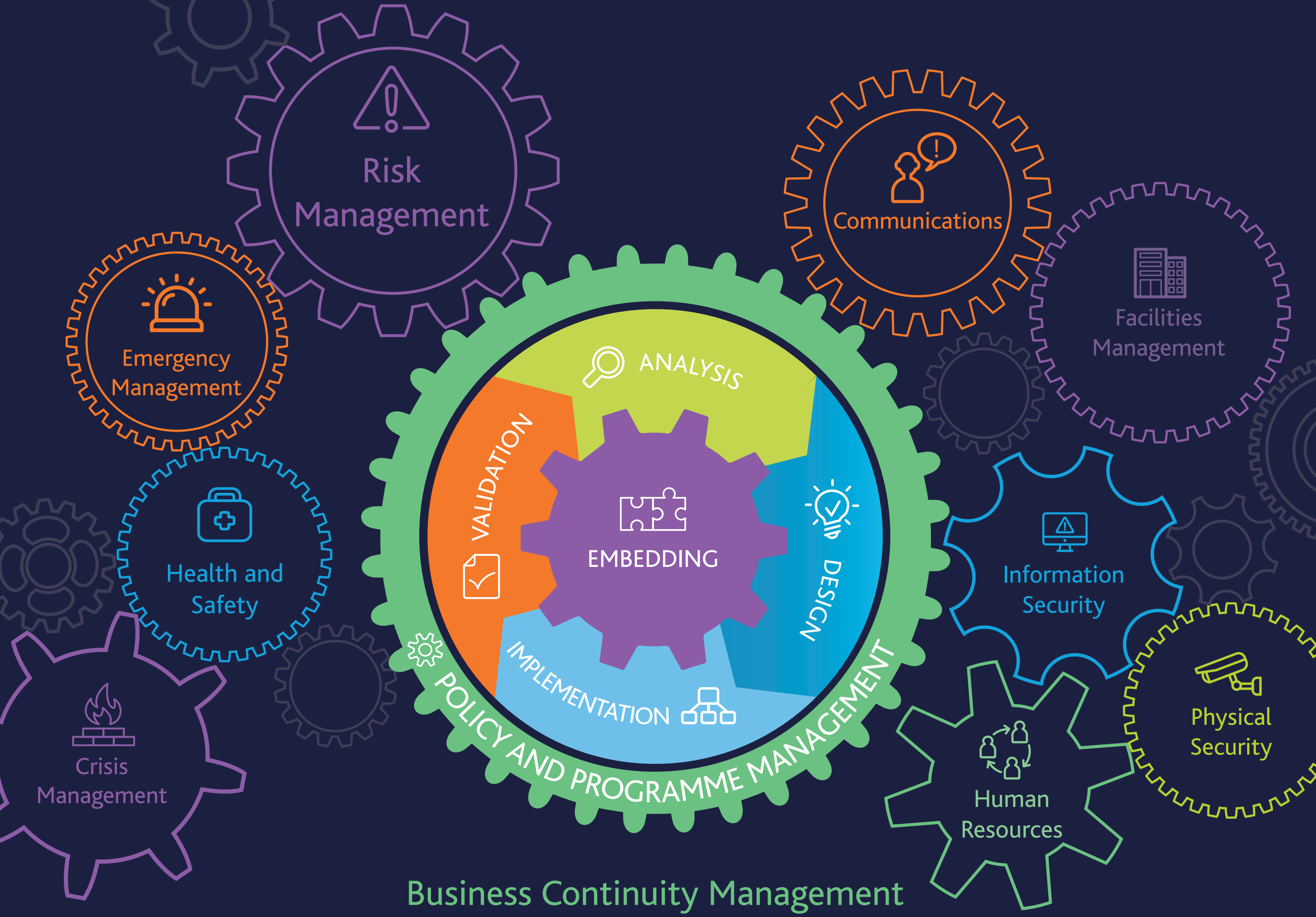
Good Practice Guidelines

2018 Edition

The global guide to good practice in business continuity.



Business Continuity Management (BCM) Lifecycle

Building organizational resilience

Leading the way
to resilience

GPG Addendum

Introduction

The International Standard for business continuity management (ISO 22301:2012) has been reviewed and updated, the current version is now ISO 22301:2019.

The BCI Good Practice Guidelines 2018 Edition (GPG) has references to ISO 22301. This document, an addendum for the (GPG), shows the changes in ISO 22301:2019 that directly affect the GPG.

Although improvements can be made, this is not a re-write or update of the GPG.

GPG versus ISO 22301

To understand the changes that have been included it is important to understand the relationship between the GPG and ISO standards which is described in the Introduction (page 7) of the GPG.

"The publications are aligned and complementary, serving two different purposes, but constitute equally essential and valuable parts of any business continuity and resilience professional's toolkit. There are minor differences in the language used, but all fundamental concepts and actions are aligned. The terminology used is listed in the GPG glossary..."

It is clear that the GPG does not mirror the ISO standard and that not all changes to the ISO standard need to be reflected in the GPG and in this addendum.

Overview of changes in ISO 22301:2019

The original version of 22301 was published in 2012. The review was started in 2017 and completed in 2019. While there are no new requirements the review brings improvements to the structure and readability of the standard. This results in a better distinction between the requirements of the Business Continuity Management System (BCMS) itself and the business continuity requirements. The requirements are now clearer and many of the terms have been updated.

Only the most significant terms have been included in ISO 22301:2019. All terms are available in ISO 22300:2021. It should be noted that all definitions are available in ISO's Online Browsing Platform (OBP)

https://bbn.isolutions.iso.org/obp/ui

Acknowledgements

The BCI would like to acknowledge the following individuals for their contribution to this project:

Catherine Thomas MBCI, Gary Dade Hon FBCI, Gianna Detoni FBCI, Ian Charters FBCI, Kate Needham-Bennett AMBCI, Kelly Blakeley MBCI, Kim Maclean-Bristol MBCI, Marie-Helene Primeau MBCI, Michael Crooymans MBCI, Saul Midler Hon FBCI, Yasmine Elhamouly MBCI.

Special thanks to Lynnda Nelson for providing a comprehensive list of changes.

Permission to reproduce extracts from ISO 22301:2019 and ISO 22300:2021 is granted by BSI.

Changes to GPG due to ISO 22301:2019

Changed source of unchanged definitions

The following definitions were included in 22301:2012 but are now sourced from ISO22300:2021. These definitions are unchanged.

Term	Definition	Source	Affects
Business Continuity Management System (BCMS)	No change	ISO 22300:2021	Glossary
Business continuity programme	No change	ISO 22300:2021	Glossary, PP1:p23
Exercise	No change (notes have changed)	ISO 22300:2021	Glossary, PP6:p89
Invocation	No change	ISO 22300:2021	Glossary
Maximum acceptable outage (MAO)	No change, but no longer used in 22301	ISO 22300:2021	Glossary, PP3:p39
Maximum tolerable period of disruption (MTPD)	No change	ISO 22300:2021	Glossary, PP3:p39
Personnel	No change	ISO 22300:2021	Glossary

Changed definitions

The following definitions have been changed. These definitions can be found in 22300:2021. Some critical definitions were also included in 22301:2019 so that they would be available immediately.

Term	Updated Definition	Source	Affects
Business Continuity (BC)	capability of an organization to continue the delivery of products and services **within acceptable time frames** at predefined capacity **during** a disruption	ISO 22300:2021	Glossary
Business continuity management	holistic management process that identifies potential threats to an organization and the impact those threats, if realized, **can cause on business operations,** and provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of key **interested parties,** reputation, **brand** and value-creating activities	ISO 22300:2021	Glossary, PP3:p50
Business continuity plan (BCP)	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 22300:2021	Glossary, PP5:p76
Business impact analysis (BIA)	**process of analysing the impact over time of a disruption on the organization.** Note 1 to entry: The outcome is a statement and justification of business continuity requirements	ISO 22300:2021	Glossary, PP3:p39
Crisis *	**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	Glossary, PP5:p71
Incident	**event** that can be, or could lead to, a disruption, loss, emergency or crisis	ISO 22300:2021	Glossary, PP5:p71
Interested party	person or organization that can affect, be affected by, or perceive **itself** to be affected by a decision or activity. Note this is preferred term – stakeholder is permitted	ISO 22300:2021	Glossary
Minimum Business Continuity Objective (MBCO)	minimum **capacity** or level of services and/or products that is acceptable to an organization to achieve its business objectives during a disruption	ISO 22300:2021	Glossary, PP3:p43
Prioritised activities	**activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption**	ISO 22300:2021	Glossary, PP3:p39
Products and services	**output or outcome provided by an organization to interested parties** Note: ISO defines product and service but uses products and services	ISO 22300:2021	Glossary, Intro:p18, PP3:p39
Recovery point objective (RPO)	point to which information used by an activity **is restored** to enable the activity to operate on resumption	ISO 22300:2021	Glossary, PP3:p48
Recovery time objective (RTO)	period of time following an incident within which a product or service or an **activity is resumed, or resources are recovered**	ISO 22300:2021	Glossary, PP3:p39
Resources	all assets **(including plant and equipment), people, skills, technology, premises, and supplies** and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective	ISO 22300:2021	Glossary
Test	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	Glossary, PP6:p90
Threat *	potential cause of an unwanted incident, which **may** result in harm to individuals, **assets, a system or organization,** the environment or the community	ISO 22300:2021	Glossary, PP3:p50

* Not included in 22301:2012 or 22301:2019

Other changes

In PP3:p48 the resources have been updated as follows:

Existing list items	Changed list items

• Buildings, work environment and associated utilities.
• Facilities, equipment, and consumables.
• ICT systems.
• Transportation.
	c) **physical infrastructure** such as buildings, workplaces or other **facilities** and associated utilities;
	d) equipment and consumables;
	e) **information and communication technology** (ICT) systems;
	f) transportation and **logistics;**

PP4. ISO 22301:2019 now refers to strategies and solutions instead of solutions. A strategy will be supported by one or more solutions.

Note: changes to definitions

Although the GPG uses its own definition of activity it is similar to that used in 22301:2012. In 22301:2019 the definition has been changed to: **set of one or more tasks with a defined output.**

The GPG has not included the term impact but often refers to it. In 22301:2019 the definition has been changed to: **outcome of a disruption affecting objectives**

Note: use of terms MAO, MTPD and RTO

During the review of 22301 it was clear that various terms are not used consistently in the field. The requirements are now described and it is noted that they may be referred to with the preferred terms MTPD and RTO.

The descriptions of MTPD and RTO in 22301:2019 Section 8.2.2 are as follows:

MTPD: the time frame within which the impacts of not resuming activities would become unacceptable to the organization

RTO: prioritized time frames as set within the time identified in MTPD for resuming disrupted activities at a specified minimum acceptable capacity

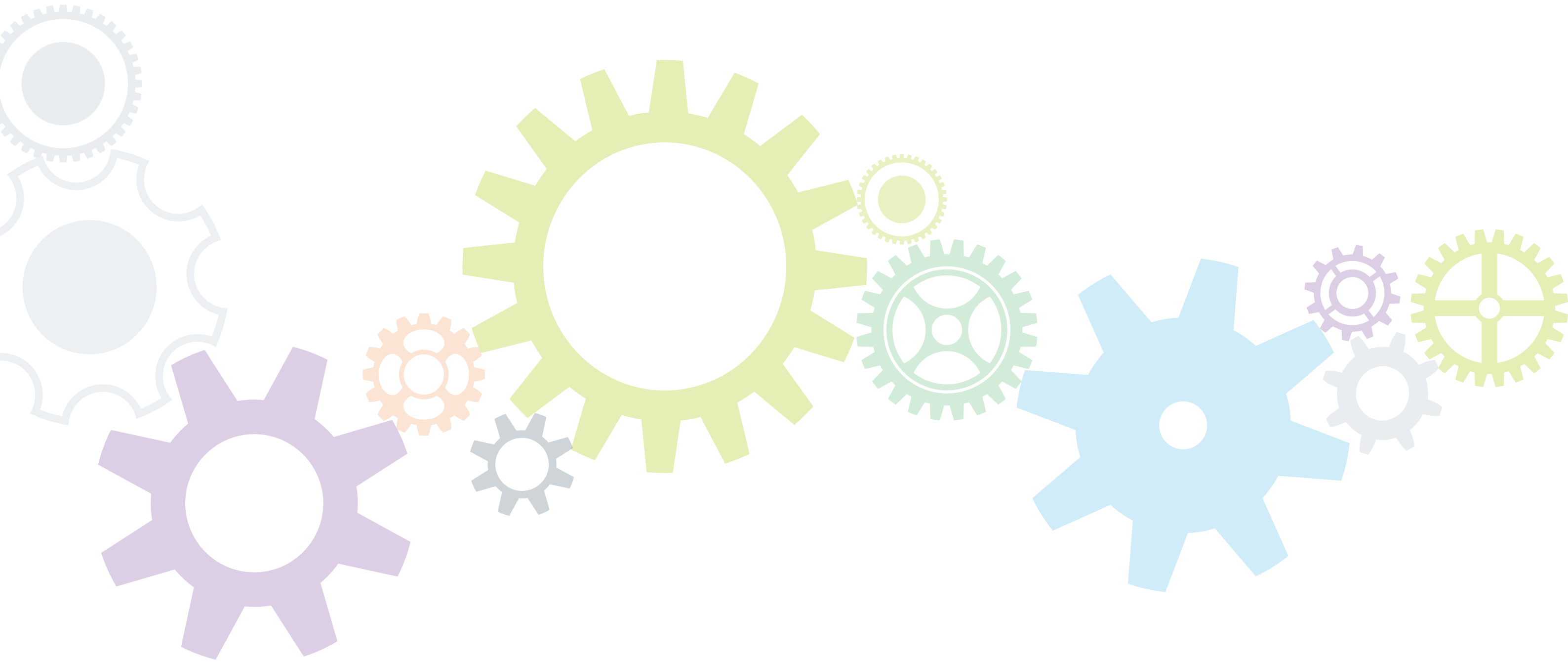
How to use these guidelines.

Each stage of the BCM Lifecycle is a Professional Practice which has its own unique icon and colour and has its title written on the right hand side of each page to help the reader navigate between them.

- PP1 - Policy and Programme Management
- PP2 - Embedding
- PP3 - Analysis
- PP4 - Design
- PP5 - Implementation
- PP6 - Validation

Each Professional Practice contains the following recurring sections which also has its own unique icon.

- General Principles
- Concept and Assumptions
- Process
- Methods and Techniques
- Outcomes and Review



Icon for Hint/tip; These hints and tips have been provided by experienced practitioners.

Please note: There will be no CBCI exam questions about the hints and tips.

COPYRIGHT PROTECTED DOCUMENT

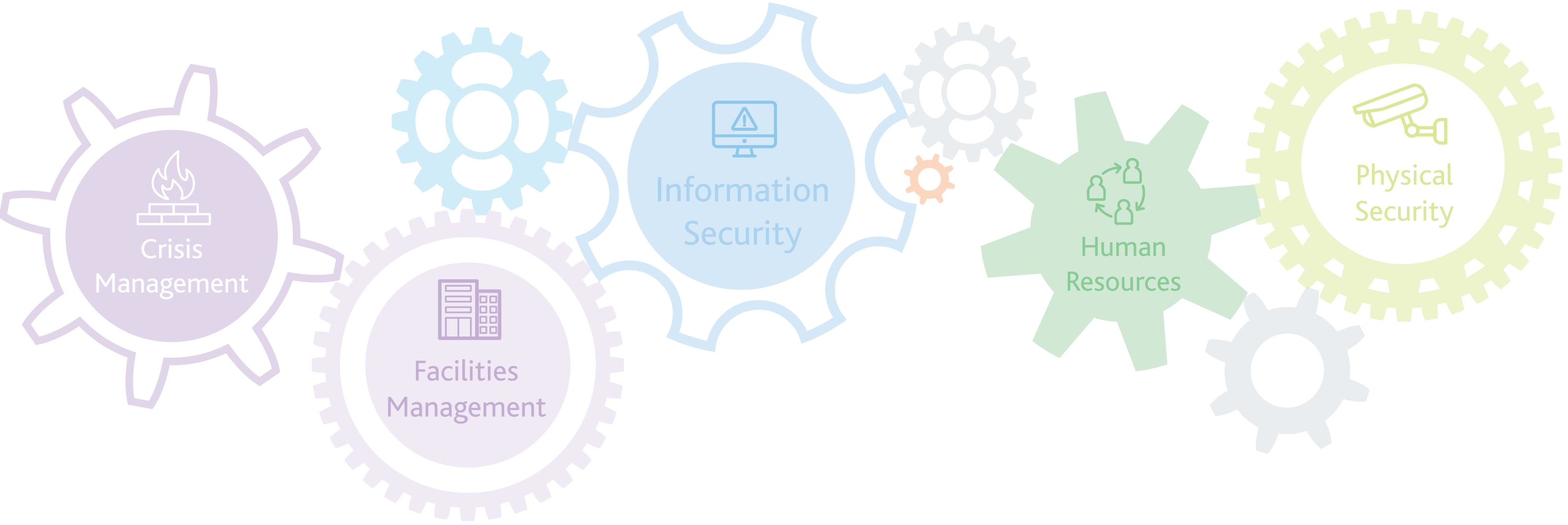
ISBN: 978 9 9932110 8 9

British National Library
This publication has been legally deposited with the British National Library

BCI Copyright
bci@thebci.org
10-11 Southview Park, Marsack Street, Caversham, Berkshire, RG4 5AF, UK.
www.thebci.org

contents

Emergency Management
Risk Management
Communications
Health and Safety


Crisis Management
Facilities Management
Information Security
Human Resources
Physical Security

Introduction to the BCI's Good Practice Guidelines **2018 Edition**

Welcome to the Definitive Global Guide to Good Practice in Business Continuity.

The business continuity (BC) profession continues to evolve as its value is recognised by a wider audience. The world in 2018 continues to be challenged by socio-economic and geo-political change. Organizations must respond and adapt to familiar challenges such as the increasing dominance of technology and the internet, as well as new disruptive threats arising from the globalisation of terrorism and the rapid increase in cyber threats. In this demanding environment, the discipline of business continuity is increasingly relevant.

The ongoing demand for global guidance in the discipline is demonstrated by the adoption and wider acceptance of the international standard for business continuity management (ISO 22301:2012) by organizations worldwide, and the publication of related standards, for example, the Business Impact Analysis (BIA) ISO/TS 22317:2015. The increasing awareness of the importance of enhancing organizational resilience reinforces the value of building effective business continuity capabilities, and is central to the purpose of the BCI.

About the BCI.

Founded in 1994, the BCI defined a set of practices for individuals to be able to demonstrate their individual capability in business continuity management. These Professional Practices form the stages of the business continuity management lifecycle and are described in the BCI's Good Practice Guidelines.

The BCI is the world's leading professional association responsible for improving organizational resilience through building business continuity capability and professional development of individuals all over the world.

The BCI vision is a world where all organizations, communities and societies become more resilient.

The BCI core values are professionalism, reliability, and inclusivity.

The BCI is built on the principle of professionalising business continuity practice, and continues to be the authoritative and reliable source of information on all aspects of business continuity theory and practice for professionals, and offers a wealth of online resources via www.thebci.org. The Good Practice Guidelines have been revised as part of the BCI's process of continual improvement and ongoing development of our body of knowledge to remain relevant to professionals worldwide.

What is Business Continuity?

Business continuity is the key discipline that sits at the heart of building and improving the resilience of organizations. It is a tried and tested methodology that an organization should adopt as part of its overall approach to managing risks and threats. Business continuity management identifies an organization's priorities and prepares solutions to address disruptive threats. This understanding supports the design and implementation of plans to protect and continue the value creating operations of an organization in the event of any disruption. An effective business continuity programme supports the strategic objectives of the organization and pro-actively builds the capability to continue business operations in the event of disruption. The programme includes the identification of risks and threats, the creation of response structures and plans to address incidents and crises, and promotes validation and continuous improvement. The programme is flexible to changes in the internal and external operating environment and delivers measurable value to the organization.

Business continuity is relevant and applicable to all industry sectors and organizations regardless of size, complexity, type, and location.

What is the BCI GPG?

The BCI Good Practice Guidelines has become the leading global guidance for business continuity professionals since it was first issued in 2001. It is the first choice of reference material for anyone needing to know about business continuity as part of their wider resilience related roles and responsibilities.

The business continuity management lifecycle provides a framework to structure the approach to business continuity.

The GPG describes not just what practitioners should do, but provides information about why and how to do it. There are hints and tips and examples throughout the guidelines to add context for the reader, and the PDF version includes links to external sources for further guidance and resources.

The GPG forms the foundation of the BCI's world class, award winning education programme, delivered through the BCI's delivery partners and approved BCI instructors.

The GPG forms the syllabus for the Certificate of the BCI (CBCI) examination leading to the internationally recognised CBCI credential.

The CBCI credential is an entry route to the higher levels of certified BCI membership. The GPG is used by higher education and in academic institutions in both undergraduate and post-graduate courses and in continuing education establishments. The GPG is recognised as industry best practice for professionals, by professionals in organizations all over the world.

Who is the BCI GPG for?

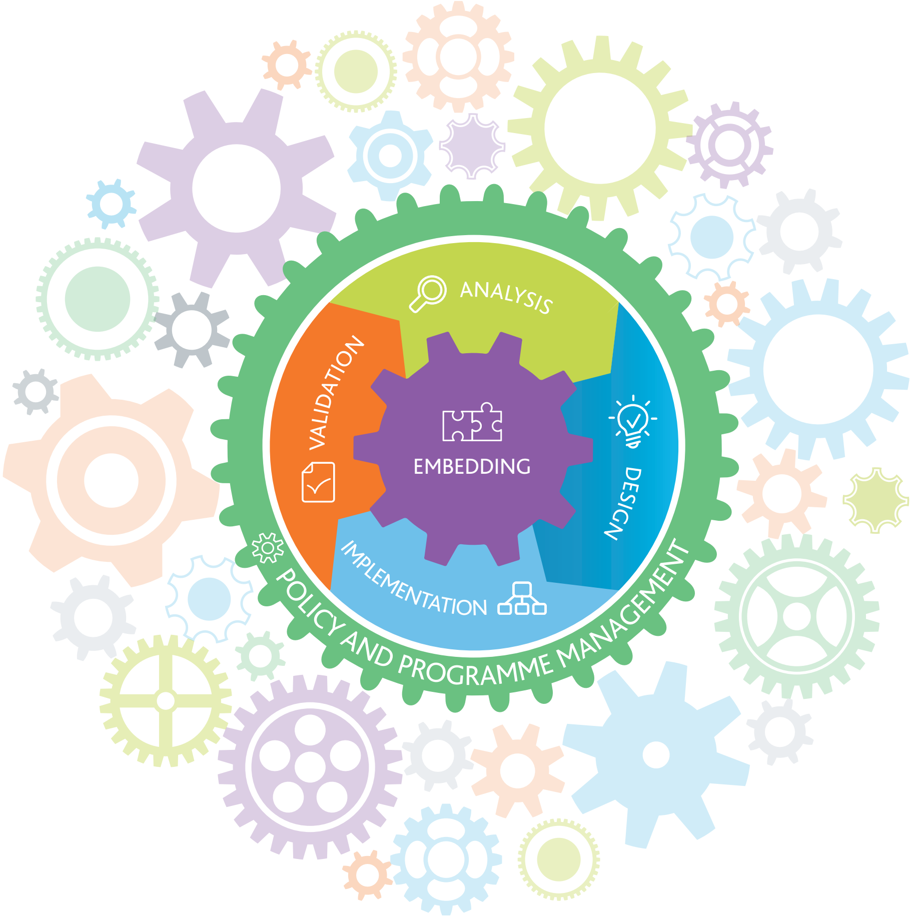
The GPG is not only for those seeking individual professional certification. As a body of knowledge, the GPG is used as an information source for business continuity training programmes and awareness campaigns for anyone who needs to better understand the subject. The GPG is relevant to anyone with a business continuity and resilience related role, which can include, but is not limited to, those working in risk management, information security, physical security, emergency management, facilities management, health and safety, communications, and human resources.

What is the difference between the BCI GPG and standards?

The international standard for business continuity management (ISO 22301:2012) specifies requirements for a business continuity management system for **organizations.** Organizations can choose to seek ISO certification from a recognised standards body for their business continuity management system.

The BCI GPG builds on the ISO requirements by defining what **individuals** need to know about how to approach business continuity management and describing the key stages in developing, implementing and managing a successful business continuity programme. Demonstrating knowledge and understanding of the six Professional Practices at the core of the GPG can lead to individual certification and a professional credential.

The GPG is developed by many of the leading global experts who have also contributed to the development of national and international standards. The publications are aligned and complementary, serving two different purposes, but constitute equally essential and valuable parts of any business continuity and resilience professional's toolkit. There are minor differences in the language used, but all fundamental concepts and actions are aligned. The terminology used is listed in the GPG glossary, and additional terminology is contained in the BCI and Disaster Recovery Journal (DRJ) glossary available on the BCI website. Those needing to know about business continuity can be confident that they are guided by internationally accepted best practices as described in the GPG.



How was the GPG created?

The GPG was created combining the shared knowledge and vast experience of over sixty volunteers from more than twelve countries, across a wide range of industry sectors. This diverse group, including BCI members and non-members, provided feedback on the 2013 version of the GPG, which formed the basis of the updates and additions that produced this revision.

What are the benefits of the GPG?

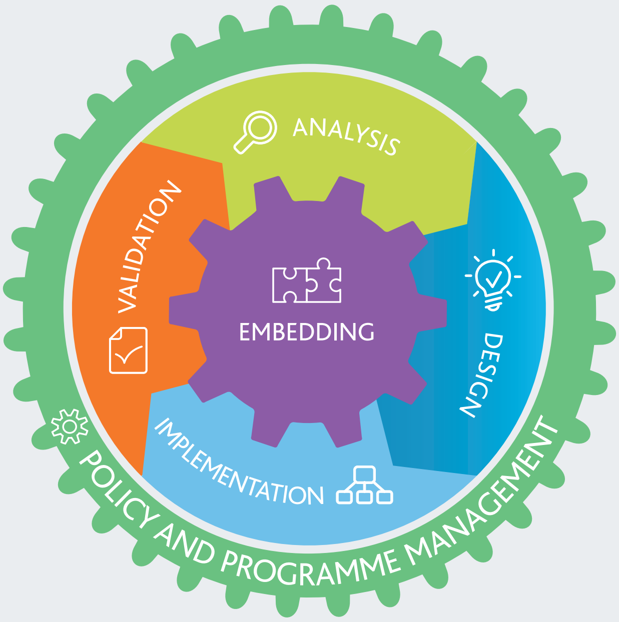
For those individuals who wish to gain an internationally recognised credential in business continuity, and become certified members of the BCI, competence needs to be shown in all six BCI Professional Practices (PPs). The Certificate of the BCI (CBCI) examination tests the knowledge of the Good Practice Guidelines subject matter across all six Professional Practices.

Successful candidates will gain a post nominal designation of CBCI which demonstrates the individual's knowledge of the Professional Practices in business continuity, and will become certified members of the BCI. CBCI certification is just the beginning. Individuals are encouraged to progress to more senior certified membership grades to demonstrate technical and professional competency. Employers increasingly specify BCI professional credentials for individuals seeking promotion or wishing to embark on, or change career in the industry. It is proven that those with BCI credentials; CBCI, DBCI, AMBCI, MBCI, AFBCI, and FBCI command higher salaries and enjoy enhanced career prospects.

Organizations that can demonstrate the competency of the individuals that they employ in business continuity roles benefit from enhanced reputation and in some industry sectors, compliance with legal and regulatory requirements.

By using the Good Practice Guidelines and having competent individuals employed to manage and implement business continuity, organizations are better protected and prepared to deal with disruption.

The BCM Lifecycle: Building organizational resilience.



The Professional Practices 2018

Management practices

PP1 Policy & Programme Management

PP2 Embedding

Technical practices

PP3 Analysis

PP4 Design

PP5 Implementation

PP6 Validation

What has changed from the GPG 2013?

The GPG 2018 edition reflects the progressive evolution of business continuity management as a discipline.

This revised version retains the six Professional Practices that make up the stages of the business continuity management lifecycle, and which lie at the core of good practice. The six Professional Practices are sub-divided into two management practices and four technical practices.

The focus and emphasis of this edition of the GPG has adapted as business continuity practices have become established and more organizations maintain embedded programmes. The 2018 edition provides guidance to business continuity professionals who are reviewing or revising an existing programme as well as continuing to be relevant to those who are initiating a new business continuity programme.

Several other changes have been undertaken throughout the 2018 edition to assist the reader's understanding and navigation. They include:

- Greater emphasis on when and how business continuity professionals can and should collaborate with professionals from other management disciplines to build more resilient organizations.

