed process and requires interaction with a wide range of managerial and operational roles from both business and technical perspectives.

The audit process should include:



Methods and Techniques

The methods used for auditing should be determined by the auditors, who should be independent of those involved in developing the BCMS. The method should also comply with the organization's BC policy, as well as the organization's established auditing procedures where relevant.

Virtual audits have been successful using collaboration tools and software. They may be considered where it is not practical or feasible for individuals to be onsite.

A BCMS audit plan should include the identification of:

- The audit objectives. These should be partly driven, governed, or restricted by legal or regulatory requirements. Limitations in the audit scope should be agreed upon with management and considered during the reporting stage to ensure the audit results accurately represent the BC programme.
- A standard audit framework (where appropriate). The audit framework should be governed or restricted by legal or regulatory requirements.

The definition of the audit scope should include:

- Corporate governance, compliance, or other issues to be audited.
- Area, department, or site of the organization to be audited.

The definition of the audit approach should include:

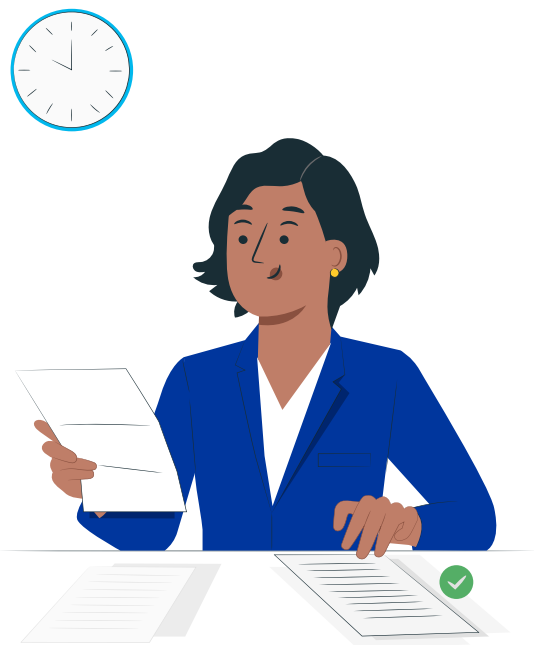
- Auditing activities, such as questionnaires, face-to-face or virtual interviews, document reviews, and solution reviews.
- An activity timetable and due dates.
- Identification of the audit evaluation criteria, such as ISO and regulatory standards.
- Any requirements for specific subject-matter expertise or outsourced service provider assistance to conduct the audit.

Outcomes and Review

The outcome of an audit includes:

- An independent BCMS audit report.
- An action plan that is agreed upon and approved by top management.
- The possibility of an unfavourable audit report, which means management should accept plans as inadequate and support the initiation of a review with a BC professional assisting the team that needs improvement.

The auditing process should be regularly reviewed at pre-agreed intervals or following significant changes, as defined within the BC policy.



Self-Assessment

General Principles

The purpose of self-assessment is for an organization to review its implementation of the BCMS and create an action plan for improvement.