- References to supply chains and outsourced service providers are made throughout the guidelines and are no longer a separate section.
- Further guidance about understanding risk assessment and how the management of risk is allied to business continuity.
- An increase in cross-references throughout the guidelines to the other stages of the lifecycle and to other BCI publications and ISO standards.
- References to additional sources of information for further reading and guidance.
- Many examples and hints and tips shared by industry professionals to add context to the concepts presented in each stage of the lifecycle.

To reflect the evolving business continuity discipline, the use of terminology in the 2018 edition has been carefully considered and in most cases the BCI has adopted ISO terms and definitions. For example, 'prioritised activities' replaces 'most urgent', 'critical activities', 'key activities', and 'important activities'. This is for consistency with the international technical specification for performing the Business Impact Analysis ISO/TS 22317:2015.

In other cases, where there is no equivalent ISO definition, the 2018 edition proposes its own definitions in the interests of clarity and improved understanding. For example:

- The term 'continuity' is used throughout the GPG 2018 edition, and should be taken as a collective term to include response, recovery and resumption of activities impacted by a disruption.
- The business impact analysis described in the Analysis stage of the business continuity management lifecycle identifies the business continuity requirements, providing information to determine the most appropriate business continuity solutions.
- The previous use of the term 'business continuity strategies' in the Design stage of the business continuity management lifecycle has caused some confusion with organizational level strategies. Consequently, the GPG 2018 edition adopts the term "business continuity solutions".
- Business continuity requirements are defined as the time frames, resources, and capabilities necessary to continue to deliver the prioritised products, services, processes, and activities following a disruption.
- There is a clear distinction made in this edition between incident and crisis management and the level of response and capability required. This concept is introduced in the Policy and Programme Management stage, covered in detail in the Implementation stage and referenced throughout.

Acknowledgements

TThe Good Practice Guidelines 2018 edition is a revision of the 2013 edition and builds on the earlier 2010, 2008, 2007, 2005 and 2001 versions. The objectives are to:

- Recognise relevant changes within the business continuity management discipline.
- Ensure the BCI global good practices remain aligned with relevant international standards.
- Ensure the GPG remains internationally relevant.

The BCI would like to acknowledge the following individuals for their contribution to this project:

Working group leaders:
Chris Oliver FBCI, Lynda Vongyer AFBCI, Brian Zawada FBCI, Mohan Menon AFBCI, Matthias Rosenberg FBCI, Kenny Seow MBCI.

Volunteers:
Alberto Mattia MBCI, Anton Wroblewski MBCI, Brigitte Theuma MBCI, Charlie Maclean-Bristol FBCI, Des O'Callaghan FBCI, Ian Charters FBCI, John Worthington, Marc Decaffmeyer MBCI, Mel Gosling FBCI, Nathaniel Forbes MBCI, Norman Powell MBCI, Rudy Muls MBCI, Malcolm Brooke, Gianna Detoni FBCI, Alex van Os de Man MBCI, David Window MBCI, Iain Taylor Hon FBCI, James Royds Hon FBCI, Jim Burtles Hon FBCI, Kevin Shaughnessy MBCI, Michael Crooymans MBCI, Saul Midler FBCI, Malin Lundkvist MBCI, Rina Bhakta, Chris Green Hon FBCI, Jon Castle AMBCI, Paul Breed MBCI, Frederik Linde CBCI, Hassan Mashhadi, Shane McMahon AMBCI, Zech Wong MBCI, Adam Barrett MBCI, Ron Miller MBCI, Chris Bakowski AFBCI, Wasim Malik AFBCI, Tim Rippon MBCI, Nalin Wijetilleke AFBCI, Tim Janes Hon FBCI, David Parsons Hon FBCI, Matthew Coffey AFBCI, Brendan Jones MBCI, David Porter AMBCI, Henri Haenni MBCI, Julie Goddard MBCI, Louise Perkins, Rebecca Robinson AMBCI, Reginald Atta-Kesson MBCI, Nashikta Authar AMBCI, Heather Merchan MBCI, David Danher AFBCI, Margaret Millett MBCI, Kimberly Hirsch MBCI, Raymond Ee MBCI, Paul Trebilcock FBCI, Toby Marriner MBCI, Robert Grosso Ciponte MBCI.

The BCI Central Office GPG 2018 editorial team:
Deborah Higgins FBCI – Editor in Chief
Lesley Grimes FBCI – Assistant Technical Editor
Anne Greenish – Assistant Editor

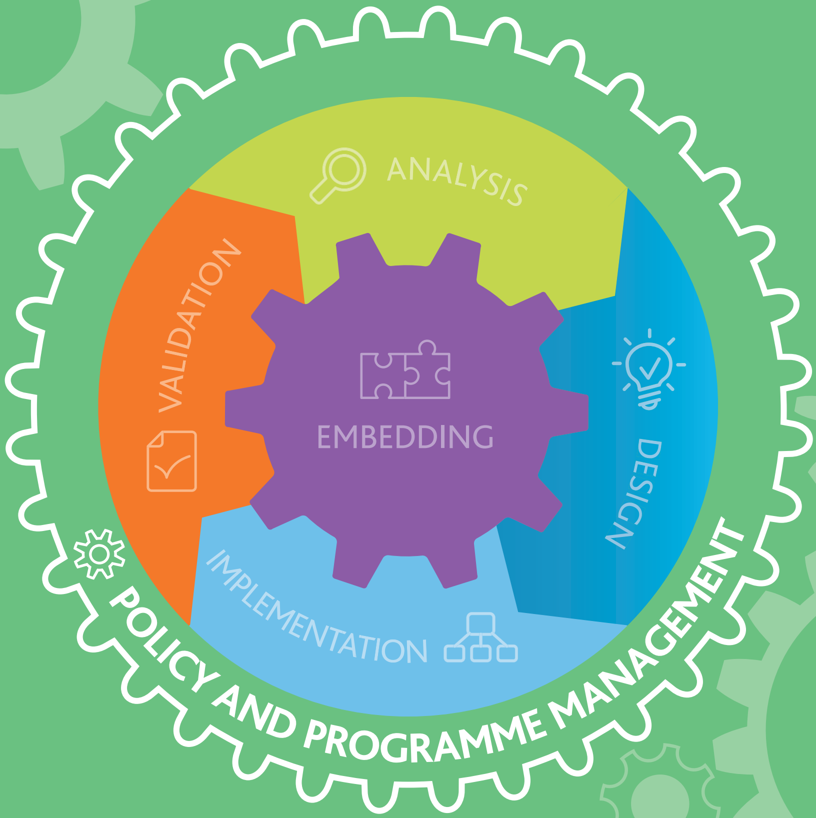
Special thanks to Tim Janes Hon FBCI for additional editorial contributions and advice.

Permission to reproduce extracts from ISO 22301:2012 and ISO/TS 22317:2015 is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001,
Email: cservices@bsigroup.com.

Glossary of Terms

Term	Definition	Source
Activity or activities	One or more tasks undertaken by, or for an organization, that produces or supports the delivery of one or more products and services.	GPG 2018
Analysis (PP3)	Analysis is the Professional Practice within the business continuity management lifecycle that reviews and assesses an organization to identify its objectives, how it functions and the constraints of its operating environment.	GPG 2018
Audit	A 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 22301:2012
Business Continuity (BC)	The capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident.	ISO 22300:2012
Business continuity management	A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.	ISO 22301:2012
Business Continuity Management (BCM) Lifecycle	The ongoing cycle of activities of the business continuity programme, that build organizational resilience.	GPG 2018
Business Continuity Management System (BCMS)	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.	ISO 22301:2012
Business continuity plan (BCP)	Documented procedures that guide organizations to respond, recover, resume, and restore to a predefined level of operation following disruption.	ISO 22301:2012
Business continuity programme	The ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.	ISO 22301:2012
Business continuity requirements	The time frames and resources, and capabilities necessary to continue to deliver the prioritised products, services, processes, and activities following a disruption.	GPG 2018
Business impact analysis (BIA)	The process of analysing activities and the effect that a business disruption might have upon them.	ISO 22300:2012
Competence	The ability to apply knowledge and skills to achieve intended results.	ISO 22301:2012
Continual improvement	A recurring activity to enhance performance.	ISO 22301:2012
Crisis	A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action.	ISO 22300:2012
Design (PP4)	Design is the Professional Practice within the business continuity management lifecycle that identifies and selects appropriate solutions to determine how continuity can be achieved in the event of an incident	GPG 2018
Embedding (PP2)	Embedding is the Professional Practice that defines how to integrate business continuity awareness and practice into business as usual activities.	GPG 2018
Exercise	The process to train for, assess, practice, and improve performance in an organization.	ISO 22301:2012
Implementation (PP5)	Implementation is the Professional Practice within the business continuity management lifecycle that implements the solutions agreed in the Design stage. It also includes developing the business continuity plans and a response structure.	GPG 2018
Incident	A situation that might be, or could lead to, a disruption, loss, emergency or crisis.	ISO 22300:2012

Term	Definition	Source
Interested party	A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.	ISO 22301:2012
Invocation	The act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services.	ISO 22301:2012
Maximum acceptable outage (MAO)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. See also MTPD.	ISO 22301:2012
Maximum tolerable period of disruption (MTPD)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. See also MAO.	ISO 22301:2012
Minimum Business Continuity Objective (MBCO)	The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.	ISO 22301:2012
Organization	The person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.	ISO 22301:2012
Organizational resilience	The ability of an organization to absorb and adapt in a changing environment.	ISO 22316:2017
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
Personnel	People working for and under the control of the organization.	ISO 22301:2012
Policy	The business continuity policy provides the intentions and direction of an organization as formally expressed by its top management.	ISO 22301:2012
Policy and Programme management (PP1)	Policy and Programme management is the Professional Practice that establishes the organization's policy relating to business continuity and defines how the policy should be implemented throughout the business continuity programme.	GPG 2018
Prioritised activities	The activities to which priority must be given following an incident in order to mitigate impacts.	ISO 22300:2012
Process	A set of interrelated or interacting activities which transforms inputs into outputs.	ISO 22301:2012
Products and services	Beneficial outcomes provided by an organization to its customers, recipients and interested parties.	ISO 22301:2012
Recovery point objective (RPO)	The point to which information used by an activity must be restored to enable the activity to operate on resumption.	ISO 22301:2012
Recovery time objective (RTO)	The period of time following an incident within which a product or service must be resumed, or activity must be resumed, or resources must be recovered.	ISO 22301:2012
Resources	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective.	ISO 22301:2012
Risk	The effect of uncertainty on objectives.	ISO/IEC Guide 73
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.	ISO/IEC Guide 73
Risk management	Coordinated activities to direct and control an organization with regard to risk.	ISO/IEC Guide 73
Test	An exercise whose aim is to obtain an expected, measurable pass/fail outcome.	ISO 22300:2012
Threat	A potential cause of an unwanted incident, which can result in harm to individuals, the environment or the community.	ISO 22300:2012
Top management	A person or group of people who directs and controls an organization at the highest level.	ISO 22301:2012
Validation (PP6)	Validation is the Professional Practice within the business continuity management lifecycle that confirms that the business continuity programme meets the objectives set in the policy and that the plans and procedures in place are effective. It includes exercising, maintenance and review activities.	GPG 2018


ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
EMBEDDING
POLICY AND PROGRAMME MANAGEMENT

BCI Professional Practices

PP1

Policy and Programme Management

Policy and Programme Management is the Professional Practice that establishes the organization’s policy relating to business continuity. It defines how this policy should be implemented, through an ongoing cycle of activities within a business continuity programme.

This stage of the business continuity management lifecycle requires top management action, support, and commitment to set up, draft and review the policy relating to business continuity and the programme used to implement it.

Introduction

Business continuity is a key management discipline that builds and improves organizational resilience. An effective business continuity programme is essential for any organization that seeks to develop and enhance organizational resilience.

The business continuity policy is the key document that sets out the purpose, context, scope, and governance of the business continuity programme.

The business continuity programme is an ongoing cycle of activities that implements the policy. These activities are carried out by following the business continuity management lifecycle.

Whilst the business continuity programme is being implemented and embedded into business as usual activities, it is important that an organization has some capability to manage an incident or crisis. If there is no such capability in place when implementing a business continuity programme for the first time, an interim structure and plan should be put in place to ensure the organization can respond to an incident.

In a large or complex organization, where a fully scoped business continuity programme may take many months to complete, an interim response structure and plan may be a sensible temporary measure. This may involve completing an initial BIA to identify high-level organization priorities, producing a strategic-level business continuity plan and conducting a short discussion-based exercise. These interim measures can then be reviewed and expanded as part of the fully scoped business continuity programme.

Establishing the Business Continuity Policy

The policy "provides the intentions and direction of an organization as formally expressed by its top management." (Source: ISO 22301:2012)

The business continuity policy sets the boundaries and requirements for the business continuity programme and states the reasons why it is being implemented. It defines the guiding principles which the organization follows and measures its performance against. It also defines how the organization should build and maintain the programme to continue to deliver products and services in the event of an incident.

General Principles

The business continuity policy provides the guiding principles around which the business continuity programme is designed and built. The policy acts as a statement to communicate the organization's principles to interested parties. As its primary purpose is communication, it should be short, clear, precise and to the point.

The following general principles should be considered when creating or revising a business continuity policy:

- The policy should provide the strategic direction from which the business continuity programme is delivered.
- The policy should define the way in which the organization will approach business continuity and how the programme will be structured and resourced.
- The policy should be supported, approved, and owned by top management to provide effective governance and leadership.
- The policy should state how it supports the strategic objectives of the organization and other relevant policies.
- The policy should be appropriate to the size, complexity, and type of organization and aligned to its culture and operating environment.
- The policy should identify any standards or guidelines that are used as a benchmark for the business continuity programme.
- The policy should be communicated, and made available to all interested parties.

A long and complicated policy will be a barrier to effective communication and embedding business continuity. The policy should focus on 'what' the organization will do, not 'how' it will be done.

Concepts and Assumptions

- Following the creation or revision of the policy, an ongoing programme of activities should be established to implement it.
- The business continuity professional should work with those individuals in the organization who have the responsibility for creating policies where appropriate.

Methods and Techniques

The following methods and techniques should be considered when establishing the business continuity policy:

- Control the distribution of the policy using an appropriate version control system.
- Use an existing template or policy (where one exists in the organization).

The use of project management methodology enables the organization to build and maintain effective business continuity management. It is also important to adopt a method that is suitable for the organization. If a method already exists in the organization, it is advisable to adopt it.

Process

The steps required to develop an effective business continuity policy are:

1. Agree the definition and objectives for business continuity within the organization.

2. Agree the scope of the business continuity programme.

3. Identify and agree on the standards or guidelines that will be used as a benchmark for the organization's business continuity programme.

4. Review and conduct a gap analysis of the organization's current policy against any new requirements where appropriate.

5. Draft the new or revised policy.

6. Review the draft policy against the organization's current standards or policies addressing related management disciplines. Identify any duplication and seek opportunities to collaborate as appropriate.

7. Circulate the draft policy for consultation with top management and other relevant interested parties.

8. Amend the draft policy, as appropriate, based on consultation feedback.

9. Facilitate the approval and sign-off of the policy by top management.

10. Ensure the approved policy is communicated to all interested parties.

Outcomes and Review

The business continuity policy should include:

- A definition of business continuity for use in the organization.
- A statement of governance and leadership commitment to the policy.
- Defined objectives and scope for the business continuity programme.
- Roles and responsibilities for the business continuity programme including an incident response capability.
- References to relevant policies, standards, and legal and regulatory requirements.
- Identification of interested parties.
- Agreed methods and frequency for measurement and review of all stages of the business continuity lifecycle.
- Agree methods for sign-off and communication of the policy and all programme activities.

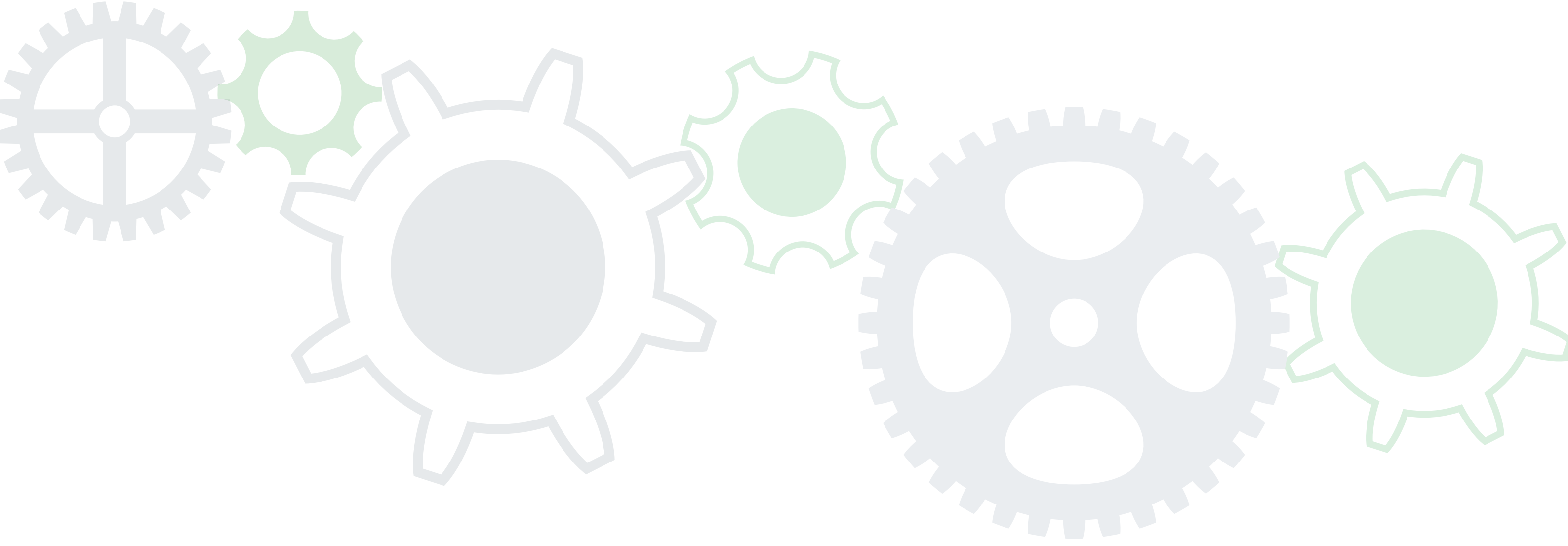
The business continuity policy should be regularly reviewed at pre-agreed intervals or following significant changes, including:

- A change in the organization's approach to risk which can be prompted by an incident or change.
- A change in market conditions.
- An acquisition, merger, or disposal.
- Changes to products or services (including those that are outsourced).
- Changes to legal or regulatory requirements.

The above changes can lead to a review at all stages of the business continuity management lifecycle.

When reviewing or auditing a business continuity policy, the following should be demonstrated:

- Top management has ensured that the policy is communicated throughout the organization.
- The policy is effective.
- The policy clearly states what the measurable deliverables of the business continuity programme are.
- There is clear top management commitment to satisfy all applicable internal and external requirements within the scope of the programme.
- There is clear and documented ongoing commitment to business continuity and continual improvement.
- Opportunities for adapting to change can be identified.



Defining the Scope of the Business Continuity Programme

The business continuity policy should clearly define the scope of the business continuity programme. Defining the scope includes consideration of the organization's products and services that are to be included or excluded in the programme. The Analysis stage should identify the requirements for business continuity and may assist with modifying the scope of the programme.

General Principles

The following are general principles that should be considered when determining the scope of the business continuity programme as part of the business continuity policy implementation:

- A definition of the scope of the programme ensures a clear understanding of which areas of the organization are to be included and which are excluded. This focuses the business continuity programme and associated activities on the organization's priorities and ensures the programme makes best use of available resources, for example, available budget.

- An understanding of the organization's strategy, objectives, culture, operating environment, and approach to risk is essential when considering the scope of the programme. Early engagement with other relevant departments or professionals such as corporate governance, enterprise risk, and security, at this stage is important and should also help to avoid overlap or conflict. Taking this organization-wide view and collaborating with others at this stage will be key to successful implementation of the business continuity policy and programme and the overall resilience of the organization.

- An understanding of the outsourced activities and suppliers of products and services.

- An understanding of the business continuity programme as an ongoing process. The programme can be implemented in stages, by focusing on some parts of the organization and extending it to other parts later. This staged implementation approach has the benefit of reducing complexity, cost, and scale. Limiting the initial scope of the business continuity programme allows for a staged approach for implementation and helps to manage risk across the organization.

Concepts and Assumptions

- The scope of the business continuity programme should be determined before proceeding with the Analysis, Design, Implementation, and Validation stages of the business continuity management lifecycle and should be reviewed at pre-agreed intervals.

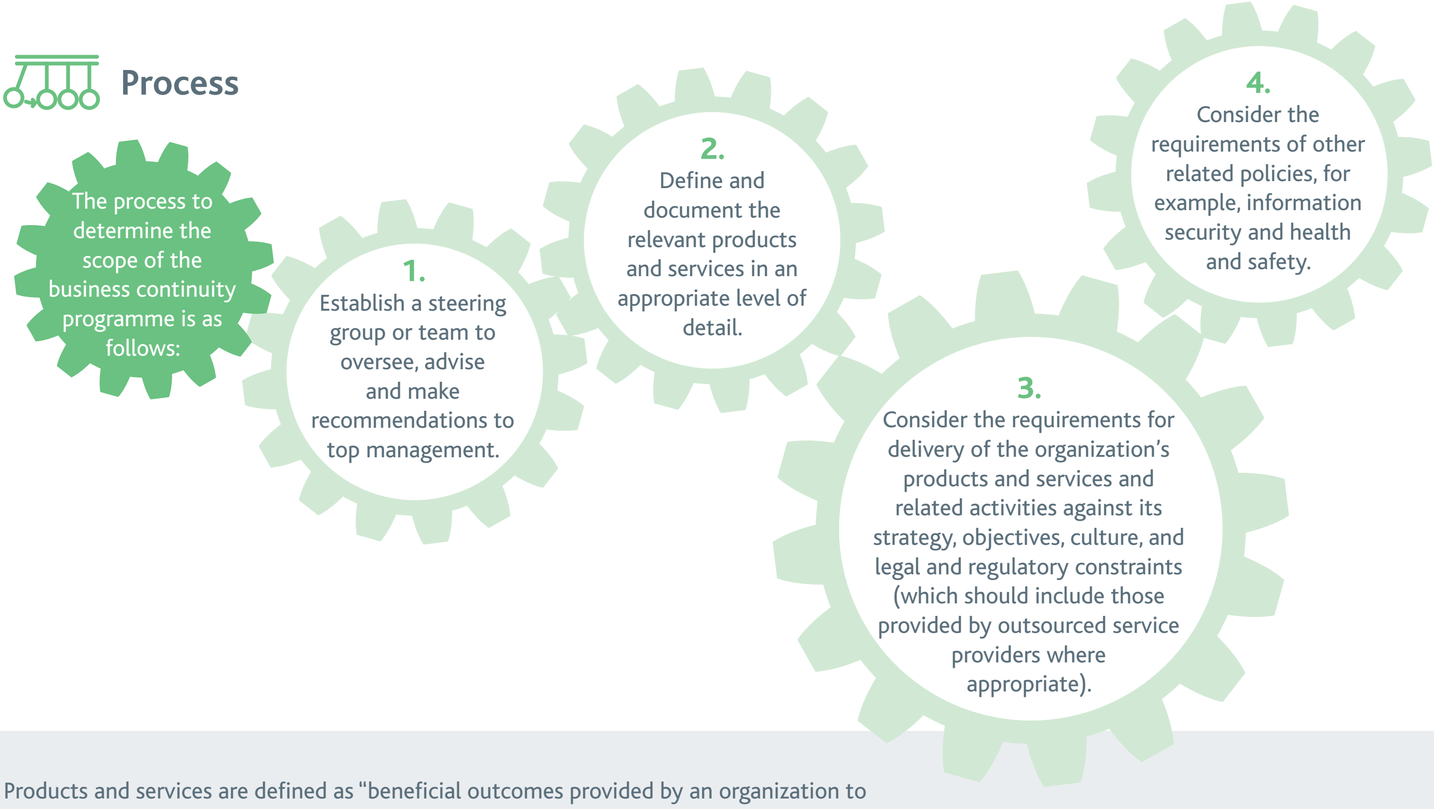
- The scope is usually defined in relation to products and services, however location may also be used to limit the scope, allowing the programme to include or exclude certain locations and sites.

- There may be occasions when an organization decides to start its initial implementation of the business continuity programme based on an agreed priority for a specific product or service. For example, a regulatory requirement, a customer demand, certification against a standard or an audit finding. In this case, the whole organization will need to include all the activities that are related to that product or service in the scope.

- When an external provider is involved in the delivery of a product or service that is within the scope of the programme, this supplier and their supply chains should also be included. This extends to supporting information and communication technology (ICT) and resources.

- When determining the scope of the programme, it is important to consider the maximum extent of damage, loss, or disruption to the organization. It is recommended that a crisis management capability is available or developed to address disruption beyond that scope.

Process



The process to determine the scope of the business continuity programme is as follows:

1. Establish a steering group or team to oversee, advise and make recommendations to top management.

2. Define and document the relevant products and services in an appropriate level of detail.

3. Consider the requirements for delivery of the organization’s products and services and related activities against its strategy, objectives, culture, and legal and regulatory constraints (which should include those provided by outsourced service providers where appropriate).

4. Consider the requirements of other related policies, for example, information security and health and safety.

Products and services are defined as “beneficial outcomes provided by an organization to its customers, recipients and interested parties…” (Source: ISO 22301:2012)

Examples of products and services are as follows:

A manufactured product or range of products.

Car insurance.

Waste collection (for a municipality or local government).

Payroll.

Logistics (for a distribution organization).

Telephone support (for a software organization).

Decisions on which products and services to include in the scope may be prompted by:

- Products which make a significant contribution to the organization’s reputation, income, or success.
- A customer contractual requirement.
- A legal or regulatory requirement.
- Physical threats, for example, proximity to other industrial premises such as a chemical manufacturing plant or hazards such as flooding.

Reasons for why a product or service may be excluded from the scope include:

- Nearing end of life (and would be terminated if disrupted).
- Low margins or low volumes (could be terminated or externally sourced if disrupted).

When deciding whether to exclude a product or service, the following issues should be considered:

- Financial loss.
- Interested parties who may be impacted by the loss of the product or service, for example, a medicine that is only made by one organization.
- Reputational damage resulting from an incident or termination in the supply of the organization’s products or services.
- The impact on legal or regulatory requirements.
- The needs and expectations of customers and other interested parties.

Reasons for excluding a product or service, together with an alternate solution to the loss of that product or service, need to be documented and agreed by top management. It is also important that the risk to the organization is fully understood and managed (this is covered further in the Analysis stage). When reviewing an existing policy and programme, the scope should be reconsidered to reflect any change in the organization’s overall strategy or operating environment. Those products and services that are out of scope should be managed outside of the business continuity programme. Top management should fully understand the implications of these choices, and document and sign off any decisions as part of the governance process.

Methods and Techniques

Methods and techniques used to decide how to define the scope of the business continuity programme include:

- Cost benefit analysis.
- Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis.
- Benchmarking against appropriate standards or guidelines.
- Market analysis techniques.
- Business impact analysis (BIA) and risk assessment (if these have already been conducted).

A detailed risk assessment is carried out in the Analysis stage of the business continuity management lifecycle. This information, and the resulting information from horizon scanning activities can provide useful input into the definition and clarification of the scope of the programme.

The business continuity professional should collaborate with other professionals both inside and outside their organization if these methods and techniques are already in use, for example, risk management, procurement, audit etc. In organizations which do not have the capability to carry out these recommended methods, it may be necessary to use an external service provider.

Outcomes and Review

The outcome is a clearly defined scope for the business continuity programme, which can be validated to ensure that the objectives of the business continuity policy are being met.

The scope of the business continuity programme should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Establishing Governance

Establishing governance for business continuity provides a central point of accountability for implementation and continuous monitoring of organization activities in accordance with the business continuity policy.

General Principles

Governance activities should include monitoring and measuring progress against key performance indicators to confirm that the business continuity policy and programme is being implemented effectively and is aligned with organizational objectives and strategy.

There are several sources of guidance for professionals on how to develop, manage, implement, and review a business continuity programme. The international standard for business continuity management ISO 22301:2012, identifies management and governance processes for operating, monitoring, reviewing and continually improving a business continuity management system. Requirements for governance of business continuity are also provided in national or international standards, legislation, regulations, or industry sector specific guidelines. Regulations in some sectors may require formal demonstration of effective business continuity management to the organization's top management.