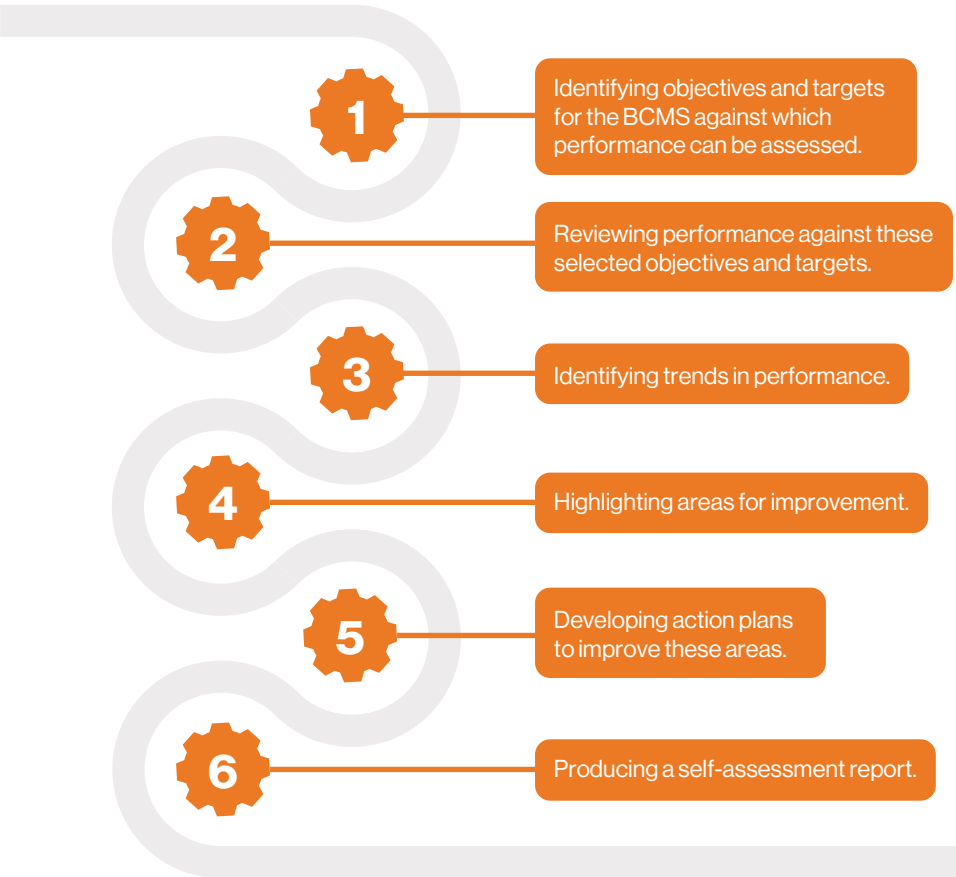
- Self-assessment can be carried out between audits to identify progress against audit recommendations.
- Self-assessment should also be carried out during and immediately after the initial implementation of the BCMS.

Concepts and Considerations

Self-assessment assumes that an organization has identified objectives and targets against which its BCMS can be assessed.

Process

The self-assessment process includes:



Methods and Techniques

Self-assessment objectives and targets include:

- Project milestones for the BCMS achieved as per the project plan.
- Percentage of plans maintained by the scheduled date.
- Percentage of members of response teams involved in an exercise each year.
- The number of unaddressed lessons learned from exercises.
- The extent of the completion of the BIAs.

A maturity model can be used or developed to evaluate progress and have a more positive effect than a pass or fail type of assessment.

Outcomes and Review

The outcomes of self-assessment include:

- An action plan for improvements.
- An improvement in the BCMS.
- An improvement in the organization's level of resilience.

The self-assessment process should be regularly reviewed at pre-agreed intervals or following significant change, as defined within the BC policy.

Quality Assurance (QA)

General Principles

QA determines how well BC is incorporated into the tasks pertaining to the BCMS.

QA should be a formal and documented process for organizations certified against international or national standards, while for other organizations it should be an informal review against expectations and intentions as expressed in the BC policy.

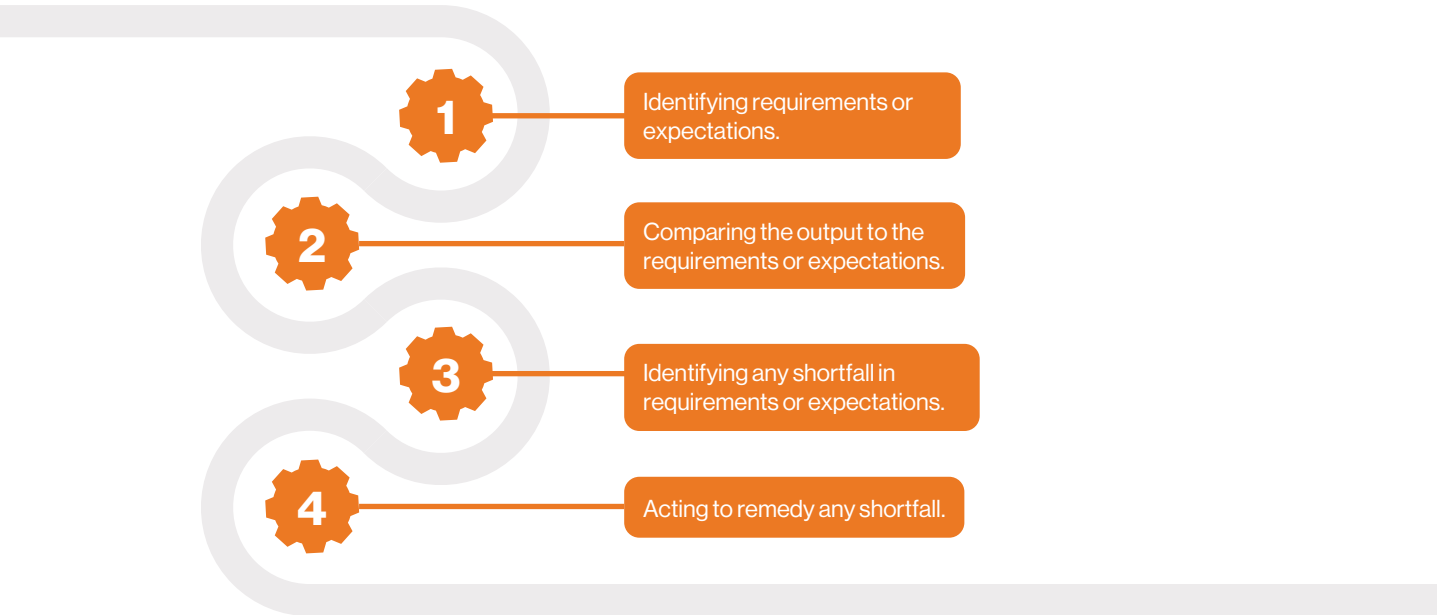
Concepts and Considerations

QA is an ongoing process throughout the BCMS. It ensures that the requirements for the outputs of the BCMS have been identified.

Process

QA can be undertaken as a continual process on all outputs or through periodic sampling.

The process involves:



Methods and Techniques

The organization can use the following methods and techniques when comparing BCMS outputs to the requirements or expectations and identifying shortfalls:

- Setting up document control standards.
- Verifying ownership of the plan.
- Ensuring the BIA identifies the MTPDs for all prioritised activities.
- Checking that the relevant details (quantity, timeframe, and source) of required resources for continuity and recovery of activity have been identified.
- Securing top management sign-off on the recommended continuity and recovery solutions, as well as their scope.
- Review of previous QA reports, their actions, and recommendations.

Outcomes and Review

The outcome of QA should be an improvement in the way the outputs from the BCMS meet the organization's requirements and expectations.

The QA process should be regularly reviewed at pre-agreed intervals or following significant changes, as defined within the BC policy.

Performance Appraisal

General Principles

Roles and responsibilities for the BCMS should have been defined in job descriptions and performance plans to establish BC governance (PP1). In addition, performance appraisals should be used to check how well those roles and responsibilities are undertaken.