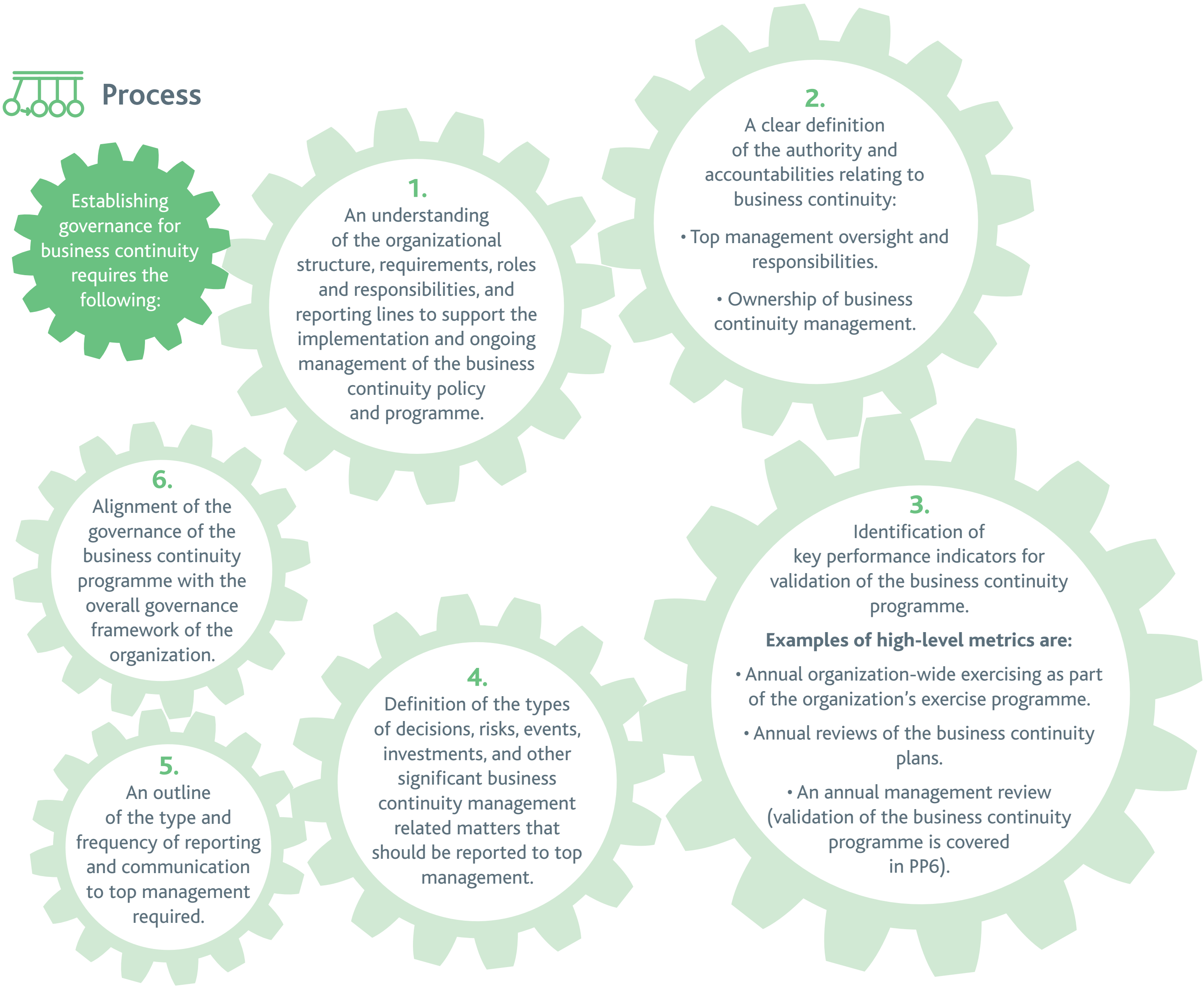
Concepts and Assumptions

Governance for business continuity primarily focuses on:

- Providing oversight and support of the business continuity programme, including provision of adequate resources and approval of budget.
- Ensuring the business continuity programme aligns with the organization's objectives.
- Ensuring the business continuity programme complies with the business continuity policy and any related legal and regulatory requirements.
- Monitoring and reviewing the business continuity programme regularly to ensure the requirements are being met.
- Supporting continual improvement.

The business continuity policy should clearly define the organization's oversight of, and commitment to, the business continuity programme. Business continuity should be aligned to the related management disciplines, for example, risk management, information security and physical security, as part of the overall approach to addressing risks and threats, and building organizational resilience.

Process



Establishing governance for business continuity requires the following:

1. An understanding of the organizational structure, requirements, roles and responsibilities, and reporting lines to support the implementation and ongoing management of the business continuity policy and programme.

2. A clear definition of the authority and accountabilities relating to business continuity:

- Top management oversight and responsibilities.
- Ownership of business continuity management.

3. Identification of key performance indicators for validation of the business continuity programme.

Examples of high-level metrics are:

- Annual organization-wide exercising as part of the organization's exercise programme.
- Annual reviews of the business continuity plans.
- An annual management review (validation of the business continuity programme is covered in PP6).

4. Definition of the types of decisions, risks, events, investments, and other significant business continuity management related matters that should be reported to top management.

5. An outline of the type and frequency of reporting and communication to top management required.

6. Alignment of the governance of the business continuity programme with the overall governance framework of the organization.

Methods and Techniques

Top management should ensure that the importance of business continuity and the business continuity policy is communicated.

Leadership and commitment to the business continuity policy and programme can be achieved using the following methods and techniques:

- Recognising and communicating the requirement for business continuity as a key management discipline when building and enhancing organizational resilience.
- Ensuring that the business continuity policy and programme is aligned to the objectives of the organization.
- Ensuring that the business continuity programme delivers its expected outcomes and meets the requirements stated in the policy.
- Maintaining support for the business continuity policy and programme.
- Ensuring individuals undertake activities so the business continuity programme is effective.

Business continuity related roles and responsibilities should be included in job descriptions and performance plans.

- Providing the resources required to implement the policy through the ongoing cycle of activities in the business continuity programme.
- Directing and supporting continual improvement of the business continuity programme for example, through reviews and self-assessments.
- Providing direction and guidance to embed business continuity into the organization's business as usual routines.

Outcomes and Review

By defining governance when establishing the business continuity policy, top management should be fully involved and accountable for the performance and effectiveness of the business continuity programme from the outset.

Top management should ensure that the business continuity policy states what measurement is required to ensure an effective business continuity programme. The appropriate methods are part of the Validation stage of the business continuity management lifecycle and are included in the business continuity programme.

The organization's top management should agree:

- What needs to be measured and monitored.
- How this should be achieved.
- The methods for monitoring, measuring, analysing, and evaluating.
- When monitoring and measuring should be performed.
- When monitoring and measuring results should be analysed and evaluated.

To do this, top management should:

- Act to address any areas of weakness or gaps in the business continuity programme objectives.
- Monitor the effectiveness of the programme.
- Ensure that the relevant information is retained as evidence of the results.

Governance of the business continuity policy and programme should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Assigning Roles and Responsibilities

An effective business continuity programme is dependent upon the early identification of clearly defined roles and the associated responsibilities and authorities to manage the programme. This will have been identified in the business continuity policy.

General Principles

The purpose of assigning roles and responsibilities is to ensure that the tasks required to implement and maintain the business continuity programme are allocated to specific, competent individuals whose performance can be evaluated and where further training requirements can be identified. The training and competency requirements for the business continuity professional and wider programme are covered in PP2.

Top management should assign accountability, responsibility, and authority to designated teams or individuals to ensure that appropriate procedures are adopted and properly implemented in accordance with the requirements of the policy. Top management should also ensure that these roles are communicated to the relevant interested parties.

Top management should ensure individuals carry out their roles as appropriate within the organization. Where the individuals are assigned business continuity responsibilities in addition to their existing role, the new responsibility should be added to their job description and communicated to all interested parties. The performance of these individuals should be measured as part of the Validation stage of the business continuity management lifecycle on an ongoing basis.

Concepts and Assumptions

Roles and responsibilities should be assigned to individuals with relevant competencies who have the appropriate authority for the role they are assigned.

By assigning a member of top management overall accountability for business continuity and its effectiveness, the organization ensures that:

- Business continuity is recognised as a key activity within the organization.
- Implementation will be achieved through collaboration with other related disciplines.
- Appropriate response roles and responsibilities will be defined based on competency.

Process

A competent individual should be identified and appointed to manage the implementation of the business continuity policy and programme. Depending on the size of the organization, this may be a full or part time role.

Additional individuals or teams may be assigned to assist with the ongoing management and delivery of the business continuity programme. These could include:

1. A business continuity steering group to give advice, guidance, and oversight.

2. Teams that will respond to an incident and that can contribute towards developing the incident response plans.

Methods and Techniques

The following table defines the skills and competencies required within the roles identified as part of the business continuity programme:

Table 1.

Role	Responsibility
Top management	Provide leadership, commitment, and resources as part of governance.
Steering group	Oversee, advise, and manage the business continuity programme, making recommendations, and reporting to top management.
Business continuity plan owner	Ensure that the business continuity plan adequately reflects the organization's business continuity capability.
Business continuity professional	Develop and deliver an effective business continuity programme. This includes facilitation and coordination of plans throughout the organization.
Incident response personnel	Respond to an incident or crisis.
Departmental representative	Communicate the implications of departmental changes that may impact the business continuity programme. Collect information for the BIA. Develop, implement, and maintain departmental plans on behalf of the plan owner. Conduct and participate in exercises.
All personnel	Acknowledge roles and responsibilities during an incident to ensure effectiveness by understanding the business continuity programme. Recognise an incident or crisis. Alert incident or crisis responders (including emergency responders as appropriate). Escalate action to the incident or crisis management team. Respond appropriately to specific threats. Respond appropriately when evacuated from the site. Understand relevant plans and associated roles and responsibilities.
Interested parties	Act where relevant within the business continuity programme or in response to an incident.

Alternate individuals should be assigned roles and responsibilities in case of planned or unplanned absence.

Succession plans should also be considered for individuals with specific roles and responsibilities, for example, incident response personnel, plan owners, and departmental representatives.

Those responsible for business continuity should 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

The outcome of assigning roles and responsibilities as part of business continuity policy and programme management are:

- Clearly defined roles and responsibilities assigned to competent individuals and teams.
- Appropriate authority assigned as relevant to the role.
- Roles and responsibilities, and authorities documented in the business continuity policy.
- Alternates for each role identified.
- Responsibilities included in the individuals' job descriptions and communicated to interested parties.

The roles, responsibilities and authorities assigned to individuals, and the competencies and skills required should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

The Business Continuity Programme

"The business continuity programme is an ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management." (Source: ISO 22301:2012)

The business continuity programme is put in place to implement the business continuity policy when the scope, governance and roles and responsibilities have been defined. An important part of the programme is to manage documentation to support the implementation where and when appropriate.

General Principles

The business continuity programme is an ongoing process, which adapts in response to the changing nature of an organization's internal and external operating environment.

Implementing a programme for the first time should involve undertaking all activities detailed in the business continuity management lifecycle, however revisions to the programme will likely involve less activity if there is no significant change in the organization's requirements.

During the initial implementation, sufficient time should be allocated to undertake the activities in each stage of the business continuity management lifecycle.

A flexible and comprehensive programme that is actively managed should be in place to ensure the organization maintains its business continuity capability and continues to develop and enhance organizational resilience.

Concepts and Assumptions

The initial implementation of the business continuity programme is likely to consist of several projects, and will benefit from the use of a recognised project management methodology and programme management capability.

Multiple business continuity professionals and individuals from other business areas may be involved in the business continuity programme. This will depend upon the size, complexity, and type of the organization.

In a small or medium sized organization, management of the business continuity programme may be given to one individual as part of their job role.

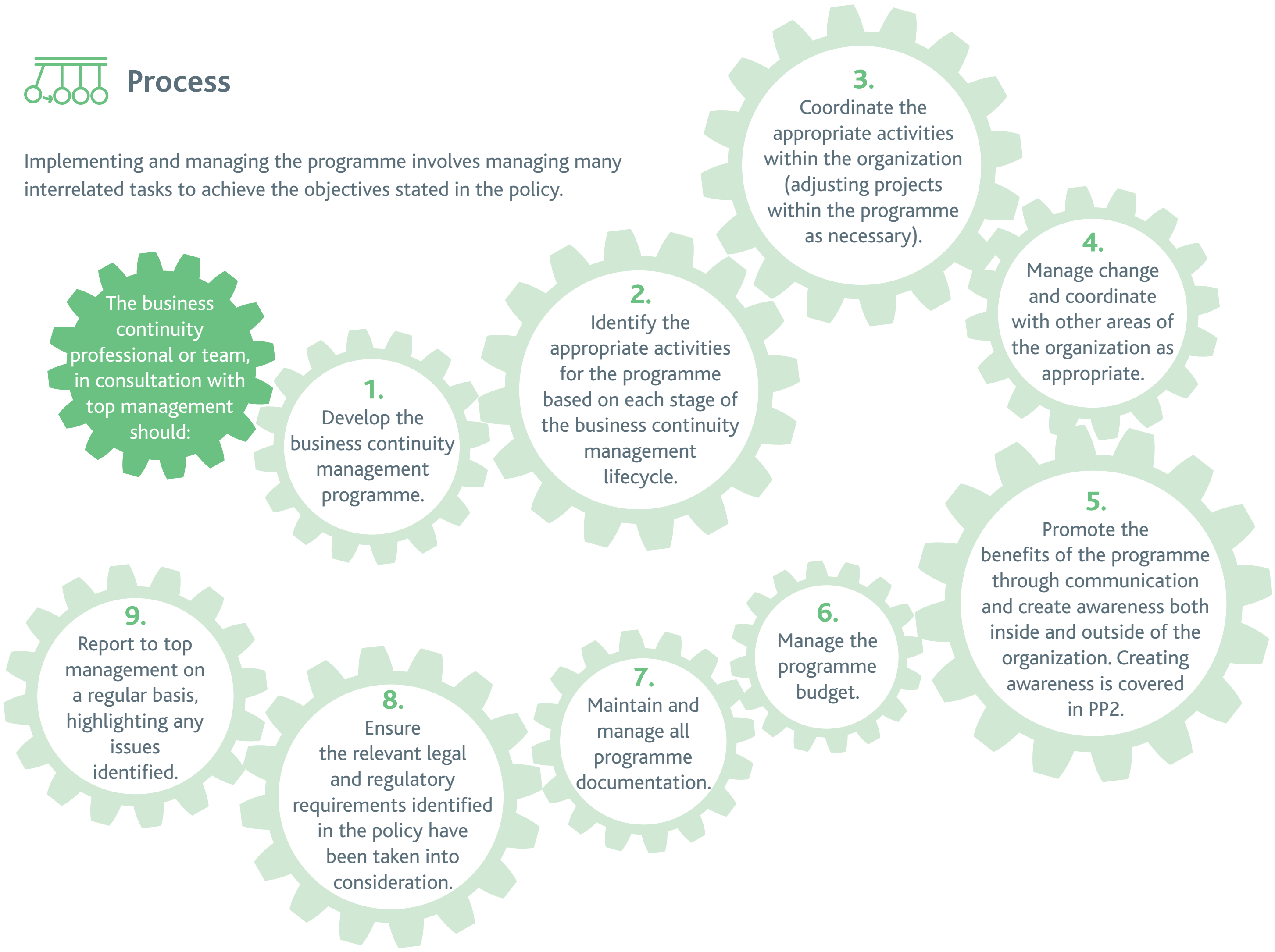
Other relevant policies and programmes within the organization should be identified and opportunities for collaboration should be considered and coordinated. For example, the human resources department may have policies for internal communications and the corporate communications department may have predetermined agreements for external communication due to a regulatory or customer requirement. These should be identified and incorporated within the business continuity programme.

The documentation in a business continuity programme has three purposes:

- To help manage the business continuity programme effectively.
- To demonstrate effective management of the programme.
- To enable a prompt and effective response to an incident.

Process

Implementing and managing the programme involves managing many interrelated tasks to achieve the objectives stated in the policy.



The business continuity professional or team, in consultation with top management should:

1. Develop the business continuity management programme.

2. Identify the appropriate activities for the programme based on each stage of the business continuity management lifecycle.

3. Coordinate the appropriate activities within the organization (adjusting projects within the programme as necessary).

4. Manage change and coordinate with other areas of the organization as appropriate.

5. Promote the benefits of the programme through communication and create awareness both inside and outside of the organization. Creating awareness is covered in PP2.

6. Manage the programme budget.

7. Maintain and manage all programme documentation.

8. Ensure the relevant legal and regulatory requirements identified in the policy have been taken into consideration.

9. Report to top management on a regular basis, highlighting any issues identified.

Methods and Techniques

Project management methodology is a useful approach when implementing the business continuity programme. Effective project management should increase the chances of successful delivery of the overall programme, within the agreed time frames and budgets.

Examples of projects as part of the business continuity programme are as follows:

- Developing and managing an exercise programme.
- Developing and delivering training and awareness activities.
- Selecting suppliers to deliver a defined product or service.

The following should also be considered when managing the programme:

- Relevant industry sector specific good practice or standards related to the business continuity discipline.
- Self-assessment against a relevant standard, legislation, or regulation.
- Relationships with suppliers or providers of outsourced activities.
- Financial management and budgetary requirements.
- Legal and regulatory advice.
- Internal and external audits (where appropriate).
- Reviews and change management requirements.

Business continuity software options can be considered a useful tool to support the business continuity programme. Specialist software may offer some advantages when managing large volumes of documents and projects. It is important to consider that this and any other technology selected as part of the programme may incur ongoing licence, maintenance, and training costs.

Outcomes and Review

The outcome of managing and implementing a business continuity programme is to maintain business continuity capability to build and improve organizational resilience using an adaptable and comprehensive approach.

A business continuity management programme consists of the following:

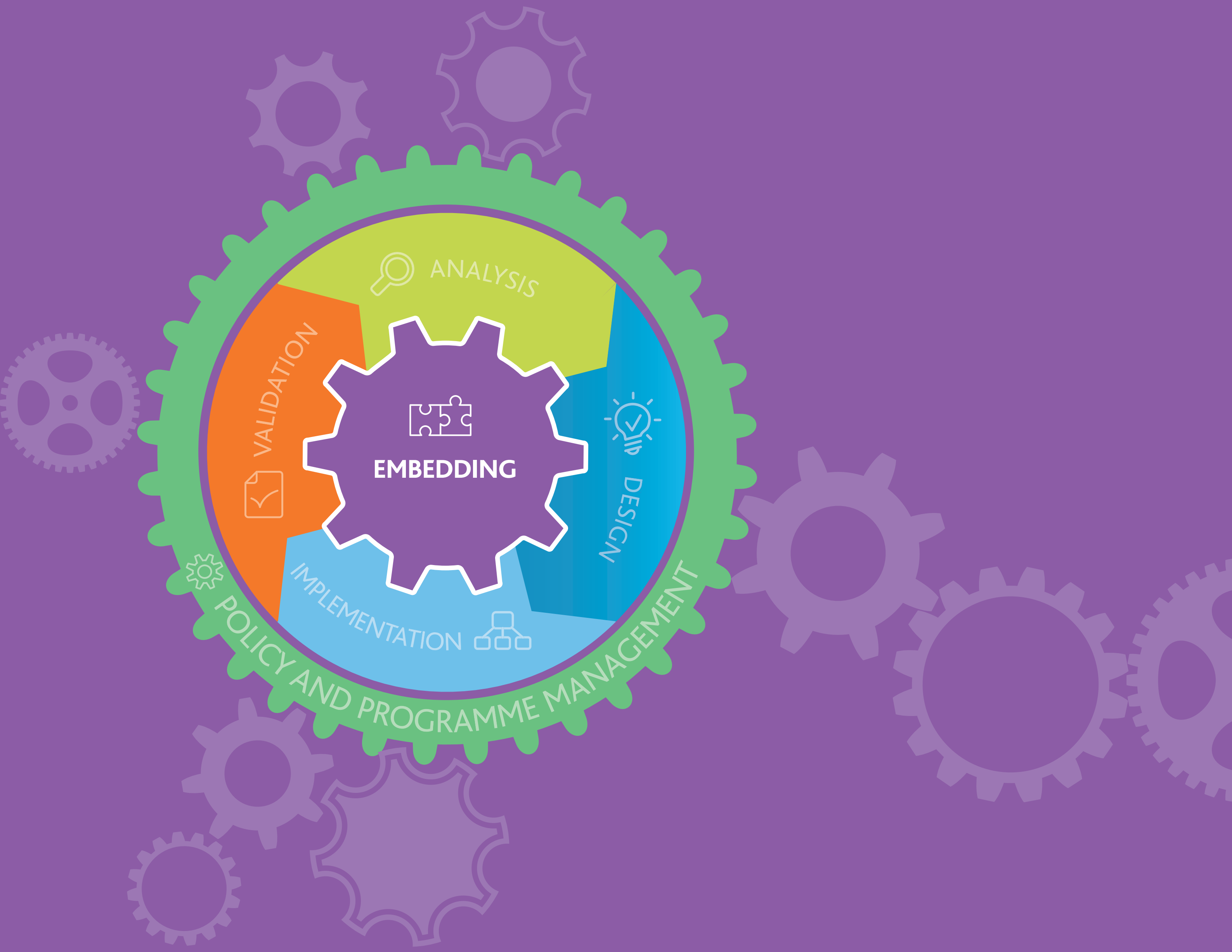
- A business continuity policy.
- A definition of the objectives of business continuity for the organization.
- A clearly defined scope.
- A definition of governance and leadership commitment.
- Roles and responsibilities.
- References to relevant policies, standards, and regulatory requirements.
- Identification of interested parties, including outsourced service providers.
- A method for review, measurement, sign off and communication.
- Ongoing budget commitment and financial support.

The business continuity programme documentation should include the following:

- Business continuity policy.
- Business continuity programme of activities.
- Project management documentation.
- Business continuity team meeting agendas, minutes, and action trackers.
- Skills and competency requirements and records.
- Training and awareness activities.
- BIA questionnaires and information.
- Risk assessment.
- Papers supporting the choice of business continuity solutions.
- Response structure.
- Business continuity plans.
- Crisis management plans.
- Exercise programme.
- Exercise reports.
- Service level agreements with customers and suppliers.
- Contracts for outsourced service provider recovery services, including workspace and salvage.
- A maintenance and review programme and reports.

The volume of programme documentation will depend on the size, complexity, and type of the organization.

The business continuity programme should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

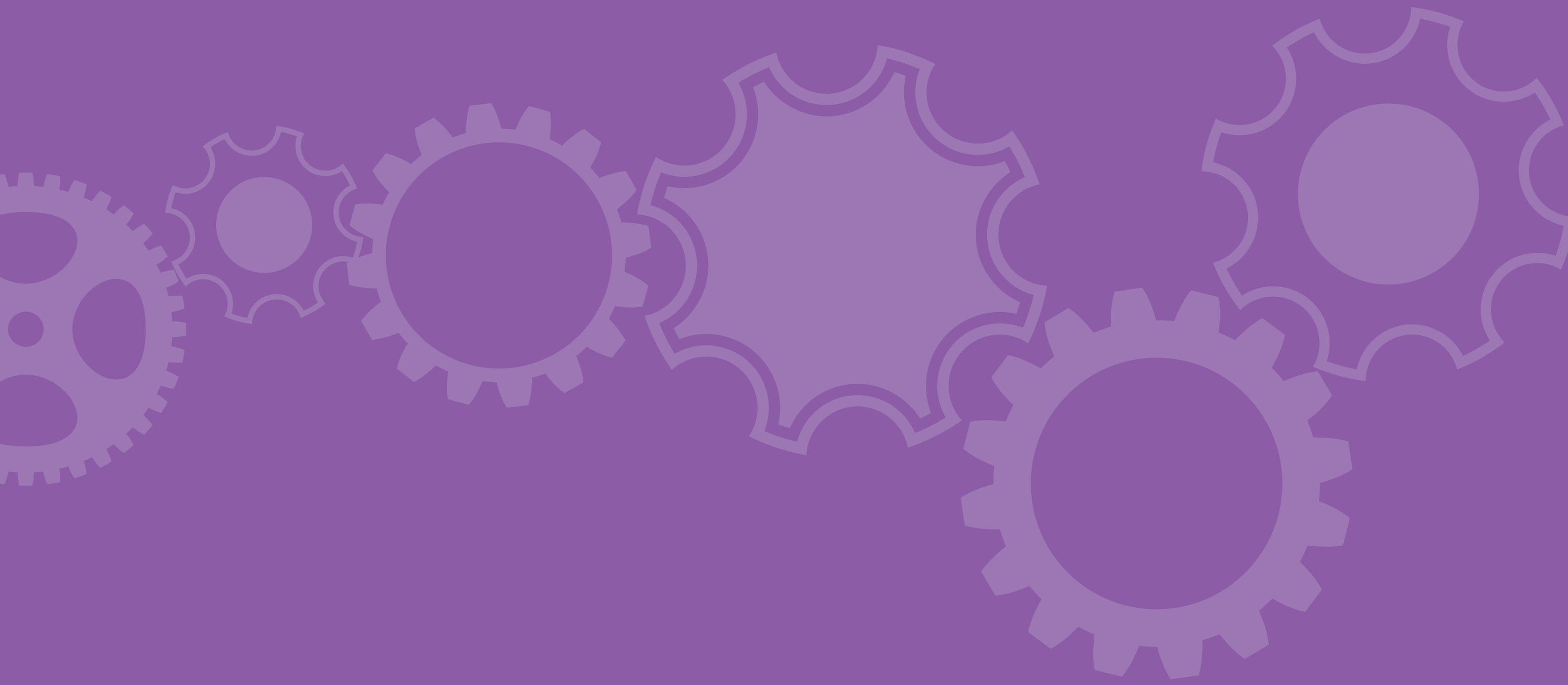

EMBEDDING
ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
POLICY AND PROGRAMME MANAGEMENT

BCI Professional Practices

PP2

Embedding Business Continuity

Embedding business continuity is the Professional Practice that defines how to integrate business continuity awareness and practice into business as usual activities and organizational culture. Embedding business continuity should be a collaborative approach between related management disciplines to improve overall organizational resilience.



Introduction

Embedding business continuity includes:

- Raising awareness about business continuity through communication.
- Encouraging buy-in from interested parties.
- Ensuring required competencies and skills are in place.
- Ensuring appropriate training and learning opportunities are provided.

Understanding and Influencing Organizational Culture

The following general principles should be considered when developing or revising the approach to embed business continuity into the organization's culture.

General Principles

Successfully embedding business continuity requires a collaborative approach from top management and the business continuity professional.

The goal of embedding business continuity is to ensure that it becomes part of business as usual across the organization.

Embedding business continuity activities should be aligned with the organization's strategic goals and culture.

Business continuity should also be considered and integrated into project and change management practices where appropriate.

The skills and competencies required to implement the business continuity policy and programme include both general management and technical skills.

Although difficult to observe and measure, culture plays an important role in the effectiveness of embedding the business continuity programme and the overall level of organizational resilience.

Successful embedding of an effective business continuity programme may require changes in the culture of the organization.

If starting a new business continuity programme, it is important to consider what the training and awareness priorities are. For example, training the individuals or teams that will be involved in response teams as a priority over organization-wide general awareness.

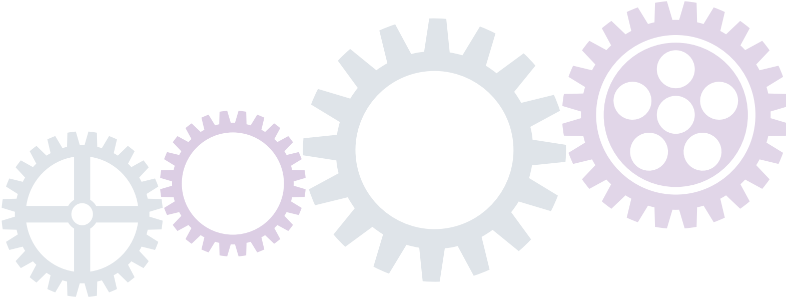
An existing programme would require a review of the embedding activities already in place. For example, a change in ownership, acquisition, or top management of an organization can result in changes to its culture as well as its strategic objectives and business operations.

Embedding activities are not unique to business continuity; other management disciplines are also embedded in a similar way. For example, health and safety, information security, and data protection practices are often part of personnel inductions.