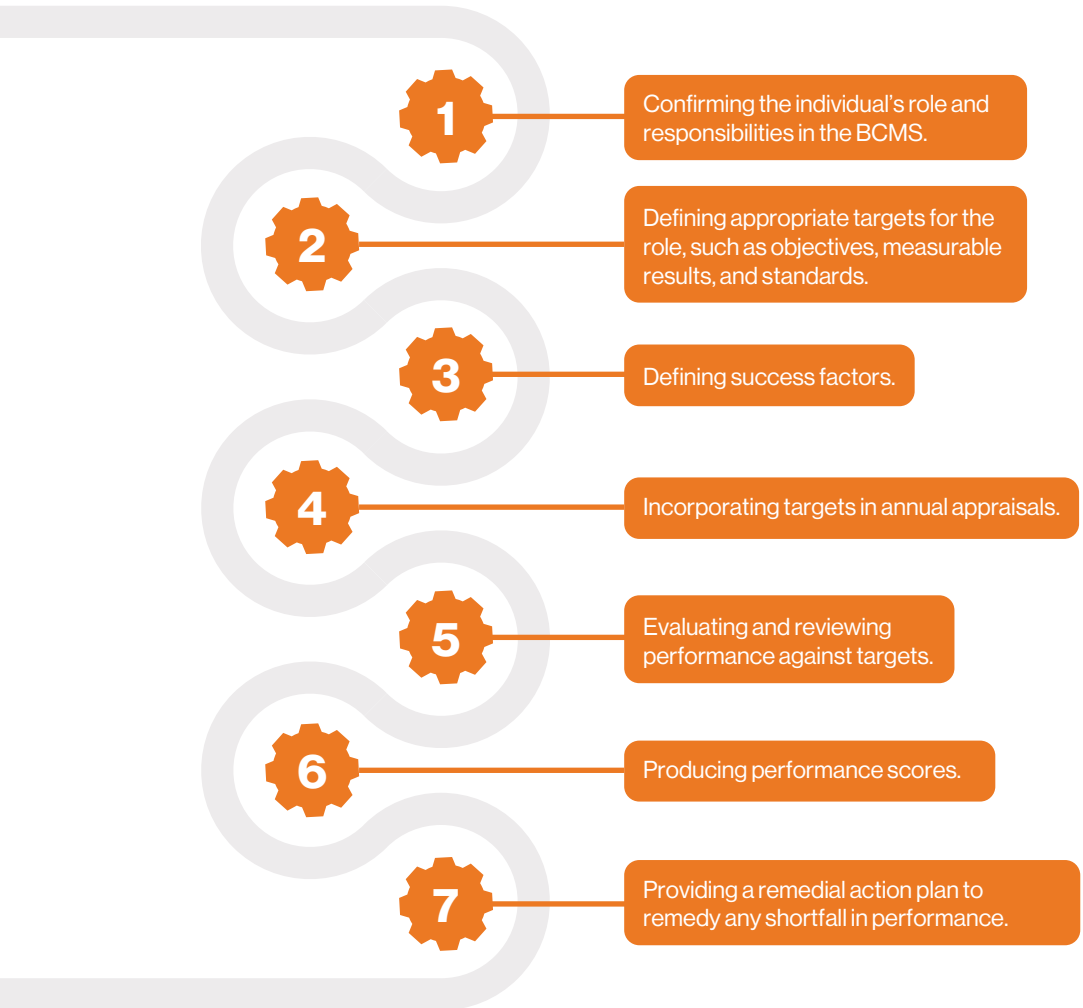
Concepts and Considerations

An organization's performance appraisal process considers that the roles and responsibilities for BC positions have been defined.

Process

The performance appraisal process can be undertaken as part of a regular personnel appraisal process or to review an individual's performance of their responsibilities in the BCMS, specifically, working with the people and culture department (PP2).

The process involves:



Methods and Techniques

A performance appraisal may include a series of metrics to evaluate personnel, these include:

- The number of times scheduled plan maintenance dates were met.
- Percentage completion of the BIAs.
- Percentage of exercises undertaken as planned with a supporting post-exercise report.
- Percentage of plans validated for objectives achievement.
- Percentage resolution of outstanding issues resulting from incidents, exercises, and audits.
- Expenditure against budget.

Outcomes and Review

The performance appraisal outcome should lead to an improvement in how personnel with a role in the BCMS:

- Carry out their role.
- Undertake their responsibilities.
- Meet their objectives.

The performance appraisal process should be regularly reviewed at pre-agreed intervals or following significant change, as defined within the BC policy.

Supplier Performance

General Principles

The review process of the supplier's BCMS or their response and recovery services should refer to a contract containing the expectations (including the performance targets) defined in their BCMS.

Concepts and Considerations

An organization can depend on suppliers that can provide priority products and services. Therefore, the supplier performance review is based on identifying the organization's suppliers and their established recovery expectations.