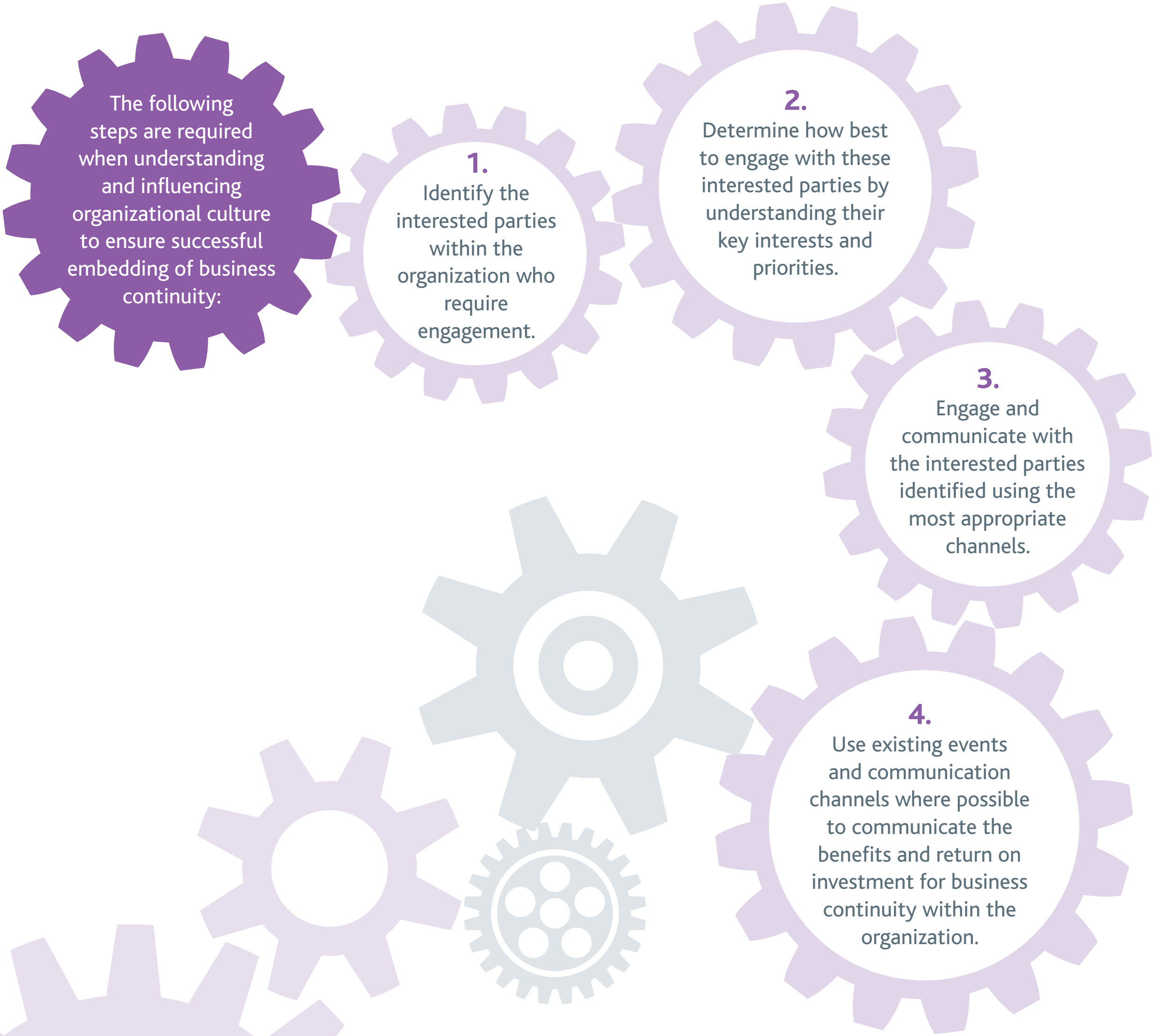
Concepts and Assumptions

Organizational culture can be defined as the "values, attitudes and behaviour of an organization that contribute to the unique social and psychological environment in which it operates."
(Source: ISO 22316:2017)

Organizational culture is sometimes referred to as 'the way things are done around here'.



Process



The following steps are required when understanding and influencing organizational culture to ensure successful embedding of business continuity:

1. Identify the interested parties within the organization who require engagement.

2. Determine how best to engage with these interested parties by understanding their key interests and priorities.

3. Engage and communicate with the interested parties identified using the most appropriate channels.

4. Use existing events and communication channels where possible to communicate the benefits and return on investment for business continuity within the organization.

Build a network of influential individuals in the organization who understand the benefits of business continuity and building organizational resilience. These individuals can act as advocates or 'champions' who make a significant contribution to successful embedding of business continuity. In organizations where such representatives exist in related management disciplines, there may also be opportunities to collaborate.

Methods and Techniques

Depending on the maturity of the organization's business continuity programme, there are several effective embedding methods that, if not already in place, should be considered:

- Changing attitudes and behaviour. It can be useful to identify the consequences of action (or inaction) and make it relevant to a person's short-term business objectives or welfare. For example, if another organization of a similar type in a similar location, has experienced disruption or significant change, and acted in a way that demonstrated a high level of resilience, lessons can be learned and shared. Equally, if an organization of a similar type in a similar location has failed to act, this can also provide learning opportunities.

- Ensuring that business continuity is considered by top management when the organization's strategic plan is being developed or reviewed.

- Including business continuity on relevant meeting agendas.

- Incorporating business continuity plans into standard operating procedures.

- Including business continuity awareness as part of induction processes.

- Scheduling business continuity exercises to coincide with planned shutdowns or quieter times.

- Ensuring business continuity requirements are considered as part of supply chain management.

- Ensuring any new products or services consider business continuity during the planning stages.

The business continuity professional should also consider and address how to effectively support, encourage and educate top management to obtain and maintain support. They should also consider the development of business continuity awareness, including the following:

- Changing roles and responsibilities.

- High personnel turnover.

- Regularly changing business processes.

- High volume of acquisitions and outsourced activities.

A continual effort is required by the business continuity professional in any organization, however, this effort will be greater in fast moving environments.

A relevant business continuity exercise which is carefully scoped and conducted, based on current risks and threats, can be an effective method to help to raise awareness and change attitudes and behaviour.

Existing emergency routine procedures, for example, fire alarm testing, practice evacuations, or security threat drills, can also be used as a business continuity exercise. Linking business continuity exercises with related events can help demonstrate the value and benefit of business continuity. Organizations in some industry sectors and regions, may have a legal or regulatory requirement to undertake exercises. These may be in the form of simple fire evacuations or large-scale exercises in conjunction with the emergency services and other interested parties. The business continuity professional should seek opportunities to integrate business continuity into these planned events whenever possible.

To motivate changes in behaviour, remove the word 'Fire' from Fire Alarm, Fire Marshall, Fire Warden, and Fire Drill where they are used. It could be replaced with the word 'Evacuation' to become Evacuation Alarm, Evacuation Marshall, Evacuation Warden, and Evacuation Drill. By doing this; roles, responsibilities, processes, and actions do not change, but personnel should recognise that their roles are not specific to a particular type of disruption. An evacuation could be activated for multiple types of disruption, not just a fire.

Competencies and Skills

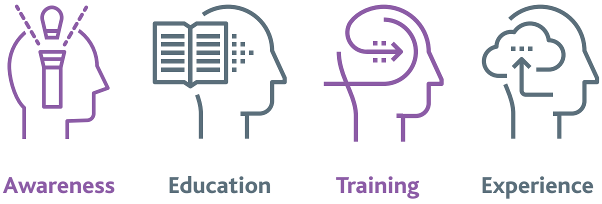
The business continuity and resilience professional, and all individuals with roles and responsibilities for business continuity should have the appropriate education, training and experience required for the development and implementation of the business continuity policy and programme as defined in PP1. The competencies and skills required of individuals should be understood by the business continuity professional and top management when embedding business continuity, to ensure the programme is delivered.

Consideration should also be given to the requirements for alternates in the event of absence, and succession planning to maintain the capabilities required.

> It is important that alternates are aware of their roles and responsibilities and are prepared and involved in the relevant programme activities.

General Principles

The business continuity professional and top management should ensure that all personnel (including any external consultants or other interested parties) who are involved in the business continuity programme have the appropriate level of awareness, education, training, and experience. This may also include key personnel in the supply chain and outsourced service providers.



The table below shows the specific core competencies and general management skills required of the business continuity professional:

Table 2.

Professional Practices	Core Competencies	Management Skills
Management Practice **PP1** – Policy and Programme Management	Project management skills and an understanding of the importance of continual improvement.	An understanding of the context of the organization and the environment in which it operates, as well as its approach to managing risk. The ability to form an organization-wide view. An ability to understand and collaborate with personnel in related management disciplines. Effective communication and interpersonal skills. Negotiating and influencing skills to gain and keep top management buy-in and commitment. Facilitation skills to guide and direct workshops, planning sessions, meetings, training, and exercises to achieve productive outcomes.
Management Practice **PP2** – Embedding business continuity	An understanding of the organizational culture and how to influence it. Knowledge of the business continuity competencies and skills required and training and awareness raising capabilities.	
Technical Practice **PP3** - Analysis	Analytical skills relating to the BIA, including the ability to analyse information, identify problems, and develop workable solutions. An understanding of risk assessment and mitigation measures.	
Technical Practice **PP4** - Design	The ability to design and select appropriate continuity solutions for the organization.	
Technical Practice **PP5** - Implementation	An understanding of incident and crisis management, including knowledge of emergency response. The ability to develop, implement and manage plans.	
Technical Practice **PP6** - Validation	The ability to develop, manage, coordinate, and deliver an exercise programme. Evaluation skills to validate the effectiveness of the business continuity programme.	

When responding to an incident, there are additional skills that may be required in an organization that might be considered outside of the core competencies and skills required of a business continuity professional, these include:

- Emergency evacuation direction.
- Security.
- Welfare and first-aid.
- Crisis management and leadership.
- Information and communication technology (ICT) service continuity and disaster recovery.
- Damage management, asset salvage and equipment restoration.
- External and internal communications to include public relations, brand, and reputation management.

The assessment of competencies and skills should extend to all contractors who work at the organization's site or who provide incident related services.

Awareness of the business continuity programme among an organization's suppliers, customers, contractors, and other interested parties can generate confidence and reassurance and help build reputation. However, as some business continuity information may be sensitive or confidential, the business continuity professional and top management should consider and agree the type of information and level of detail that is appropriate to share with interested parties.

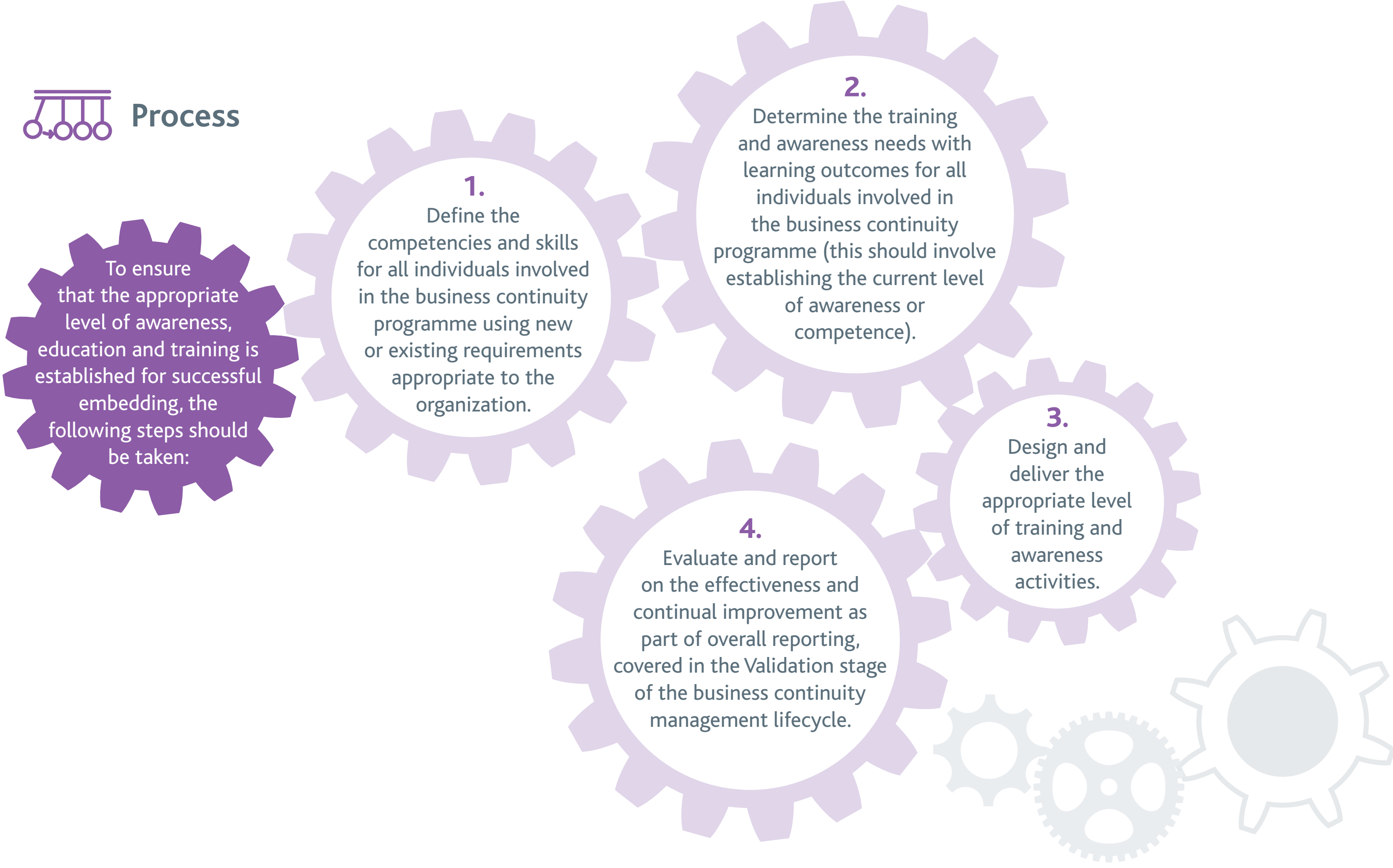
Concepts and Assumptions

Top management should provide appropriate resources to cover all current and ongoing training and awareness activities to ensure the relevant skills and competencies are maintained. For example, annual licence fees for online training, maintenance of professional credentials, and continuing professional development for relevant personnel.

The organization's approach to determining and measuring competencies and skills should be used to define the professional development of those with business continuity roles and responsibilities. For example, an individual may be required to undertake specific training as part of their role, to hold a specific academic qualification, or to hold and maintain a professional credential.

The organization may have existing competency requirements such as a list of skills in a job description. It should also carry out training needs analysis and have learning and development activities in place as part of the human resources or learning and development department. If no such process is in place, the organization should determine the most appropriate methods for ensuring that the business continuity skills and competencies of relevant personnel can be developed, measured, and documented.

Process



To ensure that the appropriate level of awareness, education and training is established for successful embedding, the following steps should be taken:

1. Define the competencies and skills for all individuals involved in the business continuity programme using new or existing requirements appropriate to the organization.

2. Determine the training and awareness needs with learning outcomes for all individuals involved in the business continuity programme (this should involve establishing the current level of awareness or competence).

3. Design and deliver the appropriate level of training and awareness activities.

4. Evaluate and report on the effectiveness and continual improvement as part of overall reporting, covered in the Validation stage of the business continuity management lifecycle.

Methods and Techniques

It may be appropriate to carry out a training needs analysis or gap analysis specifically for the business continuity programme. Alternatively, this could be incorporated into an existing activity as part of a wider learning and development programme in the organization.

Training and awareness

For each role involved in the business continuity programme, the required skills and competencies should be identified. The individuals in these roles can then be assessed based on their current level of competence and any additional training and awareness requirements can be identified. Requirements should be relevant to the individual's role in the business continuity programme and their position in the organization.

> Some organizations use intranet based modular training, meaning personnel only need to complete the sections relevant to them.

The following are additional ways to determine training and awareness needs:

- Reviewing documentation, including existing policies and procedures, incident reports, and accounts of previous business continuity exercises.
- Getting feedback from personnel, including interviews with top management.
- Observation, including reviews of current working practices.
- Internal and external audit reports, including any related non-conformities reported during a certification process where relevant.

> A gap analysis is typically performed at the beginning of a project. This will assess what is currently in place against the set of requirements that are going to be used for implementation.

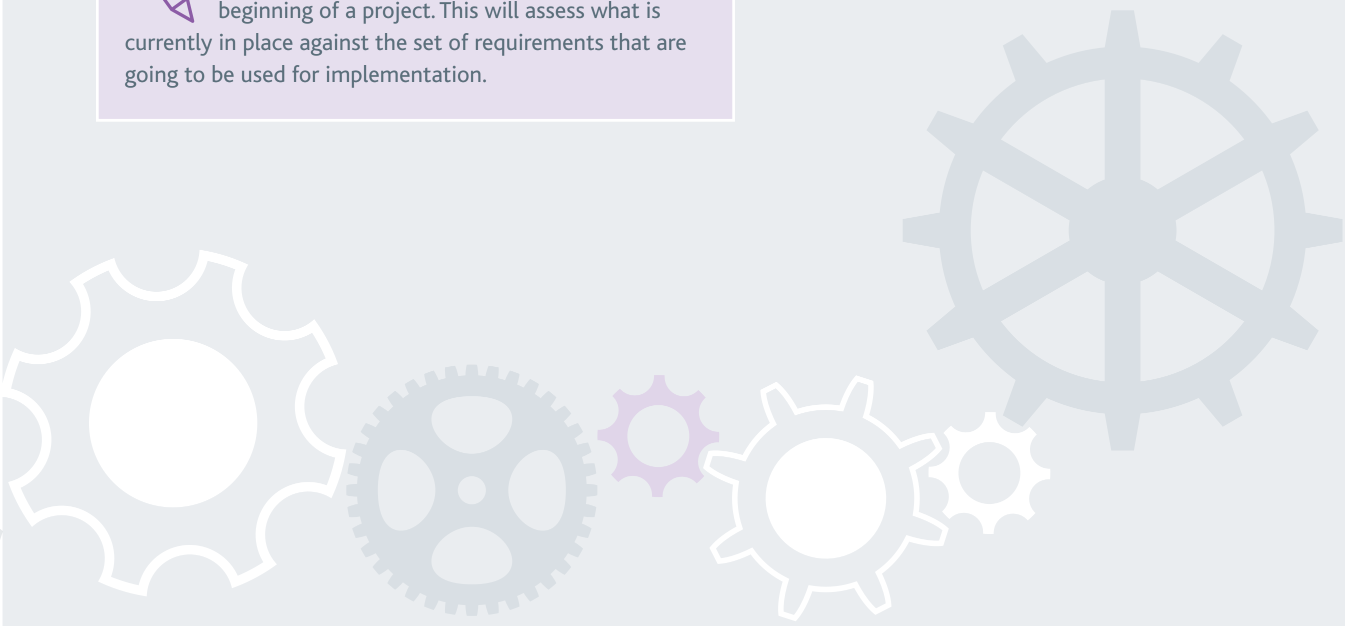
The conclusions reached from the gap analysis or alternate methods may include the following:

- No training or awareness activities are required.
- Some training or awareness is needed.
- Extensive training and awareness is required.
- Recruitment of an experienced person is required.
- Specific skills are required for a short time only and can be provided by an outsourced service provider.

Training and awareness activities should be arranged or revised as appropriate based on the findings of the gap analysis. Types of activities may include:

- Internal training and awareness activities (including exercises where appropriate).
- Self-study options.
- External training or awareness sessions.
- Mentoring (offered to certified members of BCI).
- Conferences, workshops, and seminars.
- Academic courses.

> It is important to document any training undertaken as part of the business continuity programme. This should be reflected in the individual's training record. In some organizations, extra payment or other non-financial recognition is provided for individuals that are part of on-call teams.



Competence reviews following training and awareness activities can be assessed using the following:

- Verbal or written tests.
- Self-evaluation.
- Observation of the individuals or teams.
- Assessment during continued coaching or mentoring.
- Participation in exercises designed to evaluate competence.
- Group coaching.
- Recognition of academic qualifications.
- Recognition of professional credentials and continuing professional development activities, for example, the BCI's CPD programme.

Examples of competence records include:

- Personnel training records, including attendance at courses, seminars, and conferences.
- Education and academic qualifications.
- Previous relevant experience.
- Skills or competencies demonstrated during the initial interview.
- Professional qualifications.
- Personnel appraisals.

The training and awareness activities should consider:

- Changes to business processes that affect organizational priorities or operations.
- Legislation or regulation affecting the business continuity programme.
- Change in actual or perceived threats and vulnerabilities.
- Requirements of interested parties concerning the availability of information and services, including compliance with relevant standards.

Examples of information resources for training and awareness campaigns include:

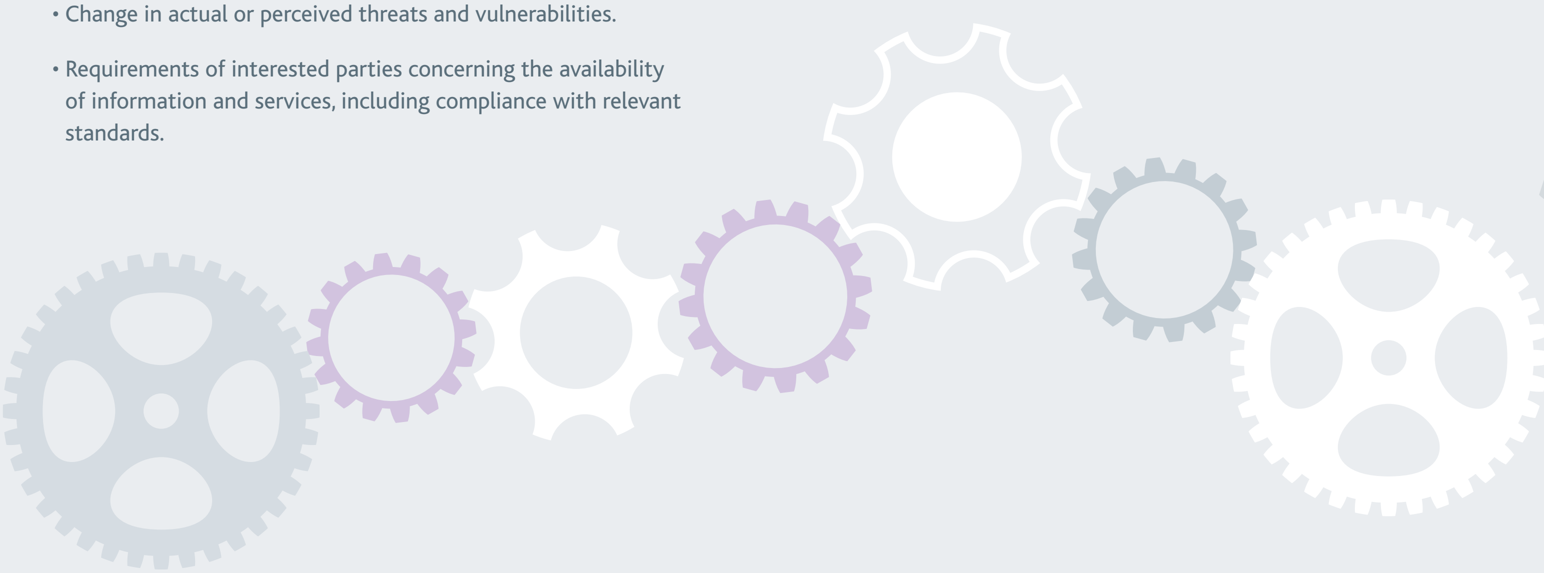
- Business continuity and resilience related websites, blogs, and social media groups.
- Books, journals, and other industry publications.
- Conferences, workshops, webinars, and seminars.
- Regional forums and working groups.
- Industry sector working groups.

The content and delivery of any communications aimed at raising the levels of awareness of the business continuity programme should be carefully considered. Coordination and collaboration with other departments and disciplines is recommended to ensure a consistent message is delivered and resources are not wasted. For example, a combined security, business continuity, and health and safety briefing may be more informative and effective than separate briefings.

Communication should be brief and relevant but should provide information on how to access further guidance.

Suitable topics for awareness raising communications include:

- A report based on a recent exercise which outlines the scenario and learning points.
- An ICT recovery test at alternate facilities which might include a photograph and participants' comments.
- A commentary on a recent incident which affected the organization.
- Examples of real-life incidents that are relevant to business continuity.



Outcomes and Review

The outcomes of embedding business continuity are:

- An improvement in the level of organizational resilience, measured by a reduction in the impact and frequency of incidents or an overall improvement in response.

- A reduction in costs associated with incidents.

- Feedback from interested parties, especially personnel and customers, indicating greater confidence in the organization's ability to handle disruptions effectively.

Outcomes of embedding business continuity can be difficult to quantify. However, it is recommended that performance measures are identified and used.

Examples of performance measures include:

- Percentage of annual review completion.

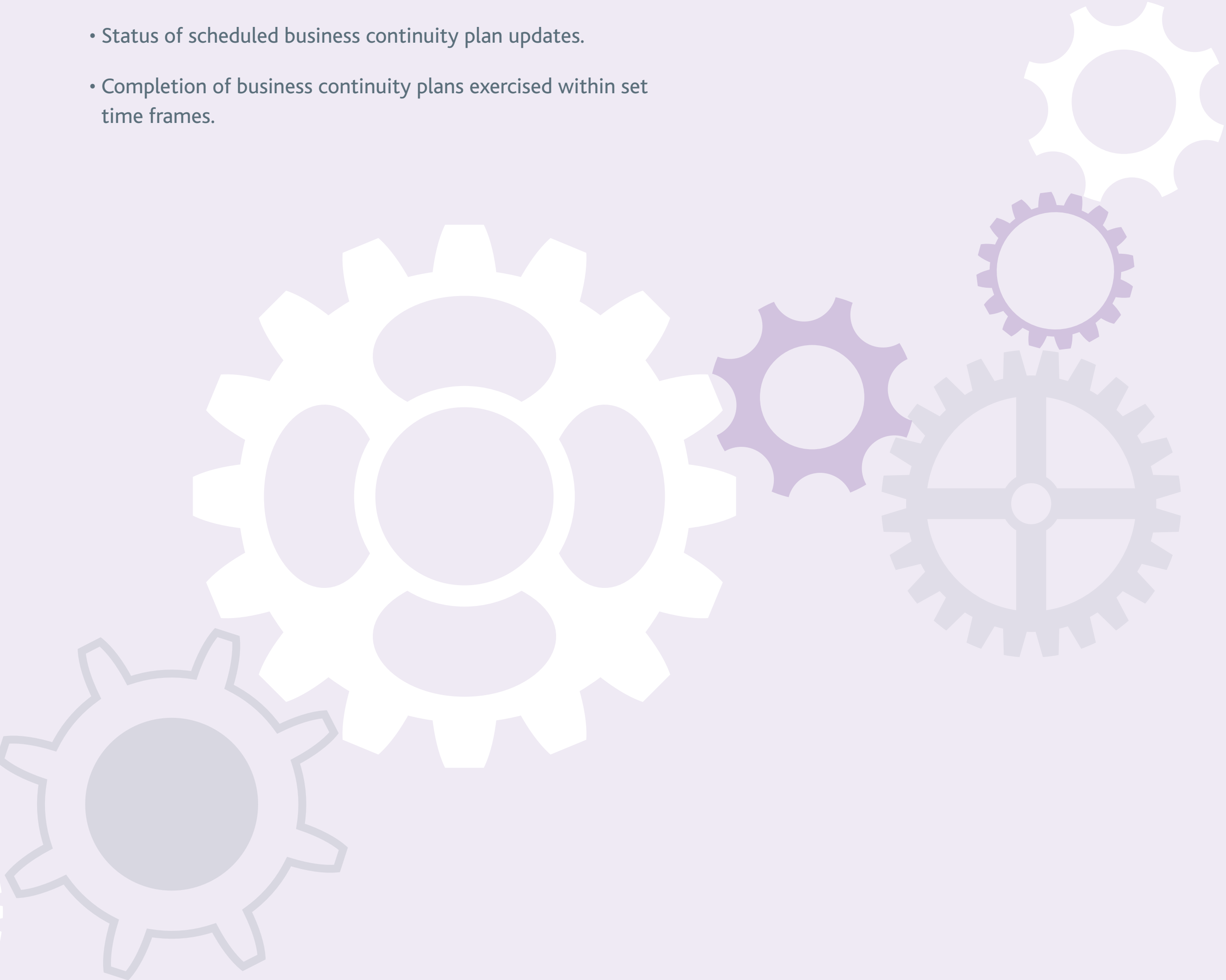
- Status of BIA review, by department.