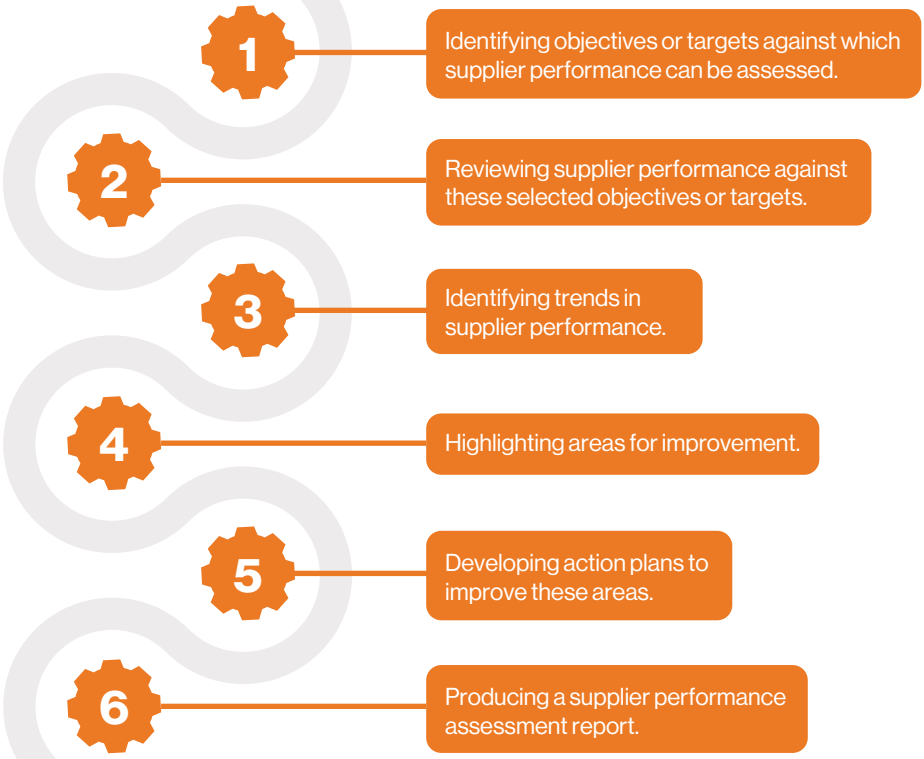
The supplier's performance can be compared to the terms in the SLA. The assessment can begin as part of the tendering process and continue during the contract period using supplier relationship management techniques or contract management.

Process

The priority suppliers' BCMS and recovery services review process should be defined in their contracts. The BCMS of priority suppliers should be reviewed as if they were part of the organization itself.

The process involves:

In this way the BC professional is applying the same review requirements and assessment of capability on a supplier as it would on an internal department being reviewed. It should be anticipated that gaps will be found, which are then tracked and addressed with the supplier as part of the ongoing relationship between the organization and the priority supplier.



Methods and Techniques

Supplier performance should be reviewed against contractual SLAs, which in the case of priority suppliers, should relate to their BCMS. Increased supplier performance and capability may be achieved by including and assessing their exercise activities.

Outcomes and Review

The outcomes of reviewing supplier performance may include and are not limited to:

- A performance rating against SLAs containing specific actions before, during, and after an incident, including RTOs, MBCOs, RPOs, and possibly MTPDs.
- An understanding of the supplier's response capability and capacity.
- A remedial action plan to reduce the risk of dependency on the supplier, for example, contingency arrangements, having alternative suppliers, encouraging the supplier to improve their performance, or putting pressure on the relevant supplier to resolve the gaps.

- Increased readiness and assurance of prioritised supplier activities (for example, get to the point of better estimating the RTO for the supplier in relation to the impact they would have on the organization if there were an incident).

The supplier's response capability and capacity performance should be regularly reviewed at pre-agreed intervals or following a significant change in process or activities as defined in the SLA.

Post-Incident Review

General Principles

The purpose of a post-incident review is to ensure that plan objectives and capabilities are effective in delivering the required response. Lessons learned should be identified, improvement opportunities documented, and action plans developed and tracked to completion.

The post-incident review is performed by collating information from those involved in an event requiring the invocation of BC plans and those involved in response and recovery efforts. Information includes a chronology of events, the performance of the plan, whether plan objectives were achieved within stated timescales, and whether those executing the plan performed as required. It should be noted that a post-incident review is not intended to assign blame but rather to identify any causation, unforeseen impacts, or gaps: and document these as improvement actions to promote continual learning and enhance resilience.

The output of the post-incident review is a report of potential findings detailing how the incidents and near misses could have been handled better.

A post-incident review meeting should be conducted as soon as possible after returning to BAU. All aspects of the response's activation, execution, and effectiveness should be reviewed. In addition, attention to the achievement of plan recovery objectives, the performance of key personnel, communications, and assumptions should be considered.

The post-incident review is not a process of questioning responsibility. Especially for collecting information related to any negative result of the incident response, it should be done carefully to avoid any negative impact (for example, penalty) on the information providers.

The lessons learned from incidents that happen in peer organizations or from near-misses may be useful inputs for future responses to incidents, even if a similar incident does not impact the organization.

Concepts and Considerations

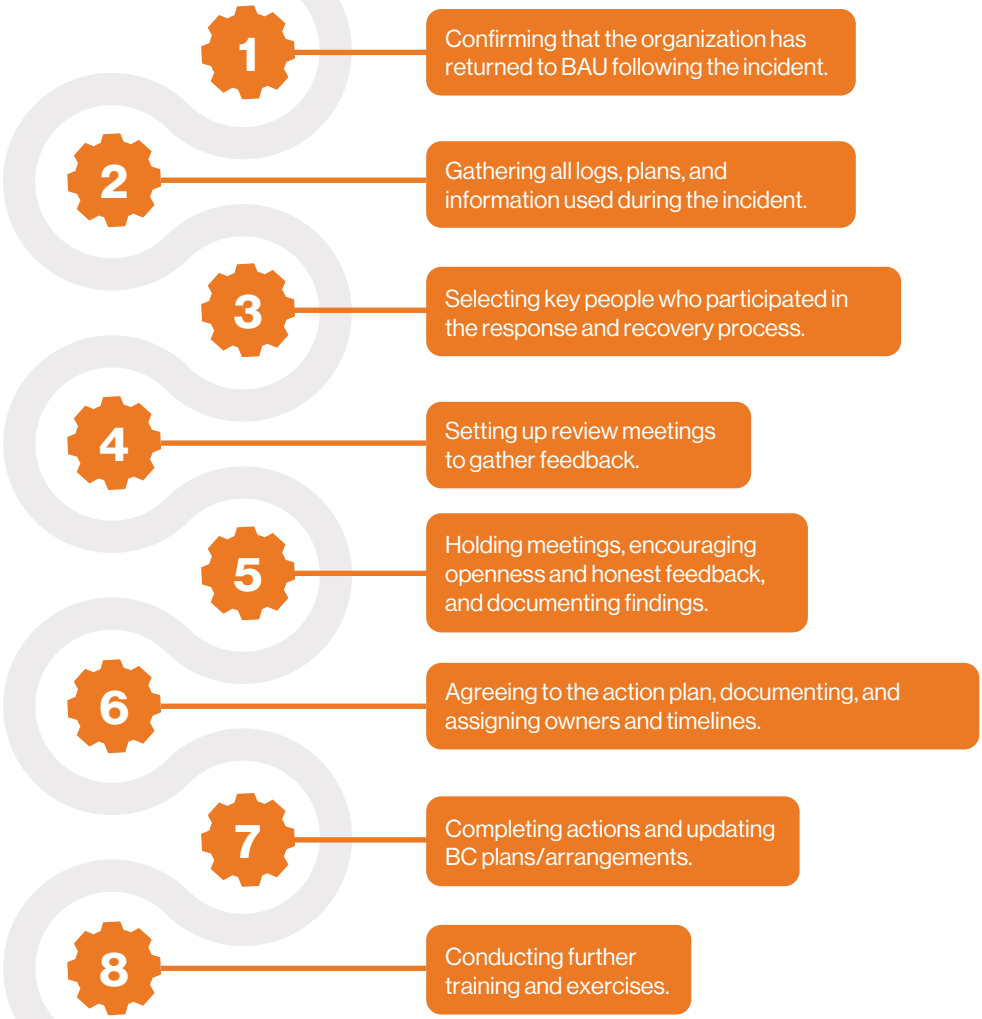
A post-incident review considers whether any gaps exist between the expected and actual response to an incident. The gaps may be uncovered by gathering information from the actual incident.