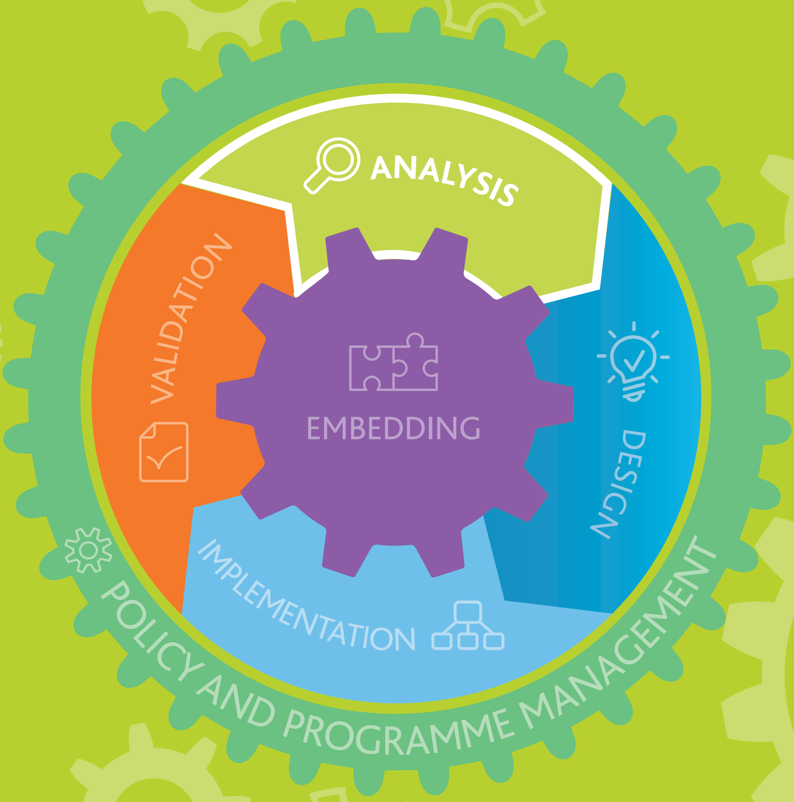
- Status of scheduled business continuity plan updates.

- Completion of business continuity plans exercised within set time frames.

The goal of embedding business continuity is to integrate it into business as usual processes and procedures. Business continuity is a key capability, and one of the management disciplines which needs to be integrated, coordinated, and aligned with other disciplines to build effective organizational resilience. It is essential for the business continuity professional to collaborate with individuals from other associated disciplines at every stage of the business continuity management lifecycle. Collaboration is particularly important in this stage of the lifecycle where there are many opportunities to communicate the benefits of a coordinated approach towards assessing and developing capabilities to build organizational resilience.

The approach to embedding business continuity should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.




ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
EMBEDDING
POLICY AND PROGRAMME MANAGEMENT

BCI Professional Practices

PP3

Analysis

Analysis is the Professional Practice within the business continuity management lifecycle that reviews and assesses an organization to identify its objectives, how it functions and the constraints of its operating environment.

Introduction

The main technique used for the analysis of an organization for business continuity purposes is the business impact analysis (BIA). The business continuity professional uses the BIA to determine the organization's business continuity requirements. There are four types of BIA:

- **An initial BIA.**
- **A product and service BIA.**
- **A process BIA.**
- **An activity BIA.**

There are many approaches to undertaking a BIA. Organizations do not have to undertake all four BIA types. A combination of the above is sometimes the most appropriate approach depending on the size, complexity, and type of the organization, and the scope of the business continuity programme.

The BIA identifies business continuity requirements, providing information to determine the most appropriate business continuity solutions. The BIA identifies the urgency of each activity undertaken by the organization by assessing the impact over time caused by any potential or actual disruption to this activity on the delivery of products and services.

Business continuity requirements can be defined as the time frames, resources, and capabilities necessary to continue to deliver the prioritised products, services, processes, and activities following a disruption.

A risk assessment should be undertaken at this stage so that mitigation measures can then be identified in the Design stage of the business continuity management lifecycle.

A thorough understanding of the organization, using these analysis techniques can often highlight inefficiencies and areas for improvement to top management. This may provide opportunities for collaboration between related management disciplines to contribute to, and build resilience. It is therefore important to identify and invite the most appropriate individuals to provide input into the BIAs, which may not be limited to individuals directly involved in the process or activities themselves.

Business Impact Analysis

General Principles

The different types of BIA provide progressively greater levels of detail and understanding about the organization.
The different types of BIA that can be used are:

Initial BIA:

To provide a high-level analysis that can be used to develop a framework for the more detailed BIAs. It can also be used to clarify the scope of the business continuity programme (This is typically only required the first time an organization conducts a BIA).

Product and Service BIA:

To identify and prioritise products and services and determine the organization's business continuity requirements at a strategic level.

Process BIA:

To determine the process or processes required for the delivery of the organization's prioritised products and services.

Activity BIA:

To identify and prioritise the activities that deliver the most urgent products and services, and to determine the resources required for the continuity of these activities.

Depending on its size, complexity and type, an organization may choose to combine these different types of BIAs.

Concepts and Assumptions

The BIA is not a one-time or single stage activity. Initially, it can help clarify the scope of the business continuity programme, after which it becomes an integral part of the ongoing lifecycle to confirm business continuity requirements, leading to the determination and selection of business continuity solutions. The BIA can be used to ask top management questions which relate to the organization's objectives and priorities, relating to products and services.

The BIA considers both the products and services that an organization delivers as well as the processes, activities and dependencies that ensure the delivery of these products and services.

- **Products and services** are defined as "beneficial outcomes provided by an organization to its customers, recipients and interested parties." (Source: ISO 22301:2012)
- **A process** is described as "a set of interrelated or interacting activities which transforms inputs to outputs." (Source: ISO 22301:2012) A process may be divided into a number of activities. For example, a process could be manufacturing (from goods receipt to delivery), managing investment, or collecting waste.
- **An activity** is defined as one or more tasks undertaken by, or for an organization, that produces or supports the delivery of one or more products and services. For example, performing quality control, undertaking home care visits, raising invoices, and answering calls through a help desk.

The level of detail to which activities need to be analysed may depend on their complexity and whether their maximum tolerable period of disruption (MTPD), maximum acceptable outage (MAO), and recovery time objectives (RTOs) can be identified. Similar activities can be grouped together.

The terms 'maximum tolerable period of disruption' or 'maximum acceptable outage' are used to describe "the time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable." (Source: ISO 22301:2012)

The word 'unacceptable' in this context means the point in time when the organization will fail or is unable to continue its prioritised activities.

The adverse impacts on the organization may be of a financial, reputational, legal, or regulatory nature, or may relate to a failure of the organization to meet its strategic objectives.

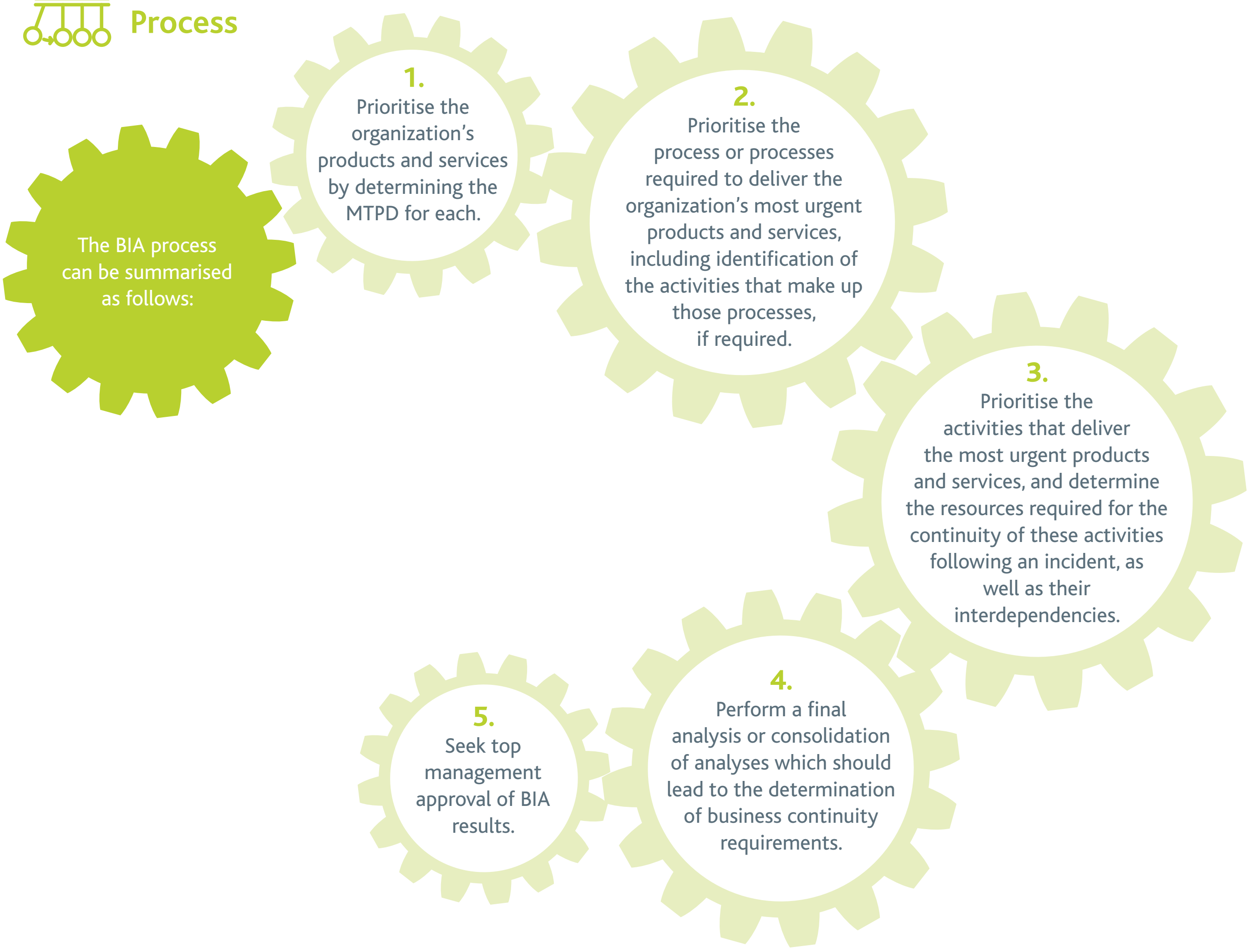
The 'recovery time objective' is defined as "the period of time following an incident within which a product or service must be resumed, or activity must be resumed, or resources must be recovered." (Source: ISO 22301:2012)

The terminology used in the BIA by an organization is not as important as understanding when the disruption will result in unacceptable consequences. The words 'critical', 'mission critical' and 'key' are often used to describe the products and services, processes, activities, and resources required following an incident. These words are often understood as meaning 'important', however this can lead to misunderstandings and exaggerations when collecting information for the BIA. It could also result in an incorrect assumption that plans are not required for 'non-critical' activities or 'non-key' personnel. It is therefore recommended that these terms are replaced with 'prioritised activities', which is defined as "activities to which priority must be given following an incident in order to mitigate impacts." (Source ISO 22301:2012)

Everyone involved in performing an activity (personnel, contractors, volunteers, etc.) is important at some point, however the focus should be on the personnel whose absence would cause immediate or rapid unacceptable impacts.

It is possible that in some organizations, information will be market or industry sensitive and should not be visible to the business continuity professional. Not having this information should not stop the BIA being undertaken but could affect the accuracy of the end results and therefore should be noted in the conclusions.

Process



The BIA process can be summarised as follows:

1. Prioritise the organization's products and services by determining the MTPD for each.

2. Prioritise the process or processes required to deliver the organization's most urgent products and services, including identification of the activities that make up those processes, if required.

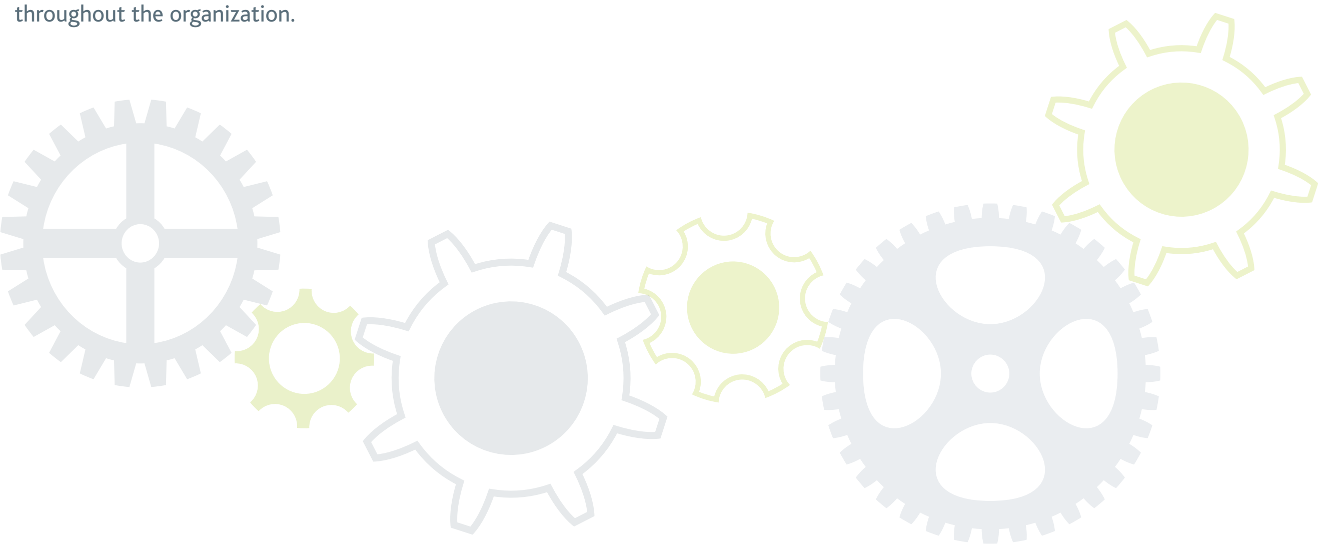
3. Prioritise the activities that deliver the most urgent products and services, and determine the resources required for the continuity of these activities following an incident, as well as their interdependencies.

4. Perform a final analysis or consolidation of analyses which should lead to the determination of business continuity requirements.

5. Seek top management approval of BIA results.

When conducting a BIA, the following points should be considered:

- The scope of the business continuity programme can be clarified, or may need to be modified following the initial BIA findings.
- Determining impacts over time should demonstrate to top management how quickly the organization needs to respond to a disruption.
- A consistent approach to performing the BIA should be used throughout the organization.
- The method used should be robust enough to ensure that the information is collected consistently and impartially. This ensures that individuals do not over or under estimate the urgency of their activities.
- Only relevant information to be used in the analysis should be collected.
- Impacts do not need to be precisely determined and can be estimated.



Methods and Techniques

Methods used to perform the business impact analysis vary from one industry sector to another, as well as from one organization to another.

Depending on its size, complexity and type, an organization may choose to combine the different types of BIAs. Examples of these combinations include:

- Combining product and service, and process BIAs.
- Conducting separate product and service, and process BIAs.
- Conducting only a process BIA.

Whichever approach is taken, the information is identified and recorded in the same way.

> Combining the different types of analysis can be a more efficient way to achieve an organization-wide view of key products, services, and processes. However, a combined approach can make the BIA process complex and challenging, therefore it is important to identify the most appropriate BIA approach for the organization.

Methods and techniques used to collect the BIA information include:

- Workshops.
- Questionnaires.
- Interviews.

Workshops can be used to collect information from individuals and teams in person, and provide an opportunity to raise awareness and embed business continuity. Interdependencies can be identified, issues can be raised and solutions explored. This method can provide information in a shorter time frame than other methods.

Questionnaires can be used to collect information from individuals or teams by paper or electronically. They can be designed to gather very detailed information and can generate a large amount of information. Using software to collect and analyse this information electronically is a useful method for medium and large organizations.

Interviews can provide high quality information but are time consuming and information can vary in detail. The business continuity professional may perform interviews to facilitate discussion regarding business as usual operations, resource needs, obligations, and possible impacts if an incident were to affect the activity's capability to deliver processes, and products or services.

To prepare workshops, questionnaires or interviews, the business continuity professional should review all relevant documents. Documents can provide additional information to assist with performing the BIA.

Examples of documents to review as part of the BIA include:

- Existing BIA information, where relevant.
- The organization's strategic plan.
- Annual reports.
- Departmental or business unit plans.
- Legal or regulatory requirements.
- Service level agreements.
- Risk assessments or risk registers.

There are a variety of software products available which are designed to assist with the BIA that may be useful but are not essential. The key benefits of using a software tool include:

- Ease of collating results.
- Storage of information.
- Automated reporting of results.

Using software does not remove the need for workshops, questionnaires, and interviews with relevant personnel.

Evaluating impacts to determine the MTPD and RTO

The BIA information collected will include identification of all products and services, processes, and activities, which are prioritised by determining the maximum tolerable period of disruption (MTPD).

The MTPD has been reached when acceptable levels of damage have been exceeded and the failure of the organization is imminent.

For example:

- Customers move to a competitor and the organization cannot attract new customers.
- The reputation of the organization is so badly damaged, through a delivery, legal or regulatory failure, that interested parties no longer want to be associated with it.
- The organization is, or will soon be bankrupt due to fines, penalties, a loss of income, or expenditure of financial reserves.
- External pressure from interested parties forces a major change in the organization's leadership or strategy.

The main factors that should be considered when estimating the MTPD of a disruption to product or service delivery are:

- Damage to financial value or viability (short or long-term).
- Damage to reputation or interested party confidence.
- Breach of legal or regulatory obligations.
- Failure to meet the strategic objectives of the organization.

In the BIA, no attempt is made to quantify the impacts to interested parties caused by the disruption. Instead, it assesses the impact that could be imposed on the organization in response, for example financial penalties or bad publicity.

It is important to consider the time frame when determining the impact of a disruption on product and service delivery. Top management should decide what is unacceptable to the organization based on the impact over time.

For some products and services in some industry sectors, a few minutes of disruption may have no impact at all, a few hours could be tolerable, but longer than a week could mean failure of the business.

Examples of impacts over time are as follows:

- Breaches of legal or regulatory requirements, for example, 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.
- Environmental damage, for example, chemical leaks due to maintenance delays or the inability of a response organization to mobilise clean-up operations, resulting in bad publicity and financial penalties.
- Delays to major projects or a new product launch, for example, delay to a development project and loss of expected revenue.
- Opportunities for competitors, for example, a government department failing to deliver a service, resulting in a decision to outsource that service to a private company.
- Health implications from a service failure, resulting in bad publicity and financial penalties.

Changes in demand for products and services may affect the MTPD and therefore make it difficult to determine. In such instances, the BIA should focus on a product or service disruption during vulnerable time frames. For example, fluctuation to delivery times due to seasonal change in demand, changes to regulatory requirements, or limited resource availability.

A one-off contract with an outsourced service provider including significant time penalties may reduce the MTPD within the organization for the period of that contract.

The duration or lead time of the process or activity delivering the product or service may be a significant consideration in the MTPD estimate. For processes or activities that take significant time, 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 process or activity needs to be repeated.

For example, a laboratory experiment may need to be restarted from scratch if disrupted, however a manufacturing process may be able to resume at several different points.

The MTPD can also be difficult to determine if the outcome of the disruption is uncertain.

Consider the following examples:

- The impacts of a delay in response time at an emergency control centre will depend on whether an emergency occurs during the time of disruption.
- The impact of a disruption to a bank's share trading activities can be unpredictable as market prices can rise and fall during the period of disruption.

The RTO should always be less than the MTPD. The RTO for a specific

The MTPD is usually expressed in terms of minutes, hours, days, weeks, and months.

Although the MTPD is an important planning concept, an aim of business continuity is to design and implement plans to ensure continuity of the organization's products and services **before the MTPD is reached.** Use the BIA to identify recovery time objectives (RTOs) for the prioritised products, services, activities and resources as this will enable the organization to develop continuity solutions and plans that avoid reaching the MTPD.

resource for example a software system, is the shortest RTO of the various activities that require that resource, unless an alternate process or manual workaround is viable without the resource. The BIA establishes the RTO as part of the business continuity requirements, however the most appropriate solution needed to achieve the RTO is determined in the Design stage of the business continuity management lifecycle. As a result, the RTO may need to be revised based on the agreed solution and the resources available to the organization.

The development of the business continuity requirements should consider more than the recovery time frame as described by the RTO. The BIA should also determine a minimum level of capability at defined points in time. One common term used to describe this capability is the 'minimum business continuity objective' (MBCO).

Where activities and resources support multiple products and services, the shortest time requirement of these products and services is the recovery time objective (RTO).

"MBCO is the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption." (Source: ISO 22301:2012)

The minimum level defined may be less than, the same as, or higher than business as usual levels, and the product or service may be delivered using a different approach. The MBCO should be achieved at a specific time after a disruption. It may be appropriate to set several MBCOs for different times after a disruption, and for each product group. Where MBCOs rely on outsourced service providers, the objectives should consider service level agreements and any legal or regulatory requirements.

Outcomes and Review

The overall outcome of performing the BIAs at each level is to determine the business continuity requirements, enabling the organization to build capability to deliver its products and services at acceptable predefined levels following a disruption.

The BIAs should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

The Initial BIA

An initial BIA defines the organization in terms of products and services, and processes. It is a high level analysis that can be used to develop a framework for the more detailed BIAs and clarify the scope of the business continuity programme.

It is usually required the first time an organization conducts a BIA. However, it can be useful to repeat the initial BIA following a substantial change in the organization or if several years have passed since the last BIA.

The initial BIA supports the requirement for continual improvement of the business continuity management system or programme, and is a technique which continually enhances and refines the results of the BIA until it satisfies the organization's objectives.

The minimum objective of an initial BIA is to identify the products and services, and processes within the organizational structure. MTPDs can be estimated at a later date. To ensure successful implementation of the business continuity programme, timely delivery of an initial BIA may be more important than delivery of a detailed BIA, if it is providing value to the organization.

Process

The process for developing an initial BIA should include:

1. Deciding the terms of reference and draft scope of the initial BIA.

2. Identifying products and services which can be grouped to simplify the information collection and analysis.

3. Agreeing the impacts to be considered, for example, financial and reputational.

4. Agreeing and documenting the impacts over time relating to delivery failure of products and services.

5. Estimating the MTPD for each product and service.

6. Identifying the processes that deliver the products or services. This should consider organization-wide and departmental processes.

7. Identifying owners for each process, **for example, subject matter experts to provide information about the processes.**

8. Identifying how and when a disruption to the process could result in damage to the delivery of products and services.

9. Presenting the findings to top management for review and approval.

The Initial BIA should consider specific impacts which may not be fully appreciated by top management, including:

- Backlogs and capacity issues.
- The duration or lead time of the process.
- Any non-standard or unique activities which are difficult to recover and could unexpectedly affect the continuity of the process.

Outcomes and Review

The outcomes of an initial BIA are:

- A list of the of the organization's products and services (grouped together where appropriate).
- The impacts over time relating to the delivery failure of products and services.
- Estimated MTPDs for products and services.
- A list of processes and owners that contribute to the delivery of the products and services.
- A breakdown of internal and external activity dependencies.
- A list of products, services, processes, and activities that have been excluded, along with the justification for the exclusion.

The Product and Service BIA

In a product and service BIA, the organization identifies and prioritises its products and services. It may also be used to review and clarify the scope of the business continuity programme in terms of products and services.

A product and service BIA can be used to determine the impact of a disruption before implementing a significant organizational change.

The following are examples of significant organizational changes:

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

Using the product and service BIA should enable the organization to take advantage of any changes to improve its business continuity capability and build organizational resilience.

Process

The product and service BIA process should include:

1. Reassessing the scope of the business continuity programme. This includes reviewing any exclusions and considering the inclusion of new products or services.

2. Collecting the information necessary to perform the product and service BIA.

3. Understanding the potential impact of significant developments within the organization or the operating environment.

4. Assigning products and services to groups for analysis purposes.

5. Reviewing impacts as well as the criteria to determine the MBCO.

6. Documenting the impacts of a product or service group delivery failure.

7. Estimating the MTPD for each product or service group.

8. Obtaining top management sign-off of the product and service BIA results.

9. Proceeding to the process BIA.

Outcomes and Review

The outcomes of a product and service BIA are:

- Clarification or modification of the scope of the business continuity programme.
- A list of the organization's prioritised products and services.
- Evaluation of impacts over time.

The Process BIA

A process BIA determines the process or processes required for the delivery of the organization's products and services and assesses the impact of a process disruption on the delivery of these products and services.

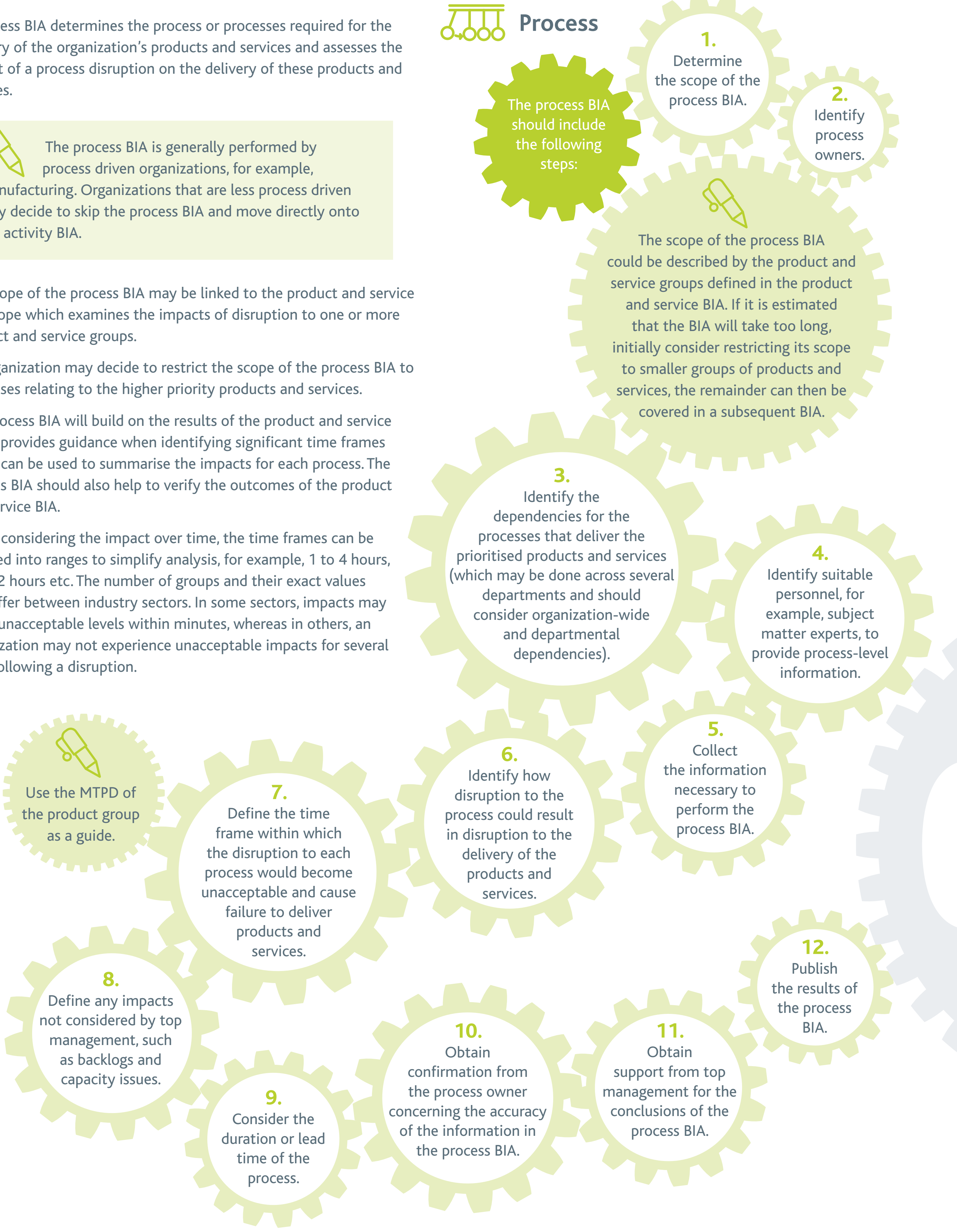
The process BIA is generally performed by process driven organizations, for example, manufacturing. Organizations that are less process driven may decide to skip the process BIA and move directly onto the activity BIA.

The scope of the process BIA may be linked to the product and service BIA scope which examines the impacts of disruption to one or more product and service groups.

An organization may decide to restrict the scope of the process BIA to processes relating to the higher priority products and services.

The process BIA will build on the results of the product and service BIA. It provides guidance when identifying significant time frames which can be used to summarise the impacts for each process. The process BIA should also help to verify the outcomes of the product and service BIA.

When considering the impact over time, the time frames can be grouped into ranges to simplify analysis, for example, 1 to 4 hours, 4 to 12 hours etc. The number of groups and their exact values will differ between industry sectors. In some sectors, impacts may reach unacceptable levels within minutes, whereas in others, an organization may not experience unacceptable impacts for several days following a disruption.



Process

The process BIA should include the following steps:

1. Determine the scope of the process BIA.

2. Identify process owners.

The scope of the process BIA could be described by the product and service groups defined in the product and service BIA. If it is estimated that the BIA will take too long, initially consider restricting its scope to smaller groups of products and services, the remainder can then be covered in a subsequent BIA.

3. Identify the dependencies for the processes that deliver the prioritised products and services (which may be done across several departments and should consider organization-wide and departmental dependencies).

4. Identify suitable personnel, for example, subject matter experts, to provide process-level information.

5. Collect the information necessary to perform the process BIA.

6. Identify how disruption to the process could result in disruption to the delivery of the products and services.

7. Define the time frame within which the disruption to each process would become unacceptable and cause failure to deliver products and services.

Use the MTPD of the product group as a guide.

8. Define any impacts not considered by top management, such as backlogs and capacity issues.

9. Consider the duration or lead time of the process.

10. Obtain confirmation from the process owner concerning the accuracy of the information in the process BIA.

11. Obtain support from top management for the conclusions of the process BIA.

12. Publish 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 business continuity programme.
- Identification of the interdependencies of the processes.
- The MTPD, RTO, and RPO where appropriate 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.

The Activity BIA

The activity BIA identifies and prioritises the activities which contribute to the identified process or processes that directly deliver the products and services.

The activity BIA is where the organization collects detailed information about the resources required to continue activities which support the organization's strategic objectives.

Dependencies on external suppliers and outsourced service providers can be determined at this level when defining resource requirements. It is usually appropriate to identify the common dependencies, for example, utilities (power, water, telecommunications etc.) at the activity level as they affect most processes.

The following information should be collected during the activity BIA:

- The processes that the activity supports (where appropriate).
- The operational methods for the activity.
- The duration or lead time of the activity.
- Fluctuations in demand or peak operating times.
- Factors not already discovered that may affect the determination of business continuity requirements, for example, backlogs, or legal and regulatory requirements of this activity.

Detailed information regarding the resources required to continue activities fall into the following categories:

- "People.
- Information and data.
- Buildings, work environment and associated utilities.
- Facilities, equipment, and consumables.
- ICT systems.
- Transportation.
- Finance.
- Partners and suppliers" (Source: ISO 22301:2012).

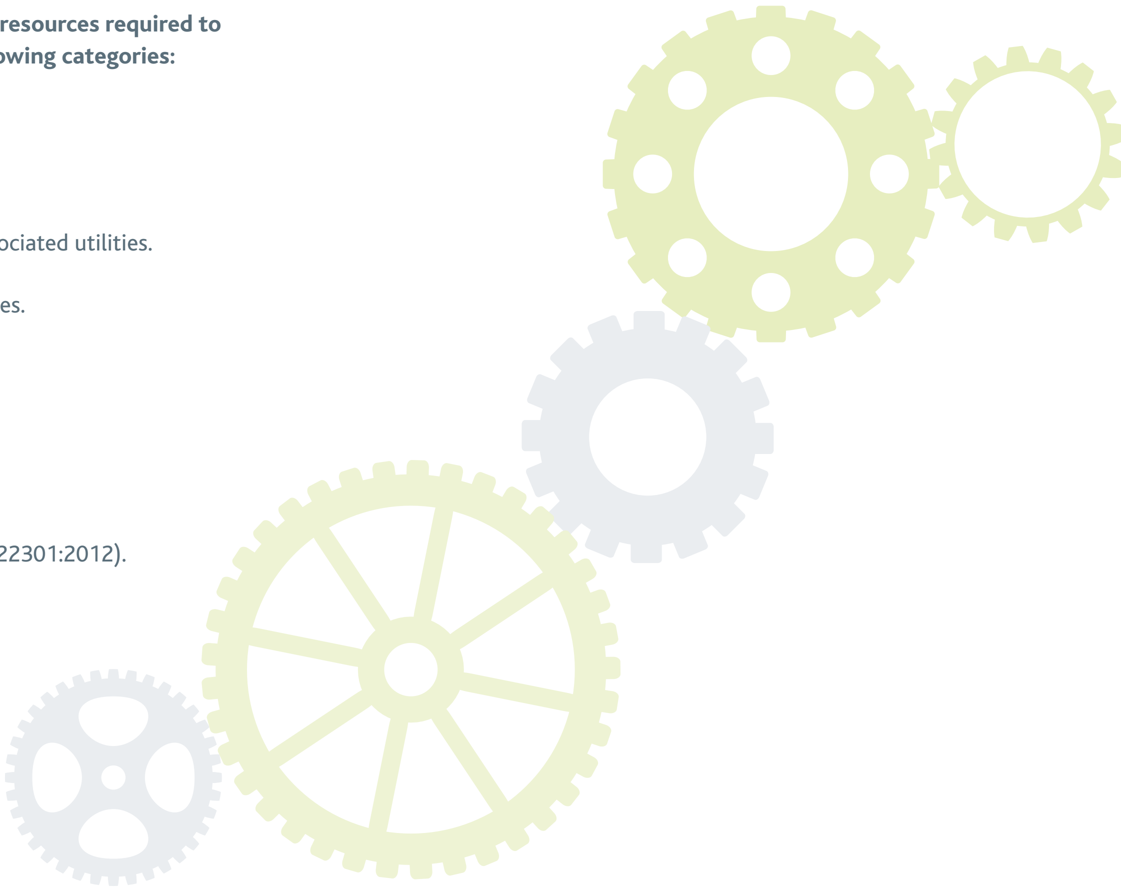
It is often assumed that the resources required after a disruption will be less than those used during business as usual, at least for a certain duration. However, in some cases, the quantity of resources in the early stages may need to be higher than usual to deal with backlogs.

For example, in a call-centre, additional personnel may be needed to deal with increased call volumes following an incident, and supporting ICT systems may need to have a higher capacity to cope with an additional number of users.

Additionally, the organization should determine appropriate recovery point objectives (RPOs) to understand how data loss may affect the recovery, as well as the availability of hard copy records (where appropriate).

"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'." (Source: ISO 22301:2012)

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 time frames. The RPO for a specific information or data set is the shortest RPO required by all users.



Process

The activity BIA process should involve the following:

1. Identify and prioritise the activities which contribute to the process or processes that deliver the prioritised products and services.

2. Collect the information necessary to perform the activity BIA, including:

- An understanding of activity details and interdependency information.
- An understanding of activity specific RTOs.
- A breakdown of the resources required to maintain the activities at an agreed level and within the MTPD and RTO.

3. Consider any additional activities that may be created during a disruption, including the need to clear backlogs.

4. Obtain approval by the activity owner to confirm the accuracy of the information.

5. Obtain the support of top management for the conclusions.

Outcomes and Review

The outcomes of an activity BIA are:

- A list of activities that contribute towards the processes needed to deliver products and services.
- The MTPD and RTO and the justification for each activity, which should determine the time frame of the solutions for each activity.
- A breakdown of activity dependencies, both internal and external.
- An understanding of the resources required to provide the agreed service levels.
- The RPO for data and hard copy records.
- Documentation of the internal and external interdependencies for the prioritised activities.

Risk and Threat Assessment

Business continuity management is defined as "a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause…" (Source: ISO 22301:2012)

The BIA evaluates the impacts over time relating to the delivery failure of products and services following a disruption and determines the business continuity requirements.

The business continuity professional uses risk assessment techniques to identify unacceptable levels of risk and single points of failure. Risk assessment information and methods to evaluate the threat of disruption enable effective business continuity solutions and mitigation measures to be designed.

General Principles

During the Analysis stage, the BIA is typically conducted first so that the risk and threat assessment and mitigation measures can focus on the organization's prioritised activities and supporting resources. This can maximise the benefit of any investment, and reduce the frequency or impact of disruptions.

A risk is defined as "an effect of uncertainty on objectives" (Source: ISO Guide 73).

A threat is defined as "a potential cause of an unwanted incident, which can result in harm to individuals, a system or an organization" (Source: ISO 22300:2012).

Concepts and Assumptions

If an organization has an established risk management function, information may already be available that will support the organization's business continuity programme. Business continuity professionals should collaborate with risk professionals in the organization where appropriate. Having an existing risk management function is not required for successful risk assessment as part of an effective business continuity programme.

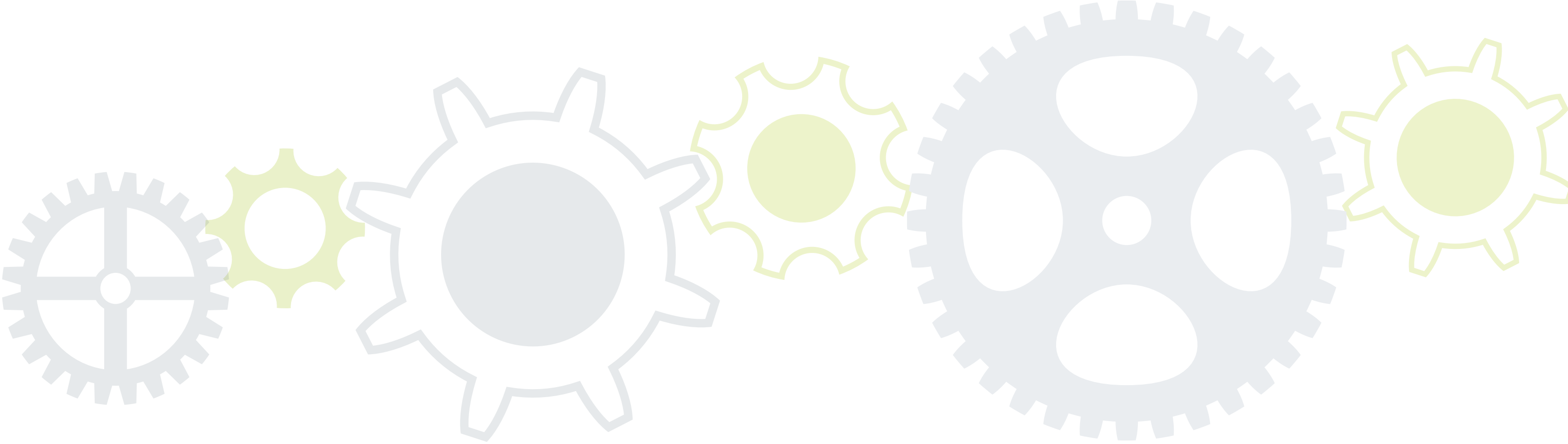
Risk assessment typically involves methods to identify, analyse and evaluate a range of risks relevant to the organization. It uses a formula based on probability and impact to calculate a risk score.

A risk assessment is defined as "an overall process of risk identification, risk analysis and risk evaluation." (Source: ISO Guide 73)

Risk assessment methods can be effective when analysing known and anticipated risks, however, the business continuity professional should be aware of some limitations to risk assessment techniques when they are being used to evaluate threats and the causes of disruptions.

Significant disruptions typically occur infrequently, meaning estimations based on the probability of a threat occurring are based on limited data sets and historic information, and the time frame under consideration.

Risk assessment methods typically consider short time frames relevant to the organizational planning process. Disruptions such as a volcanic eruption or a 1 in 100 year flood which are low frequency high impact events may not be taken into consideration.



Risk assessment as part of the business continuity programme considers the risk of disruption due to various threats. These Good Practice Guidelines refer to this process as a risk and threat assessment.

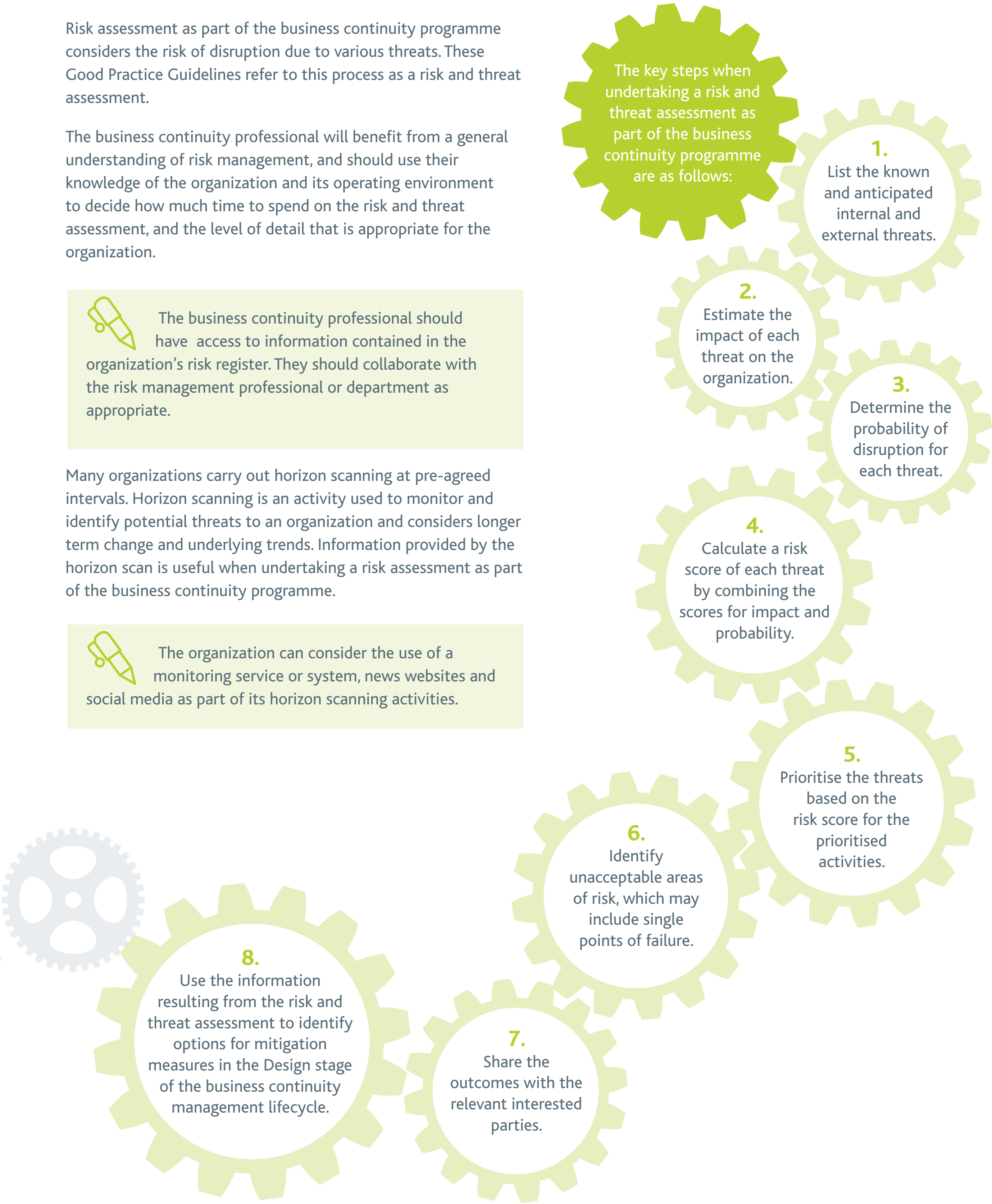
The business continuity professional will benefit from a general understanding of risk management, and should use their knowledge of the organization and its operating environment to decide how much time to spend on the risk and threat assessment, and the level of detail that is appropriate for the organization.

> The business continuity professional should have access to information contained in the organization's risk register. They should collaborate with the risk management professional or department as appropriate.

Many organizations carry out horizon scanning at pre-agreed intervals. Horizon scanning is an activity used to monitor and identify potential threats to an organization and considers longer term change and underlying trends. Information provided by the horizon scan is useful when undertaking a risk assessment as part of the business continuity programme.

> The organization can consider the use of a monitoring service or system, news websites and social media as part of its horizon scanning activities.

Process



The key steps when undertaking a risk and threat assessment as part of the business continuity programme are as follows:

1. List the known and anticipated internal and external threats.
2. Estimate the impact of each threat on the organization.
3. Determine the probability of disruption for each threat.
4. Calculate a risk score of each threat by combining the scores for impact and probability.
5. Prioritise the threats based on the risk score for the prioritised activities.
6. Identify unacceptable areas of risk, which may include single points of failure.
7. Share the outcomes with the relevant interested parties.
8. Use the information resulting from the risk and threat assessment to identify options for mitigation measures in the Design stage of the business continuity management lifecycle.

See tables 3 and 4 for examples of a risk assessment matrix.

The tables below are examples of a simple 3x3 risk assessment matrix. Many organizations use more detailed matrices (4x4 or 5x5), which may produce different risk score results, for example, Extreme, High, Medium, Low.

Table 3.

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 $1 M cost/lost revenue	National damage to reputation/customer or community support	Potential for irreversible injuries/ fatalities
2-Moderate	2 to 5 days	$100k to $1 M 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 support	Potential for minor injuries (time off work)

Table 4.

Probability of Disruption	3 - Likely	2 - Possible	1 - Unlikely
3-Major	Frequent occurrence/At least once in 3 year period	Infrequent occurrence/ Once in 10 year period	Exceptional occurrence/ Once in 30 year period
Combining the probability and impact scores for each threat produces a risk score (High/Medium/Low)			
3-Major Impact	High	High	Medium
2-Moderate Impact	High	Medium	Low
1-Minor Impact	Medium	Low	Low

Methods and Techniques

If an organization has an established risk management function, consider collaborating with the risk professionals to adapt the pre-existing risk assessment methods for the business continuity programme.

Risk assessment information may include information about the frequency and impact of past disruptions. A risk matrix may be available where impact ratings are grouped into impact categories that relate to the organization, for example, financial, environmental, legal and reputational. Care should be taken to ensure that the impact ratings are appropriate to describe the consequences of disruptions.

Organizations may find the following sources provide useful information to carry out a risk assessment:

- Risks and threats identified during the BIA process.
- Risks and threats 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 location.
- Information or reports relating to threats and past disruptions.
- Horizon scanning activities.
- Publicly available records about known local hazards.

Outcomes and Review

The outcomes from the risk and threat assessment as part of the business continuity programme are:

- An awareness of the range of potential threats that could disrupt the organization’s activities.
- A prioritised list of the threats based on the risk of disruption to the organization’s activities.
- Identification of any unacceptable risks and single points of failure.
- Identification of potential options for measures to reduce the frequency or scale of impact of the prioritised threats.

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

Final Analysis and Consolidation

Following all BIAs, it is good practice to perform a final analysis to consolidate the information collected and finalise the business continuity requirements.

This final analysis should “...challenge and check the information to ensure that it is:

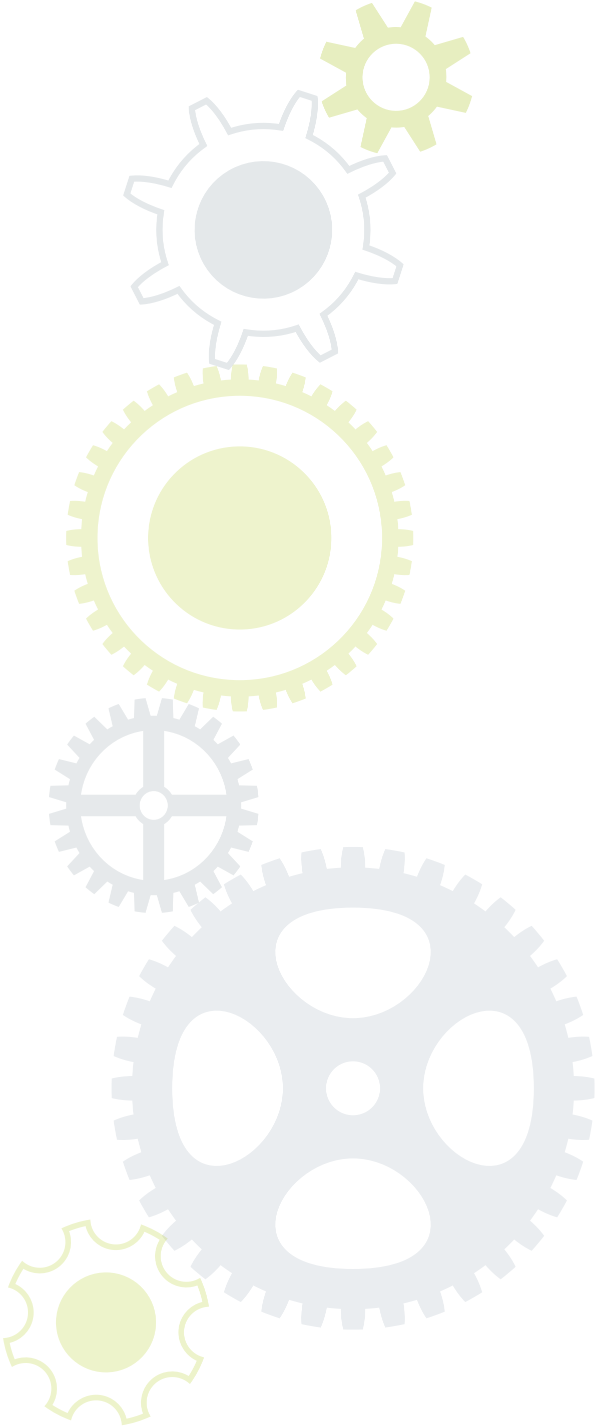
- Correct, accurate and reliable.
- Credible, believable, and reasonable.
- Consistent, clear, and repeatable.
- Current, up-to-date, and available in a timely manner.
- Complete and comprehensive.” (Source: ISO/TS 22317:2015)

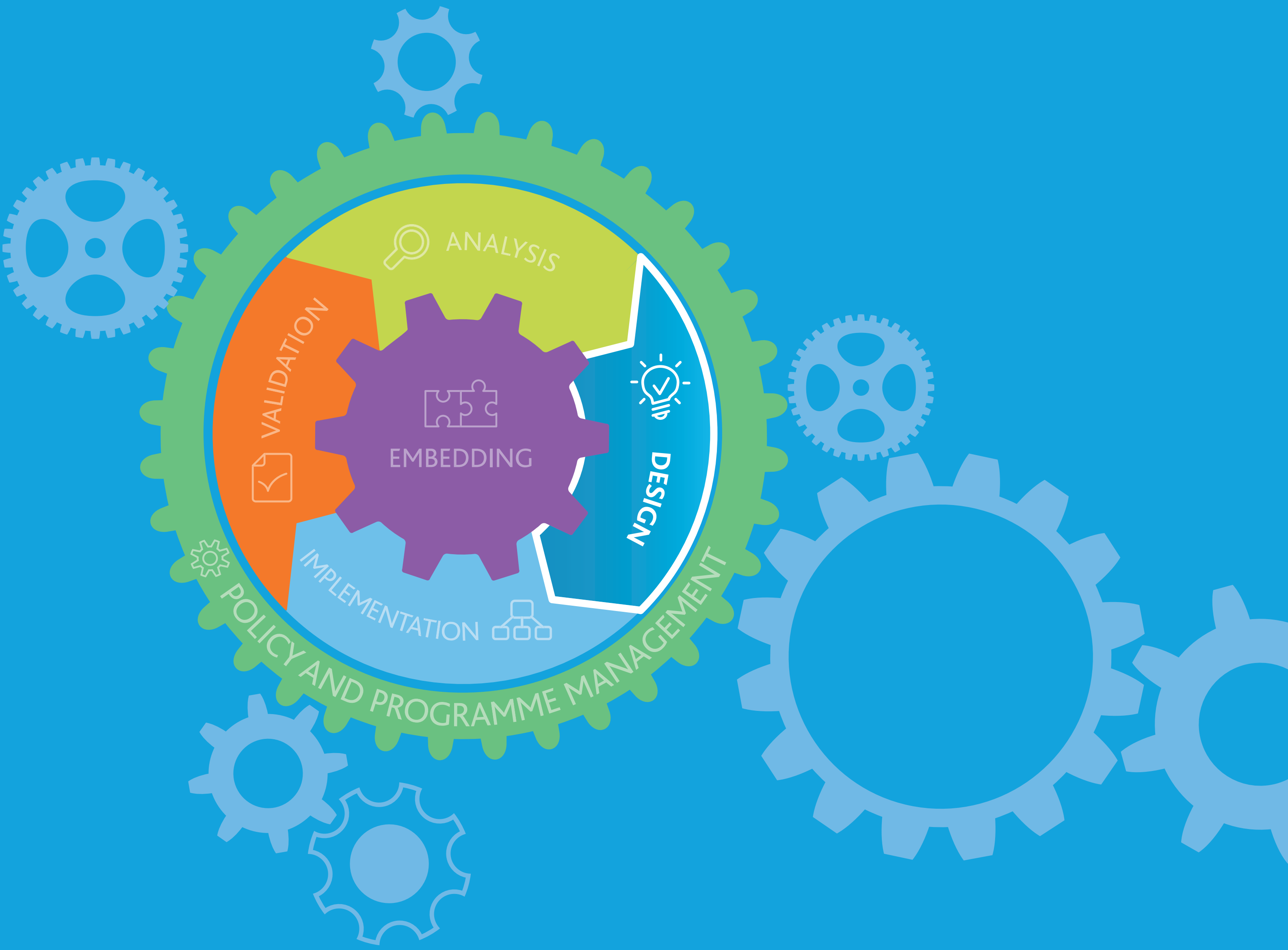
This final analysis and consolidation activity should result in the following:

- “Confirmation of impacts over time.
- Review and confirmation of resource dependencies and requirements.
- Consolidation of resource requirements, for example, across processes, organizational structures, or locations.
- Review and confirmation of the interdependencies of processes and activities, and their relation to the delivery of products and services...”. (Source: ISO/TS 22317:2015)

After consolidating the information, the business continuity professional should present the outcomes of the BIA to top management for review and approval. This is typically done in a BIA summary report to highlight key findings and enable the business continuity solutions and mitigation measures to be designed.

The BIAs should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.




ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
EMBEDDING
POLICY AND PROGRAMME MANAGEMENT

BCI Professional Practices

PP4

Design

Design is the Professional Practice within the business continuity management lifecycle that identifies and selects appropriate solutions to determine how continuity can be achieved in the event of an incident. The Analysis stage identifies the business continuity requirements and the Design stage determines the solutions that should then be implemented to best achieve these requirements.

Introduction

At this stage in the business continuity management lifecycle, the business continuity professional should design solutions that enable the organization to respond to an incident, and continue to provide its prioritised activities.

The requirements that support the implementation for each proposed business continuity solution are determined, and the most appropriate ones are selected in consultation with top management. Some solutions will be dependent on suppliers, their supply chains, and outsourced service providers.

An important part of this stage of the business continuity management lifecycle is to consolidate the selected solutions to ensure that opportunities for organization-wide collaboration are considered prior to progressing to the implementation stage.

Proactive mitigation measures are designed to address the risks and threats identified in the Analysis stage. Mitigation measures can be implemented to protect the organization and reduce the impact of disruption to the prioritised activities.

For organizations implementing a business continuity programme for the first time, the Design stage identifies and selects solutions that deliver the business continuity requirements identified during the Analysis stage.

For existing programmes, the Design stage should consider the following:

- Reviewing existing solutions to ensure that the most appropriate and cost effective options are in place.
- Identifying and selecting solutions that are required to adapt to changes in the prioritised activities or the impacts over time as identified during the Analysis stage. For example, a legal or regulatory change in requirements that the organization must meet.
- Maintaining or improving capability.

Designing Business Continuity Solutions

Designing solutions for how an organization is going to continue operating following a disruption is based on the business continuity requirements identified in the BIA, and the outcomes from the risk and threat assessment.

General Principles

The business continuity requirements and the outcomes of the risk and threat assessment are reviewed and appropriate business continuity solutions designed.

Once the solutions are designed, top management should agree the most appropriate solutions, and projects should be initiated to implement these solutions.

Price versus performance, and cost versus benefit are often used to guide top management when agreeing the most appropriate solutions.

The selection of solutions can also be influenced by legal or regulatory requirements or a commercial decision to gain competitive advantage.

Concepts and Assumptions

Organizations that already have a business continuity programme in place may have solutions that have been designed and implemented but are no longer relevant due to changing threats.

For any solution being designed, it is not only the business continuity requirements which should be met, but consideration should be given to any interdependencies identified, particularly when the solutions rely on suppliers and their supply chains.

For example, a supplier whose machinery becomes unavailable may no longer be able to meet the existing RTO or provide the service. Without a service level agreement in place, this unavailability may not be discovered until the business continuity plan is invoked.

Service level agreements can be put in place with suppliers to support the selected solutions. Such agreements can offer some assurance that the organization will be notified of any changes in the supply chain to avoid undesirable consequences.

Organizations that have an existing business continuity programme and those implementing a programme for the first time will probably have some level of continuity capability already in place. Designing or redesigning business continuity solutions is required where current continuity capabilities do not meet the requirements identified in the Analysis stage of the business continuity management lifecycle.