Compared to exercises, live incidents provide far greater learning value since they will provide real-time experience and test how effectively plans perform under stress.

The person leading the post-incident review should have the relevant experience, competencies, and skills to carry out this task impartially.

Process

The process involves:



Methods and Techniques

A post-incident review should include information relating to the following:

- Incident response activity log (chronology).
- Interviews with the people involved in the incident response.
- Videos and photos that were taken during the incident.
- Media coverage related to the incident.

The decisions made during the incident response should be reviewed carefully (for example, considering the result of any different decision), especially if the outcome of the incident response is not favourable. The activity log should record each decision during the incident response.

Outcomes and Review

The outcome of the post-incident review is a post-incident report which includes potential findings detailing what went well and how the incident could have been handled better.

The post-incident review process should be regularly reviewed at pre-agreed intervals or following significant change, as defined within the BC policy.

Management Review

General Principles

A management review provides opportunities for top management to understand the performance of the BCMS. It should be aligned to organizational objectives and their adequacy to address governance; and the overall approach to managing risk should be understood.

Concepts and Considerations

A management review considers that the organization's intentions and directions as identified in the BC policy are effectively adhered to.

Methods and Techniques

A management review should address the following items:

- The status of actions from previous management reviews, post-exercise reports, audits, and post-incident reports.
- Changes to the internal and external environment, if relevant to the organization's BC programme.
- Information regarding the programme's performance, including trends in audit findings and corrective actions, results or outcomes from self-assessment, quality assurance, performance appraisals, and supplier performance reviews.
- Opportunities for improvements.
- Results of exercises or lessons learned from real incidents.
- Risks or issues not adequately addressed in the BC programme.
- Adequacy of the BC policy.
- Results of self-assessments of the BC programme.

Outcomes and Review

The outcomes of the management review include:

- An action plan for improvements.
- Continual improvement of the BCMS.
- An enhancement of the organization's level of resilience when identified improvement opportunities are rectified.
- Renewed tone from the top with clearer messages on focus areas for BC.

Over time, the BC professional should recognise an improvement in BC outcomes and the BCMS as the organization improves its BC culture by better Embracing BC (refer to **PP2**). The management review process should be regularly reviewed at pre-agreed intervals or following significant changes, as defined within the BC policy.

Epilogue

The PPs detailed in this GPG are designed to assist the BC professional in establishing and maintaining a BCMS for their organization.

The methodologies presented have been compiled by accredited BC professionals worldwide and the content is periodically revised to stay current. The GPG is therefore widely accepted as a definitive guide to establishing a complete BCMS or improving existing ones. However, this GPG as a standalone document cannot incorporate the almost infinite risks and requirements across countless industries and hundreds of geographies where the profession of BC is practiced.

This might seem counter to the point of this GPG being a comprehensive tool. On the contrary, this GPG emphasises within its PPs the importance of iterative reviews for the purposes of continuous improvement. This makes the techniques and processes to create or improve a management system detailed in the GPG highly scalable.

Clarifying any Potential Contradiction of Terms

Perceived contradictions may arise when BC professionals consider whether this GPG is comprehensive or complete. The GPG and the Professional Practices within are comprehensive. This means a fully functional BCMS may be created using only the techniques, definitions and processes provided within this GPG.

However, one of the many crucial summary points of this GPG is that no management system can ever be complete due to continuous improvement efforts. Therefore, each PP is denoted as part of a never-ending series of projects and procedures. This is why the BCMS has replaced the previous lifecycle (See Figure 3).

Figure 3

The evolution of macro trends, such as industry innovation, technology, new regulations, and infectious diseases, means a periodic review is one of the keys to success when it comes to the BCMS. Striving for completion is implied in every PP but should always be considered beyond reach for a seasoned professional. This is because an experienced professional knows that tomorrow may bring about the unknown, which could trigger a large review and refresh for the entire management system. Such changes to the BCMS will invariably create a level of resilience that was not there previously.

To best anticipate the unknown, the GPG Edition 7.0 review team and all other volunteers that contributed to previous versions help bring a diverse view and extensive experience. This broad vision helps foresee as many perspectives as possible to support professionals in creating or improving a comprehensive BCMS. Additionally, if there is an existing BCM process already implemented in an organization, GPG Edition 7.0 will support that revision to a new BCMS.

World Beyond the GPG

The GPG signposts multiple national and international standards throughout the various PPs. This is to help professionals worldwide become aware of important resources and techniques which may help the next review cycle for the PPs become more comprehensive, and for the BCMS to be resilient against the impacts and incidents tomorrow will bring.

There are references throughout this GPG to standards on the following practices:

- Supply chain management.
- Security and resilience.
- BC strategy.
- BIA.

This signposting is vital because the GPG is charged with being a scalable and comprehensive document. This means this GPG cannot be too prescriptive about any single PP, nor could it reference statutory requirements that could be geographically or industry specific.

This scalable yet generic approach is deliberate. The approach to BC should not be influenced or lacking when used in conjunction with local directives. One size cannot fit all when there are as many variables as the practice of BCM to take into consideration. Therefore, professionals must research best practices relevant to their industries and geographies, beyond what is included within this GPG to better their BCMS.

The increased statutory parameters might make PP implementation more complex, requiring the engagement of more innovative techniques to conduct a successful BIA or implement a security and resilience strategy.

It might also transpire that the previous implementation of a BCMS disregarded supply chain resilience from its scope as it was not a factor in operations. However, in the next review of the processes set up following the actioning of the PPs, the organization could expand operations where supply chain resilience becomes of paramount importance. Such evolutionary changes are not uncommon and therefore charge the BCI and this GPG with the responsibility to refer to all tools required to improve any BCMS from a global perspective.

In conclusion, it is entirely possible to create a quality BCMS using only the information outlined in this GPG. However, to completely tailor a BCMS to a specific organization, maintain its relevance and add value, it is essential to engage with information on offer beyond this GPG. This is especially true if a professional has solely created a BCMS that incorporates the PPs and has done a complete review cycle to improve it over a year or two.

Lastly, the BC world comprises individuals who are passionate about the profession and will always make time to answer questions from new professionals, or even provide mentoring. Feel free to reach out to any person mentioned in this GPG for mentoring or general advice if you are starting out on your journey in the world of BCM.

How Could the GPG Enhance a Professional's Career in BC?

The GPG is recommended reading for anyone interested in learning about BC and resilience.

To obtain recognition of competency in this area, professionals can obtain the globally recognised credential 'CBCI' by becoming a member of the BCI. This requires them to achieve the CBCI qualification via the CBCI Examination, which may be taken at the end of a CBCI Certification Course. The GPG is a core text for this course.

The Gateway to BCI Membership

Candidates who successfully achieve the CBCI qualification are awarded one year's complimentary CBCI level membership to the BCI.

This membership provides the post-nominal credential of 'CBCI', which is used to demonstrate the level of qualification achieved by the individual. It also provides access to wide-ranging benefits to enhance a professional's career development.

CBCI Certification and BCI membership are just the beginning. Professionals are encouraged to progress to more senior certified BCI membership grades to demonstrate technical and professional competency. Employers increasingly specify BCI professional credentials for individuals seeking employment, promotion, or wishing to embark on or change their career within the industry.

Find out more about the CBCI certification course and examination and BCI membership, at thebci.org

Find out more
www.thebci.org

BCI Membership Grades

Affiliate
Student

CBCI

AMBCI

MBCI

FBCI

Leading the way
to resilience

Central Office
The BCI Forum Ltd t/a The Business Continuity Institute

9 Greyfriars Road
Reading
Berkshire
RG1 1NU
United Kingdom

Tel : +44 (0) 118 947 8215
Email : bci@thebci.org

www.thebci.org

ISBN: 978-1-3999-5059-6