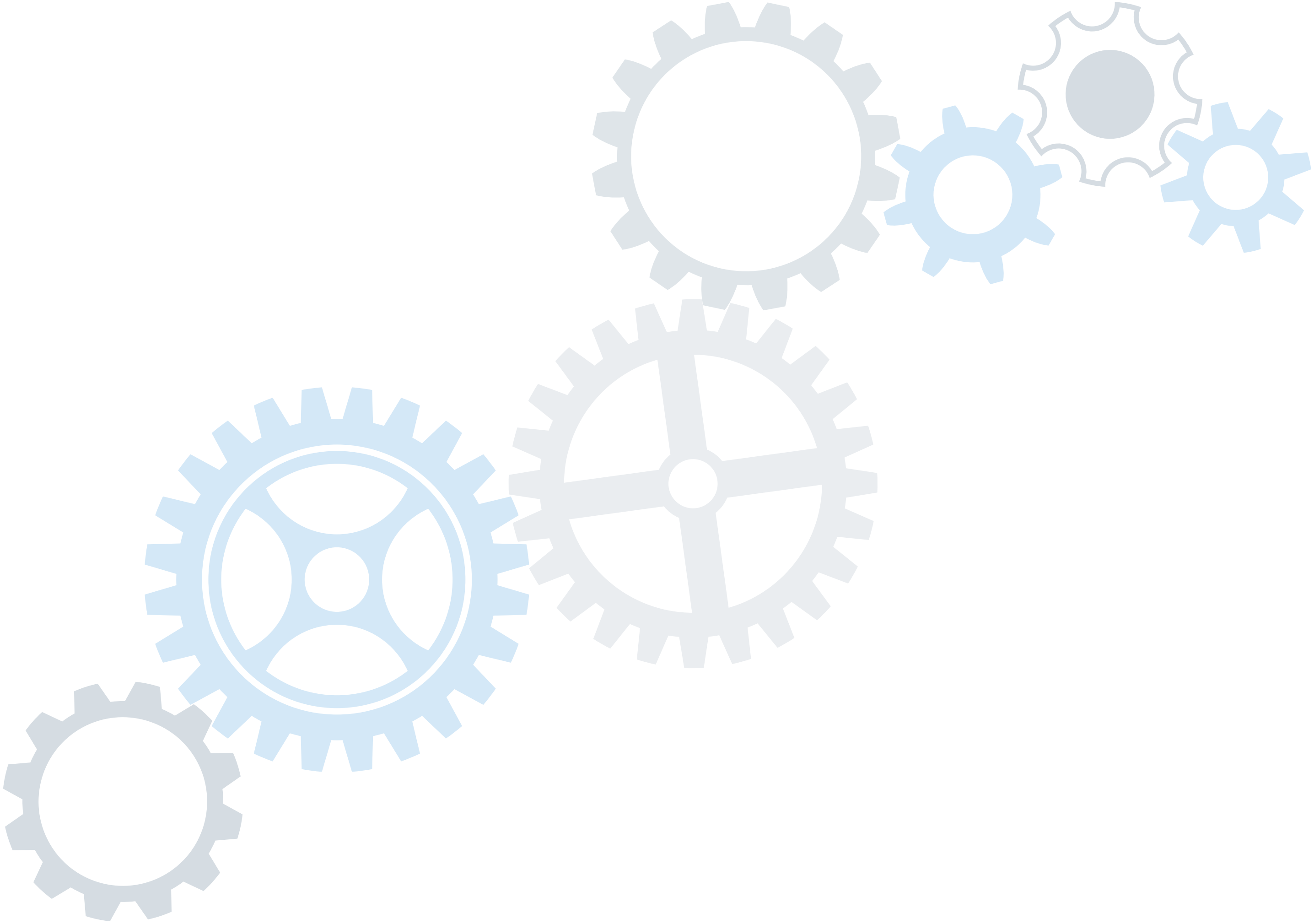
The difference between current capability and business continuity requirements indicates either:

- A gap where the requirement is not being met, creating an operational exposure.
- An overinvestment where the capability is greater than the organization needs it to be. This can present opportunities to reduce cost and complexity of existing solutions.

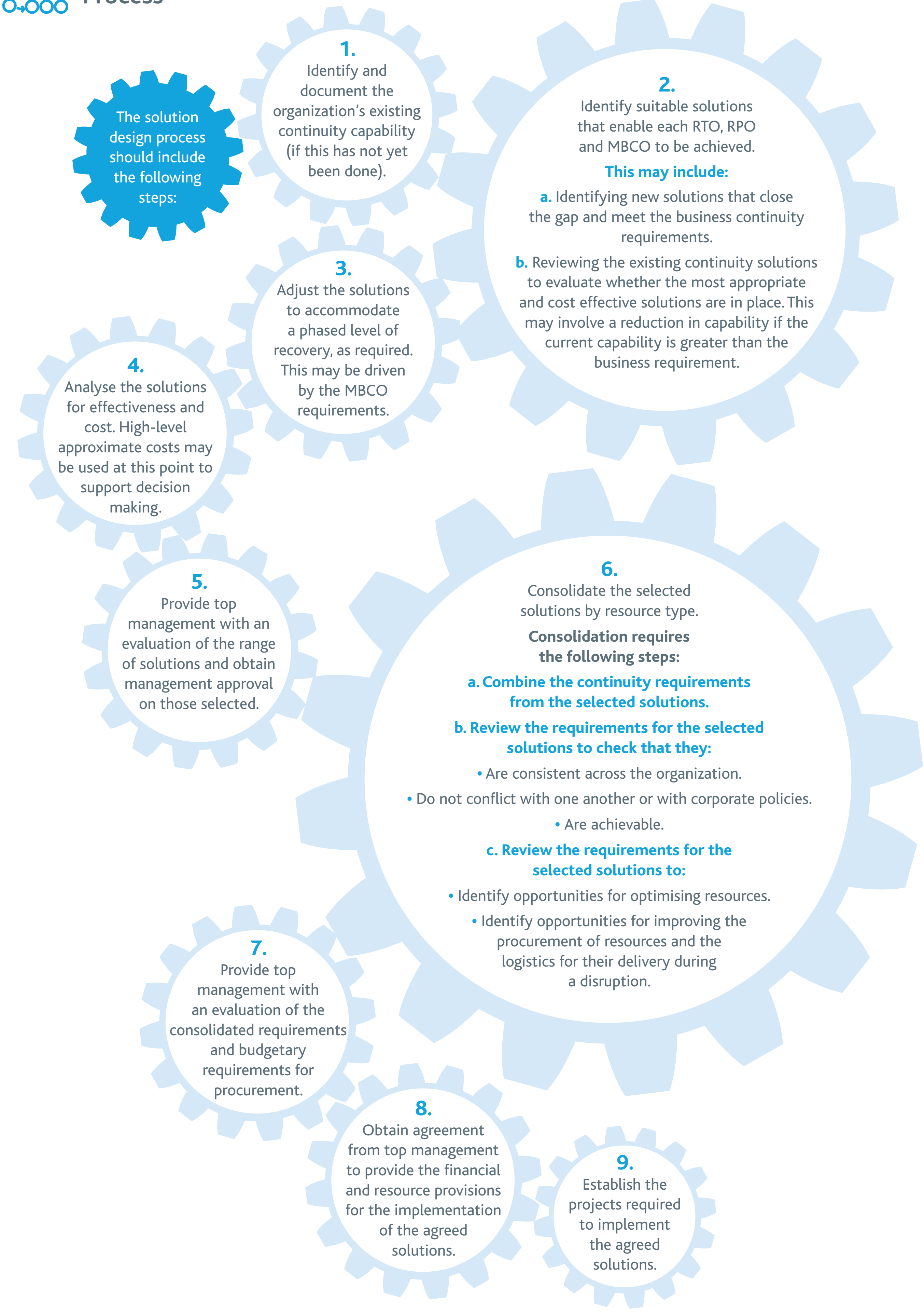
The business continuity professional should identify potential solutions to these gaps in consultation with those individuals who have roles on the business continuity programme, for example, the business continuity steering group and departmental representatives. This process should involve reviewing lessons learned from any disruption or significant changes in the organization, industry sector or locations that are in scope.

When additional information is required to support decision making, a cost benefit analysis can be used. A cost benefit analysis identifies in detail the costs of implementing and maintaining the solution and compares these to the benefits.

> If cost was not a consideration, it would be possible to design and implement a perfect solution or range of solutions. In practice, there is always a compromise between cost and speed of recovery. Generally, the shorter the RPO and RTO, the more expensive the solution is. Ultimately, the goal should be to balance continuity capability against reasonable and affordable costs.



Process



The solution design process should include the following steps:

1. Identify and document the organization's existing continuity capability (if this has not yet been done).

2. Identify suitable solutions that enable each RTO, RPO and MBCO to be achieved.

This may include:

a. Identifying new solutions that close the gap and meet the business continuity requirements.

b. Reviewing the existing continuity solutions to evaluate whether the most appropriate and cost effective solutions are in place. This may involve a reduction in capability if the current capability is greater than the business requirement.

3. Adjust the solutions to accommodate a phased level of recovery, as required. This may be driven by the MBCO requirements.

4. Analyse the solutions for effectiveness and cost. High-level approximate costs may be used at this point to support decision making.

5. Provide top management with an evaluation of the range of solutions and obtain management approval on those selected.

6. Consolidate the selected solutions by resource type.

Consolidation requires the following steps:

a. Combine the continuity requirements from the selected solutions.

b. Review the requirements for the selected solutions to check that they:

- Are consistent across the organization.
- Do not conflict with one another or with corporate policies.
- Are achievable.

c. Review the requirements for the selected solutions to:

- Identify opportunities for optimising resources.
- Identify opportunities for improving the procurement of resources and the logistics for their delivery during a disruption.

7. Provide top management with an evaluation of the consolidated requirements and budgetary requirements for procurement.

8. Obtain agreement from top management to provide the financial and resource provisions for the implementation of the agreed solutions.

9. Establish the projects required to implement the agreed solutions.

Methods and Techniques

There are many well established business continuity solutions that can be used within an organization.

These solutions include:

Diversification: Separating activities and resources and running live activities at two or more locations so that in the event of disruption at one location, the activities can continue at the alternate location. This solution can be costly and may not protect an organization if the disruption is not confined to a single location or area. Consideration should be given when designing this solution, so that in the event of disruption at one location, the alternate location can cope with any extra workload that has been displaced from the disrupted site. This may involve the suspension of non-essential operations at the alternate location until the disrupted location can recover. This solution may be appropriate where the RTO is measured in seconds, minutes, or hours, rather than days.

Replication: Duplicating resources to enable activities to be recovered quickly is a variation on diversification. The replicated site is maintained at a high state of readiness with all required resources in place. It does not become operational until it is required to take over any disrupted activities displaced from the site of the incident.

An alternate location solution that is pre-equipped and can be activated in a very short time frame can also be referred to as a 'hot site'. However, this can be an expensive solution as it means having resources in place but unused until they are required for business continuity purposes.

This business continuity solution may be suitable where the RTO ranges from a few hours to a few days, as long as personnel can be moved to the alternate location within their activity RTOs. However, it relies on personnel being both able and willing to work away from their primary location for an unknown time frame.

Standby: Where the RTO allows for a longer response time, measured in days rather than hours, an appropriate solution may be to have a standby facility available that can be made operational within the RTO. This solution can be referred to as a 'warm site' and is particularly suitable where an organization has access to a facility that has been temporarily shut down, but can be reactivated and become operational at short notice. This solution relies on personnel being both able and willing to work away from their primary location for an unknown time frame.

A warm site standby solution may be suitable for lower priority activities which can be temporarily suspended after a disruption occurs to allow time for the warm site to be reactivated and prepared for occupation.

Post-incident acquisition: When prioritised activities have RTOs that are measured in days or weeks, organizations can consider a business continuity solution where the required resources are acquired after the disruption occurs. This solution relies on the organization having a predefined and prioritised list of resource requirements. It also depends on suppliers' ability to provide the resources in suitable quality and quantity within acceptable time frames. This would not be an appropriate continuity solution where there is a requirement for specialised resources, for example, equipment, facilities, supplies, or skills, that might be difficult to obtain or which have long lead times that exceed the identified RTOs.

Do nothing: This solution involves waiting until after the incident to decide what to do. This may be an appropriate solution where the RTO is measured in weeks or months, or where it is impossible, too difficult, or too expensive to provide alternate facilities or resources before an incident occurs.

The business continuity professional should always document the reasons why doing nothing is the selected solution, to avoid disputes or conflicts should an incident occur.

Organizations will usually find the best outcome is in combining business continuity solutions, so that the solutions reflect the priority and RTOs of the processes and activities. This combined approach also allows limited resources to be allocated in advance to the continuity solutions that support the highest priority activities, while providing low, or no up front cost solutions for lower priority activities.

Solutions and their implementation might require technical skills beyond those of a business continuity professional. Technical advice might need to be sought from experts in other management disciplines or departments in these instances. For example, specialists in ICT, procurement/purchasing and supply, inventory management, and capacity planning may be required to identify and implement solutions.

Resource requirement examples for business continuity solutions

The tables below highlight some resource requirement examples for the different solutions:

Buildings and work environment

Table 5.

Business continuity solution option	Office location	Remote working location
Diversification	Separate premises where the same activity occurs in parallel.	A department's operations are entirely remote or there is a combination of personnel working remotely and at the office.
Replication	Separate premises that have all facilities required to undertake an activity, but it is not currently being used.	Remote working is available and ready at any time with office equipment and ICT available, though not currently being used.
Standby	Separate premises that have some of the facilities required to undertake an activity, but additional facilities will be required before the activity can be undertaken.	Remote working can be made ready following simple setup or partial acquisition.
Post-incident acquisition	Suitable premises can be acquired which may or may not already have the facilities required to undertake an activity.	Remote working is generally not ready but can be made ready through the acquisition of office equipment and ICT.

People

Table 6.

Diversification	People in separate locations that are concurrently undertaking the same activity.
Replication	People in another location that are experienced and able to undertake the same activity, but not yet doing so.
Standby	Individuals in another location that have been trained to do the same activity, but are not yet experienced and will require guidance.
Post-incident acquisition	External people skilled in undertaking an activity that can be hired, or internal personnel that can be trained to undertake an activity.

Information and communication technology systems and data

Table 7.

Diversification	Two copies of a system and its data in separate locations that are kept synchronised and live.
Replication	An operational copy of a system and its data held in a separate location that is periodically synchronised with the live version and needs switching to be made live.
Standby	An operational copy of the system held in a separate location and a backup of its data that needs to be loaded and tested with manual switching to be made live.
Post-incident acquisition	Backup copies of the system and its data that need to be installed on equipment acquired after the incident.

Equipment

Table 8.

Diversification	Duplicated operational equipment held in a separate location, with an automatic transfer from one to the other.
Replication	An exact non-operational copy of the equipment held in a separate location that can be rapidly made live.
Standby	Replacement equipment held in a separate location that needs to be made operational.
Post-incident acquisition	Equipment that can be acquired from a supplier.

Consumables

Table 9.

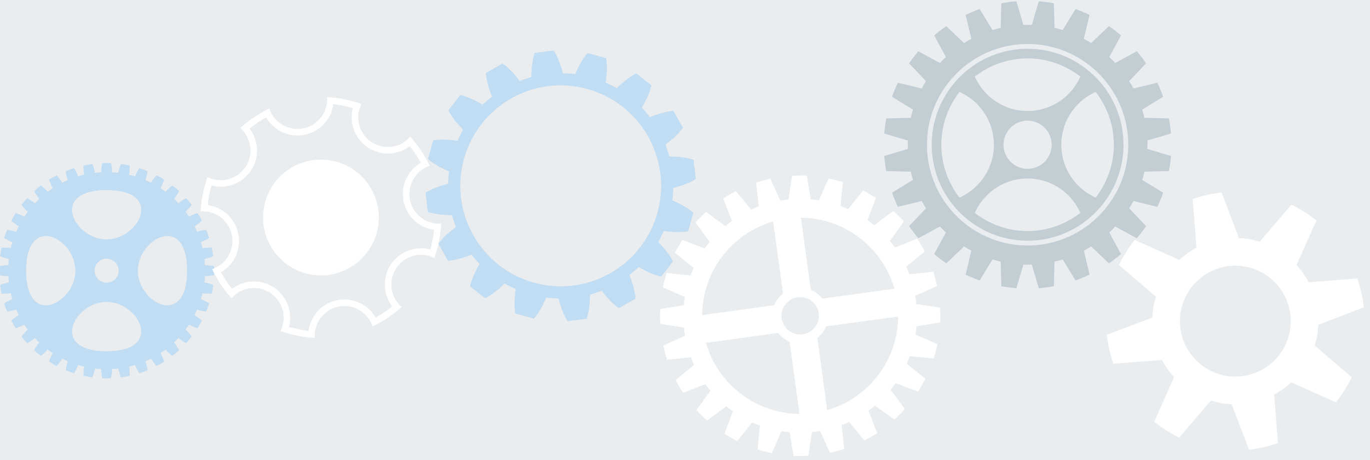
Diversification	Duplicated items held in separate locations with stock being supplied from both locations.
Replication	Duplicated items held in a separate location that is not currently being used.
Standby	Replacement items held in a separate location that could be used with modification.
Post-incident acquisition	Items that can be acquired from a supplier.

Suppliers

Table 10.

Diversification	Separate suppliers that are currently providing the same product or service.
Replication	An alternate supplier that has already been contracted to provide the same product or service as an existing supplier, but is not currently doing so.
Standby	A pre-agreed supplier that can provide the same product or service as an existing supplier and has agreed to do so when required, but there is currently no contract in place.
Post-incident acquisition	Suppliers that can be asked to supply a product or service.

Business continuity solutions for other types of resources will usually fit into one or a combination of the examples above.



Further considerations

Remote working: Many organizations have adopted policies and technologies that enable personnel to work away from their primary place of work. This may be a regular or temporary arrangement and is a variation on the standby solution. Where remote working is possible, it provides organizations with further options to include in the combination of business continuity solutions.

Key requirements to support remote working at any location are stable electric power and other utilities, adequate ICT facilities, appropriate data security, and a suitable work space to conduct business activities. The organization should also have the ability to cope with larger than usual requirements for remote ICT access.

> Working remotely has the benefit of isolation during a pandemic based incident or crisis. It is also effective when being at work or commuting to work is no longer reliable or safe, for example, during industrial action, terrorist attack, or severe weather.

If selected and implemented as part of the business continuity plan, remote working is a solution that should be tested as part of the exercise programme.

Partial failures: Although solutions are sometimes discussed in terms of total site or facility failure, depending on the scope of the business continuity programme, it is often necessary for the solution to be flexible to cover isolated failures, for example, the loss of only one ICT system, a single production line, or partial loss of a large building.

Solutions for isolated failures may sometimes not be feasible, for example, if several ICT systems or production lines are closely linked, they cannot be transferred to another location in isolation.

In some industries, there may be no feasible alternate site solutions to address a total site outage, for example, in the case of a disruption to a major transportation hub that is too expensive or difficult to duplicate.

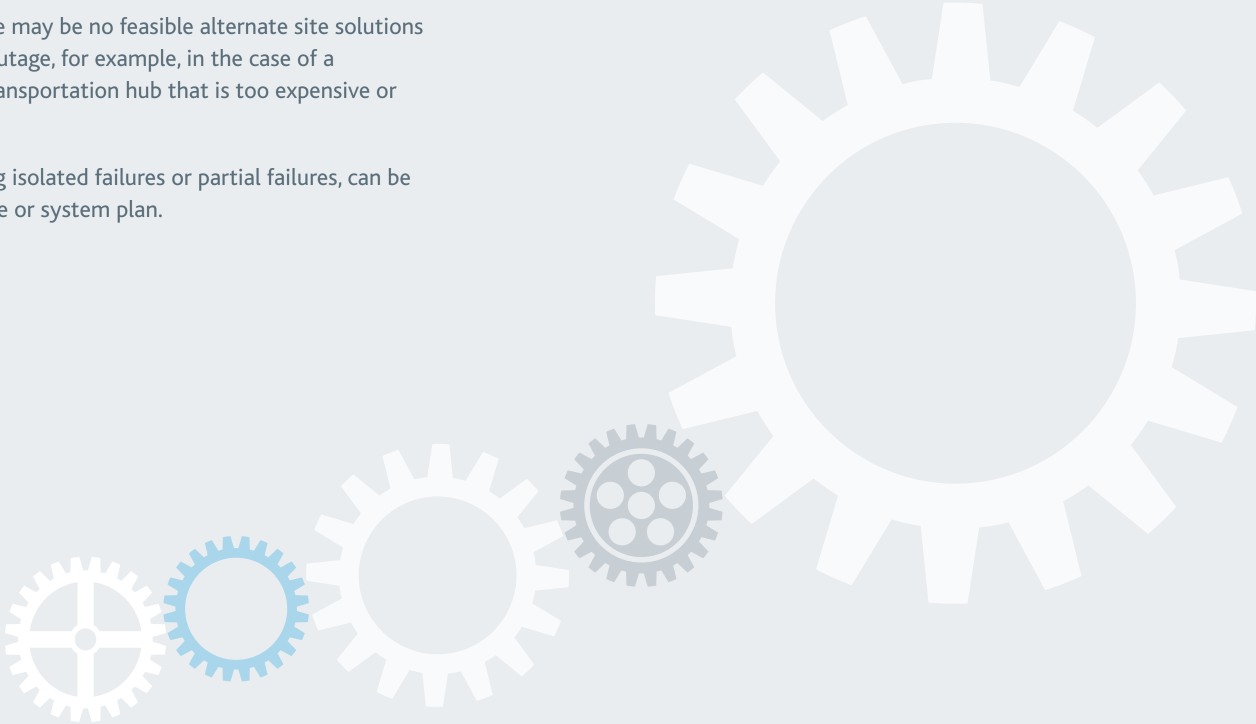
In such cases, addressing isolated failures or partial failures, can be covered by a specific site or system plan.

Finance: It is essential to plan for short and long term funding of personnel and the organization in the event of an incident. Agreements should be drawn up with banks and easily accessible assets should be identified that can fund an organization during a disruption. The organization should also agree and document the terms for payments to non-essential personnel that are not actively employed during an extended disruption. This should include consideration of any legal, regulatory, or duty of care responsibilities.

Insurance: Insurance can provide financial compensation for loss of assets, increased costs, recovery, and protection for associated legal liabilities. However, it is unlikely to provide cover for the full expense of a disruption, including intangible impacts such as the loss of customers, personnel, or reputation. There can also be a long period of time between a disruption and insurance payments being agreed. Therefore, it is important that those responsible for developing the business continuity solutions are aware of the organization's level of insurance.

Business interruption insurance is most closely associated with business continuity. It is not a complete solution unless RTOs are measured in months, and specialist equipment, facilities, or skills are easy to obtain.

It is important to note that business interruption insurance typically covers loss of business revenues (gross margins) and additional costs of working which are related to other insurable losses (such as loss of premises). More recently, some insurers have started providing cover for a wider range of disruptions, for example, supplier failure due to socio-economic or geo-political changes, however these broader scope policies can be expensive.



Safe separation distance: Many incidents, for example, earthquakes, wild fires, or major floods and other natural disasters, can result in the loss of access to a wide geographic area, so the organization should consider the need for adequate separation distance between the original and duplicate resources that form the basis of the business continuity solution.

The following should be considered:

- Keep duplicate copies of vital resources in a remote location.
- Use multiple suppliers.
- Replicate operations in different locations or designated recovery sites.

The selection of a safe separation distance will define the maximum geographic extent of an incident that the organization's business continuity solutions can effectively respond to. That selection should consider the following factors:

- The organization's strategy, objectives, and culture.
- The organization's target market.
- How far personnel are able or willing to travel to a relocation site.
- RTOs and RPOs.
- The organization's geographic environment and it's susceptibility to natural disasters.
- How the spread of a natural disaster is likely to affect the organization. For example, a hurricane can have a diameter of hundreds of kilometres whereas floods are generally more localised.
- Any existing legal or regulatory requirements relating to safe separation distance.

Geographical separation usually decreases the likelihood of two sites being affected by the same incident. However, this may not provide protection for threats that are not location specific, for example, outbreaks of disease, or cyber attacks.

Service levels: Many organizations will have identified only the minimum level of service that is acceptable to achieve its immediate business obligations during a disruption. This has been defined in the Analysis stage as the minimum business continuity objective (MBCO). Other organizations will have identified a phased level of resources required to enable service levels to be increased over a specific time frame from the minimum acceptable level to a normal level.

Where alternate sites or facilities are involved in the business continuity solution, it is recommended to have service level agreements (SLAs) to formalise the commitments of the alternate facility provider during an incident.

Design detail: The extent and detail to which business continuity solutions need to be designed should depend on the urgency with which they are required and the complexity of the product or service, process, or activity being recovered.

A detailed business continuity solution is required for processes and activities with short RTOs. Less detail is needed when the RTO is in weeks or months, unless deemed necessary by the organization.

Classification schemes: Some organizations may choose to classify activity and resource RTOs. For example, an A/B/C/D classification scheme may be used where category 'A' delivers the prioritised activities and resources, based on metrics such as the RTO and RPO. Category A will use the most advanced or sophisticated solutions compared to Category D whose activities and resources require less urgent and less sophisticated solutions.

Interested parties: There may be many individuals and groups affected by a disruption. For example, in a fire, contractors may be injured, residents evacuated from their homes, and local businesses experience reduced trade.

The organization's level of responsibility in such situations should be clearly understood.

The organization should ensure that the needs of various interested parties are identified, prioritised, and agreed when designing business continuity solutions.

Emergency responders: The organization should be familiar with the procedures of the local emergency responders and may benefit from contacting these groups in advance. They may provide useful information relating to the Design stage of business continuity solutions. For example, law enforcement agencies may have identified exclusion zones that result in denial of building access which lasts longer than the RTO.

Supply chain: In the Analysis stage, key suppliers of products, services or activities are identified. Solutions for the loss of these suppliers and the disruption to the products, services, and activities need to be identified in the Design stage to enable their RTOs to be achieved.

The organization should consider that the required products and services may not be commercially available. For example, there may be commercial competition restrictions or environmental, legal, quality, security, or ethical constraints.

Outsourced service providers may be best placed to perform duties which are commonly available, for example, cleaning, security services, and transportation.

Subcontracting during incidents: Outsourced service providers can provide a product or service, provide process infrastructure, and takeover disrupted activities. Subcontracting can be particularly suitable for manufacturing, where the added cost of having alternate sites replicated or on standby is too expensive. However, in some situations, the only option for subcontracting may be to use another organization operating in the same market, which could be a competitor. Collaboration with competitors should be considered, where appropriate.

Reliability: When the business continuity solutions being considered involve an outsourced service provider, there is often a need for compromise between the cost and reliability of the outsourced provider. Arrangements may vary from verbal agreements through to a service level agreement. The shorter the RTO, the more important the reliability of the delivery becomes.

Similarly, where the outsourced supplies or services have been prioritised by the organization, care should be taken to determine the reliability of the supplier and to have a suitable solution in place to address supplier failure.

Consolidation

There is usually an opportunity to combine certain elements of the design process to remove duplication and ultimately make the design more efficient. The following examples highlight the concept of consolidation:

Purchasing leverage: If the total requirement for recovery resources is known, then the organization is more likely to obtain better terms from its supplier than if each individual requirement is separately negotiated. This consolidated approach should be undertaken by personnel who are experienced in procurement and contract negotiation.

Logistics: The logistics for the phased delivery and acceptance of consolidated resources across multiple departments can also be streamlined through consolidated procurement and delivery.

Conflict: Two or more areas of the organization may be planning to use the same resource as part of their continuity solution and would therefore be in conflict during an incident, for example, meeting rooms in another office.

Optimisation: Two or more activities may require a resource, for example, a printer, photocopier, or projector, but may be able to share its use with others. Consolidation can optimise the use of resources by identifying opportunities for sharing.

Consistency: The approach to continuity solutions may be inconsistent within the organization, for example, the implementation of information security. Consolidation can highlight the additional resources needed to ensure consistency.

Capability: When applied throughout the organization, a continuity solution, for example, remote working, may not be achievable using the existing infrastructure. This may work when only a few individuals work remotely, but not when everyone in the organization with the capability tries to do so at the same time. Consolidation may identify further resource requirements to support such situations.

Care should be taken to ensure consolidated solutions do not conflict with other common or unique individual solutions, organizational policies, supplier accreditation, or legal and regulatory constraints.

Outcomes and Review

The main outcomes from designing business continuity solutions are:

- A set of business continuity solutions which are agreed by top management.
- A business continuity capability, based on the agreed solutions that should be used when developing and implementing plans.
- Sufficient information and clarity of solutions to establish projects with appropriate funding and resources for implementing the agreed solutions.
- A consolidated set of resource requirements to be used when purchasing resources.

The agreed business continuity solutions should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Risk and Threat Mitigation Measures

Mitigation measures should be identified and implemented to reduce the impact of a disruption to the organization's prioritised activities. The business continuity professional should collaborate with risk, physical security, and information security professionals to develop and implement mitigation measures as appropriate. Organizational resilience can be increased when related management disciplines are coordinated, not only within the organization but with suppliers and other interested parties.

General Principles

Measures selected should be targeted at unacceptable levels of risk, any single points of failure, and the main threats to the organization's prioritised activities. All of these are identified in the Analysis stage of the business continuity management lifecycle.

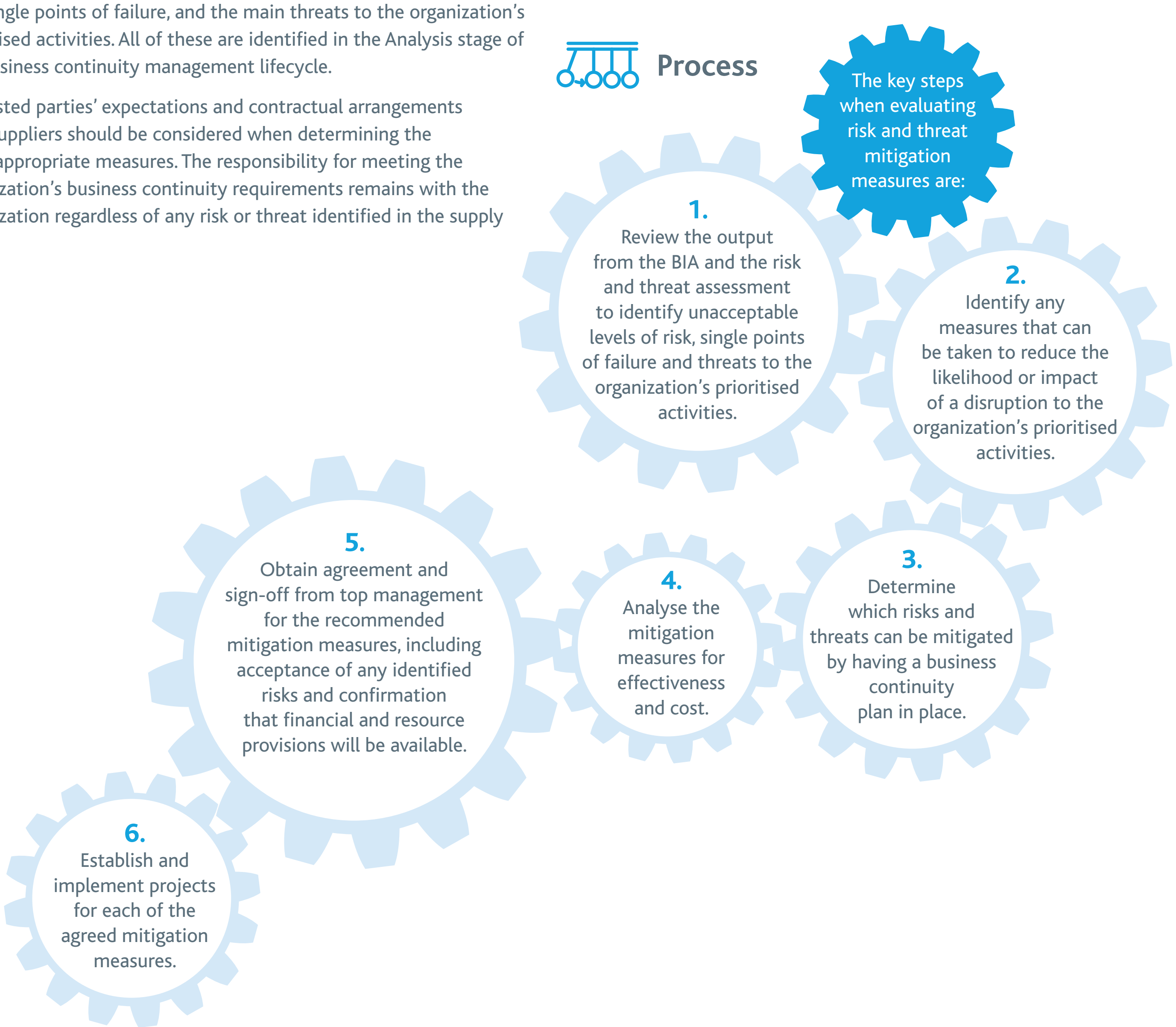
Interested parties' expectations and contractual arrangements with suppliers should be considered when determining the most appropriate measures. The responsibility for meeting the organization's business continuity requirements remains with the organization regardless of any risk or threat identified in the supply chain.

Concepts and Assumptions

Designing mitigation measures assumes that the benefits of the proposed measures can be evaluated. Understanding the benefits relies on knowing the likelihood of a threat being realised, which in many cases is based on historic information or probability.

There may also be a legal or regulatory requirement to ensure appropriate mitigation measures are in place. For prioritised activities that are outsourced or dependent on suppliers, measures should be considered and a cost benefit analysis carried out as part of the evaluation. There may be additional costs incurred when outsourced service providers are involved.

Process



The key steps when evaluating risk and threat mitigation measures are:

1. Review the output from the BIA and the risk and threat assessment to identify unacceptable levels of risk, single points of failure and threats to the organization's prioritised activities.

2. Identify any measures that can be taken to reduce the likelihood or impact of a disruption to the organization's prioritised activities.

3. Determine which risks and threats can be mitigated by having a business continuity plan in place.

4. Analyse the mitigation measures for effectiveness and cost.

5. Obtain agreement and sign-off from top management for the recommended mitigation measures, including acceptance of any identified risks and confirmation that financial and resource provisions will be available.

6. Establish and implement projects for each of the agreed mitigation measures.

Methods and Techniques

Cost benefit analysis: A cost benefit analysis can be used to evaluate mitigation measures by comparing the cost of the measure with the likely benefit to be gained. When undertaking a cost benefit analysis, the time frame in which the solution or measure should be effective and the likelihood of the threat being realised in that time frame need to be determined.

For measures that reduce the **likelihood**, the benefit is calculated by estimating the reduction in likelihood of the threat being realised after the mitigation measure has been put in place, and multiplying it by the impact on the organization if the threat was realised, in terms of cost.

For measures that reduce the **impact**, the benefit is calculated by estimating the reduction in the impact of the threat to the organization in terms of cost, after the mitigation measure has been put in place and multiplying it by the likelihood of the threat occurring.

Examples of specific measures that can be implemented are as follows:

- Physical security to prevent theft and unauthorised entry.
- Information security to prevent loss of information and unauthorised access.
- Monitoring systems to provide prompt warning of fire, utility failures, equipment failures and potential threats.
- Sprinkler and fire suppression systems to prevent fire from spreading.
- Resilient telecommunications networks to ensure there are no single points of failure.

Further guidance can be obtained from the relevant international and national risk management standards and guidelines such as ISO 31000:2009. Other professional associations and organizations also publish good practice guidance regarding risk management and mitigation measures in their specific areas of expertise.

Managing supply chain risk: The threat of disruption to the organization's products and services caused by failure in suppliers and their supply chains can be reduced by ensuring that suppliers have effective and adequate business continuity arrangements in place. This can be achieved by:

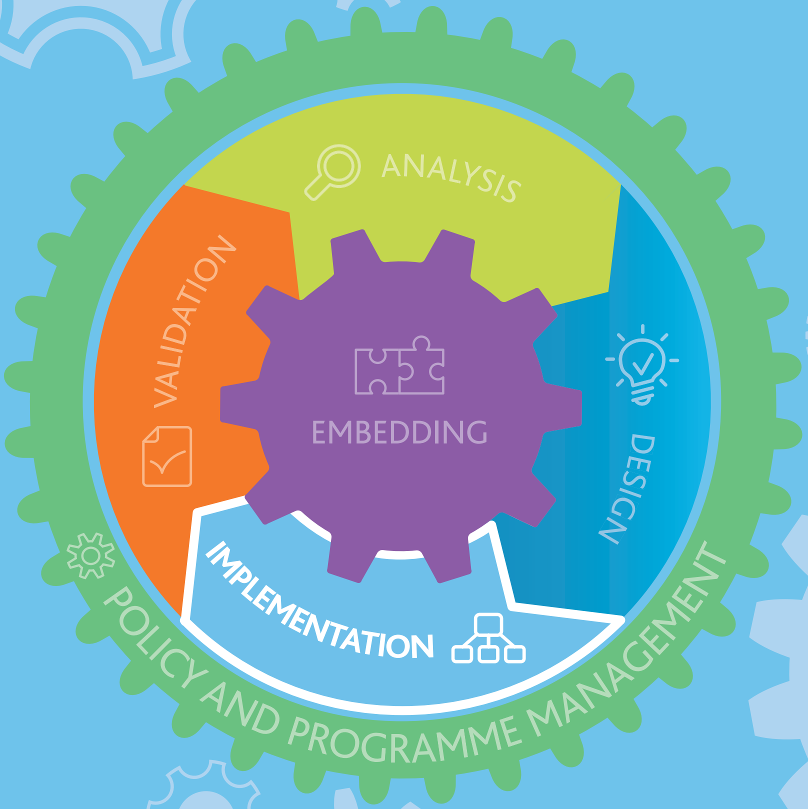
- Including business continuity requirements in supply contracts.
- Seeking evidence of compliance with a recognised business continuity standard.
- Reviewing each supplier's business continuity programme to ensure that it is effective and adequate.
- Undertaking joint exercises with suppliers.
- Agreeing realistic service levels for supply disruption.

Assessing the suitability of a supplier's business continuity programme or selection of any outsourced service providers should occur prior to any contract being agreed or as part of ongoing relationship management with the supplier. Failure to do so and any subsequent requests for enhanced arrangements may be considered a contract variation and result in increased costs. In addition to seeking evidence of an effective business continuity plan, the specific time objectives offered for the service should be requested (RTOs, MBCO and MTPDs). These time objectives should align with the business continuity requirements of the organization.

Outcomes and Review

The main outcomes when designing risk and threat mitigation measures are projects for implementing the agreed measures to reduce the likelihood or impact of a disruption to the organization's prioritised activities.

The mitigation measures should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.


ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
EMBEDDING
POLICY AND PROGRAMME MANAGEMENT

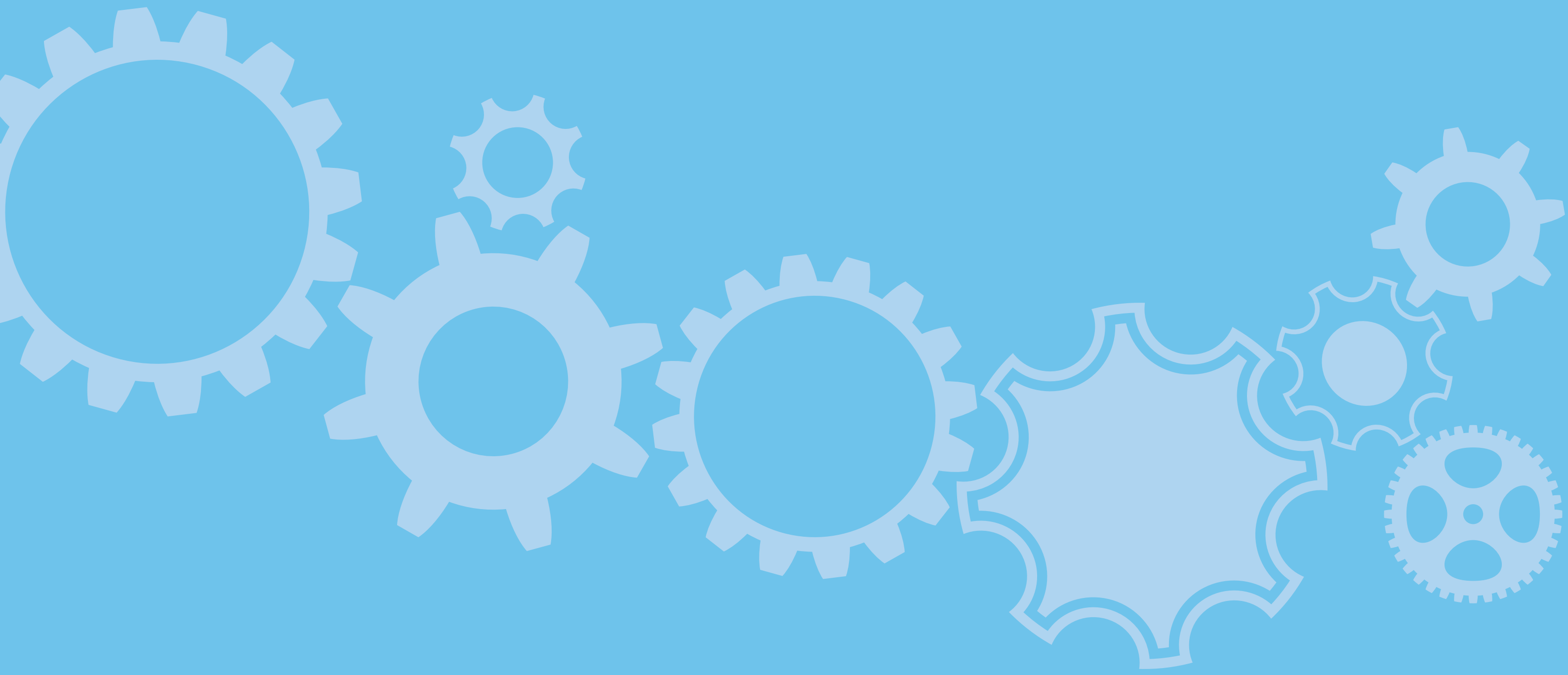
BCI Professional Practices

PP5

Implementation

Implementation is the Professional Practice within the business continuity management lifecycle that implements the solutions agreed in the Design stage. Implementation is achieved by developing business continuity plans to meet the organization's agreed business continuity requirements and solutions identified in the Analysis and Design stage of the lifecycle. The Implementation stage also includes the development of a response structure that defines the necessary roles, authority and skills required to manage an incident.

The aim is to identify and document the priorities, procedures, responsibilities, and resources that will support the organization when managing an incident. This should achieve continuity of the prioritised activities and ensure recovery of disrupted activities to a predefined level of service (the minimum business continuity objective) within the planned time frames.



Introduction

The term 'business continuity plan' (BCP) suggests a single document. However, a variety of plans can exist at any organizational level. The BCP may in fact comprise several documents. It can cover a complete organization or part of an organization and can be structured according to the size, complexity, and type, for example, by products, services, locations, divisions, or departments.

The key requirements for implementation of an effective business continuity plan are as follows:

- An ability to recognise and assess existing and potential threats when they occur and to determine an appropriate response.
- A response structure in place for the activation, escalation, and control of the organization's response.
- Personnel with the authority and competency to implement the agreed solutions and measures.
- An ability to communicate effectively between internal and external interested parties.
- Access to sufficient resources to support the agreed continuity solutions.

The business continuity plans are not intended to cover every eventuality as all incidents are different. The plans need to be flexible enough to be adapted to the specific incident that has occurred and the opportunities it may have created. However, in some circumstances, incident specific plans are appropriate to address a significant threat or risk, for example, a pandemic plan, or a product recall plan.

> Plans developed to address a specific threat or risk are often called contingency plans.

Many organizations may have existing procedures in place that address the response to various types of disruption.
For example, plans for evacuation, health and safety, ICT service continuity, physical security, crisis communication, and information security.

Many disruptions will have a broad impact on organizations and require the activation of several response plans to effectively deal with the same incident. An effective organizational response capability can be achieved if business continuity professionals collaborate with other professionals who are accountable for managing the response in their respective management disciplines.

Response Structure

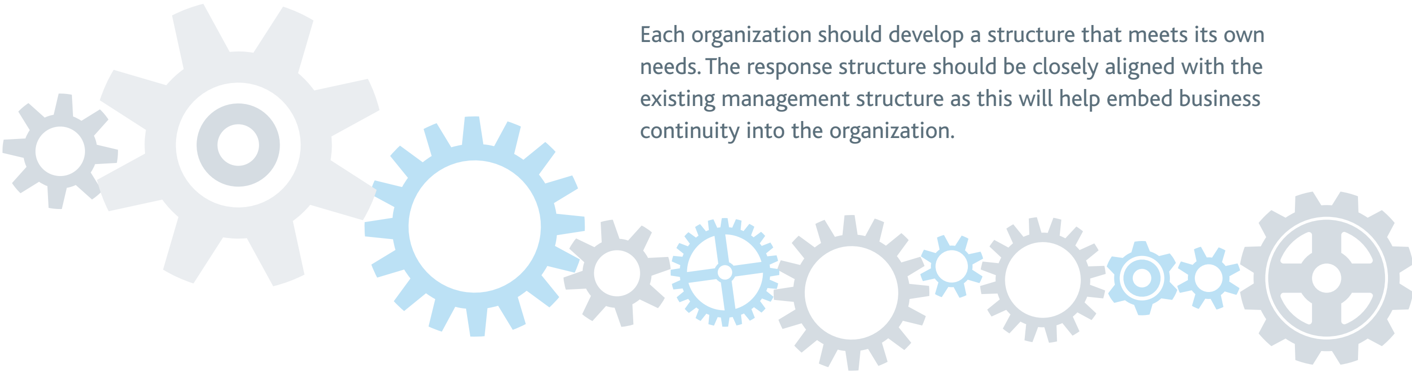
The purpose of establishing a response structure is to ensure that the organization has a clearly documented and well understood mechanism for responding to an incident, regardless of its cause. The response structure establishes command, control, and communication systems to help the organization manage the incident and minimise the impact of the disruption.

General Principles

The response structure identifies:

- The individuals and teams responsible for response activities.
- The roles and responsibilities of the individuals and teams.
- The relationships between the individuals and teams.
- The documented procedures to support the individuals and teams.

Each organization should develop a structure that meets its own needs. The response structure should be closely aligned with the existing management structure as this will help embed business continuity into the organization.



Business continuity can become embedded in an organization more easily if the response structure makes use of familiar organization terms that are already part of business as usual, for example team names, titles, and roles.

An effective response structure includes mechanisms that enable information to be communicated quickly and accurately to relevant individuals and teams throughout the organization. It should also recognise and include external suppliers related to prioritised activities.

Concepts and Assumptions

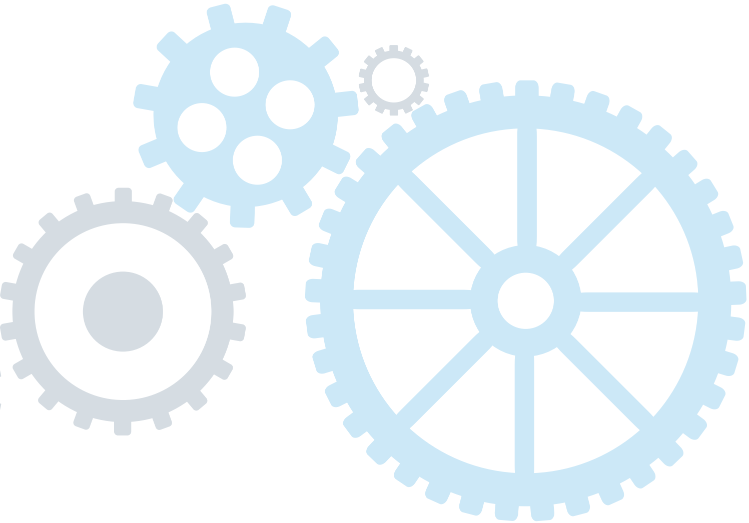
An organization's response structure should be flexible and capable of dealing with many types of disruption. There are two main types of disruption:

- An **incident,** defined as "a situation that might be, or could lead to, a disruption, loss, emergency or crisis." (Source: ISO 22300:2012)
- A **crisis,** defined as "a situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action." (Source: ISO 22300:2012)

Incidents and crises are linked, but are distinctly different from each other and so require a different level of response.

An organization's management of an incident is likely to be addressed using established plans and procedures.

A crisis is an unpredictable situation which exceeds anticipated limits and requires a flexible, creative, and strategic level response. The existing response structure, information, and procedures in the business continuity plan should be built on and adapted when responding to a crisis where relevant.



An incident, while unexpected, creates a level of disruption that falls within anticipated conditions and limits, and so can be managed using plans that were developed with those parameters in mind. For example, a business continuity plan may be designed to address operational disruption in a particular building, or an ICT service continuity plan that may be designed to deal with the loss of a specific cluster of servers.

A crisis involves a severe level of disruption that exceeds the anticipated conditions and limits, or may be a situation that an organization had not forecast during the planning process. For example, a regional power outage may simultaneously disrupt multiple buildings and sites operated by an organization. A major cyber attack could impact numerous suppliers at the same time causing significant and unpredicted disruption to an organization's supply chain.

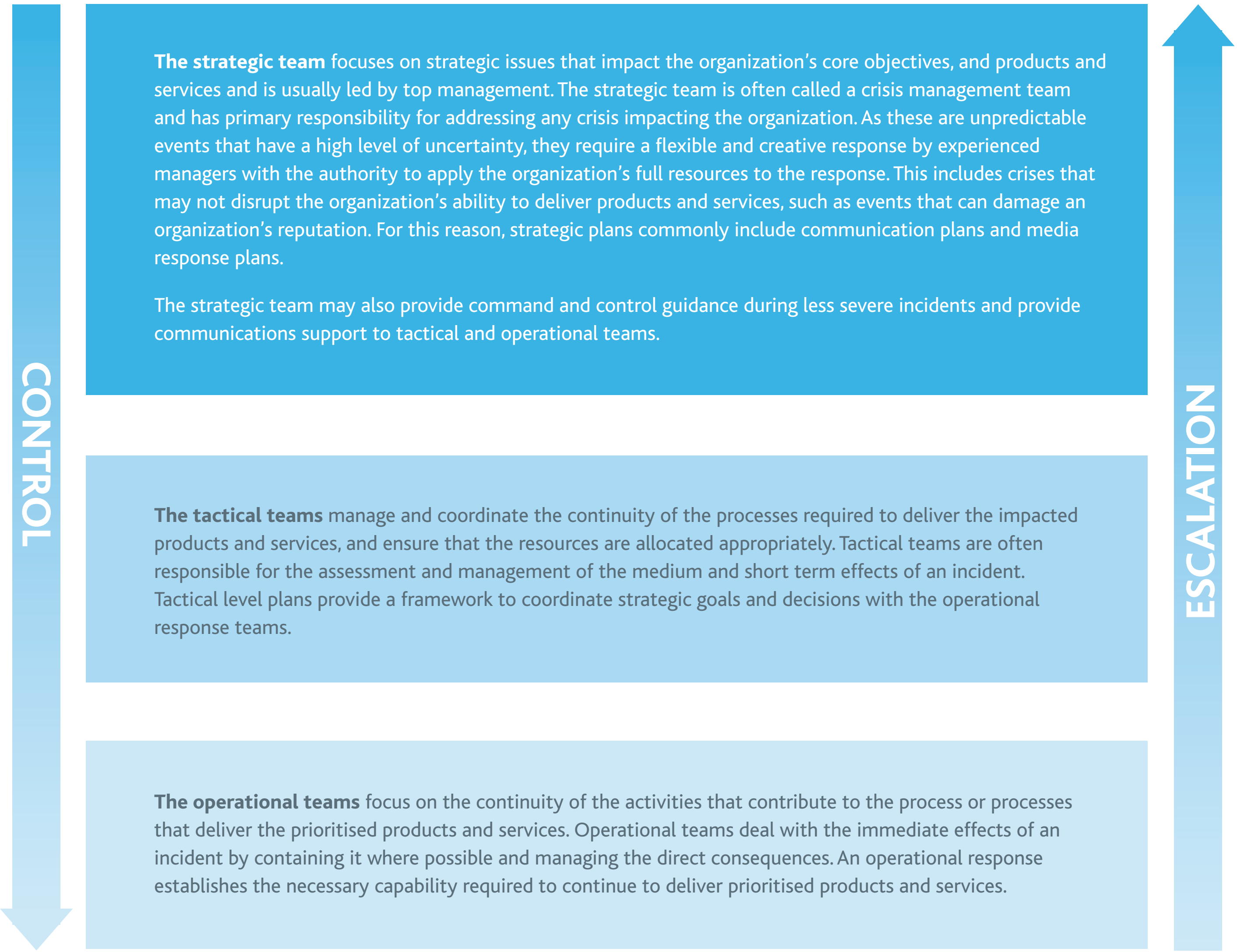
Disruptions can be immediate and obvious, but can also develop slowly over time. The response structure should include a mechanism for individuals and teams to promptly identify an incident, so that the situation can be assessed by experienced and authorised personnel and the appropriate response taken.

The key requirements for an effective response structure are:

- The ability to recognise and assess threats when they occur.
- Clear procedures for escalation when a disruption has occurred or may soon occur.
- Individuals and teams with the authority and capability to develop and select an appropriate response to an incident.
- Clearly understood procedures in place for the activation and control of the response to an incident or crisis.
- Responsible personnel with the authority and capability to implement the agreed business continuity solutions as defined within the organization's plans.
- An ability to communicate effectively with internal and external interested parties.
- Access to sufficient resources to support the implementation of the continuity solution.
- An ability to recognise when key external suppliers should be notified and included in the implementation of the continuity solution.
- An agreed budget for supporting the response structure.

There can be many different types and levels of response teams in an organization's response structure. Response teams should address the strategic, tactical, and operational levels which are appropriate to the organization. Therefore, the number of individuals or teams, and the plans that support them, are determined by the size, complexity, and type of organization.

In some organizations, it may be appropriate to have up to three levels of teams in the response structure. The strategic, tactical, and operational teams in a response structure undertake different activities as follows:



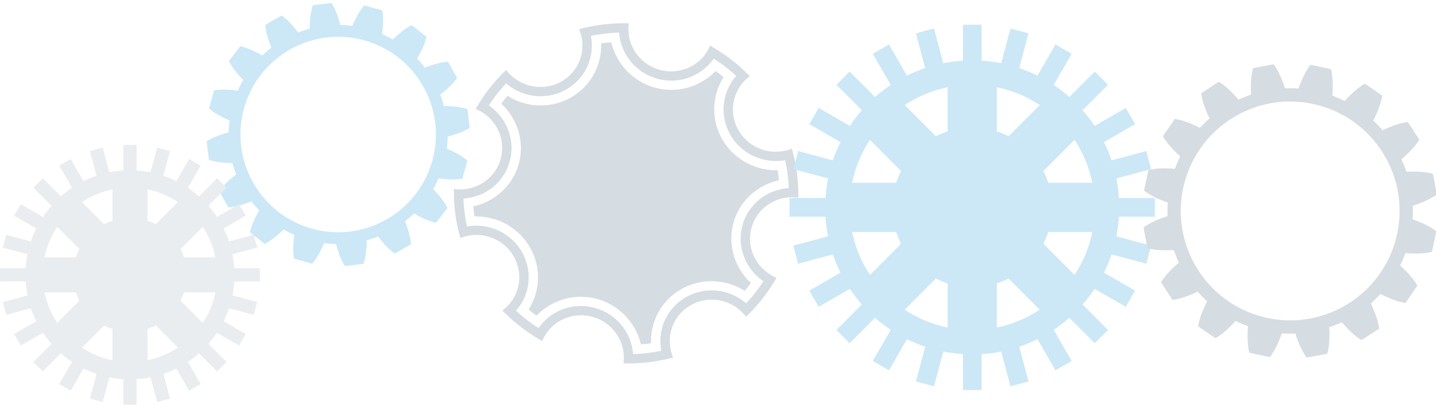
The strategic team focuses on strategic issues that impact the organization's core objectives, and products and services and is usually led by top management. The strategic team is often called a crisis management team and has primary responsibility for addressing any crisis impacting the organization. As these are unpredictable events that have a high level of uncertainty, they require a flexible and creative response by experienced managers with the authority to apply the organization's full resources to the response. This includes crises that may not disrupt the organization's ability to deliver products and services, such as events that can damage an organization's reputation. For this reason, strategic plans commonly include communication plans and media response plans.

The strategic team may also provide command and control guidance during less severe incidents and provide communications support to tactical and operational teams.

The tactical teams manage and coordinate the continuity of the processes required to deliver the impacted products and services, and ensure that the resources are allocated appropriately. Tactical teams are often responsible for the assessment and management of the medium and short term effects of an incident. Tactical level plans provide a framework to coordinate strategic goals and decisions with the operational response teams.

The operational teams focus on the continuity of the activities that contribute to the process or processes that deliver the prioritised products and services. Operational teams deal with the immediate effects of an incident by containing it where possible and managing the direct consequences. An operational response establishes the necessary capability required to continue to deliver prioritised products and services.

In some organizations, one or more of the levels may be combined into a single team, for example a combined tactical and operational team.



Process

Each organization should develop a response structure that meets the requirements of the business continuity policy and supports the agreed continuity solutions. The key steps when establishing a response structure are as follows:

1. Identify, understand, and work within the organization's existing management and leadership structure.

2. Identify the responsible individuals and roles in any existing response teams or plans.

3. Understand the requirements and scope of the business continuity programme.

4. Consider the continuity solutions agreed in the Design stage of the business continuity management lifecycle.

5. Develop a draft response structure.

6. Present the response structure to top management and seek feedback.

7. Update the response structure based on top management feedback.

8. Obtain top management approval for the updated response structure.

9. Document and publish the approved response structure.

10. Implement the approved response structure in any existing business continuity plans.

11. Rehearse the response structure as part of business continuity exercising.

In some organizations, response plans may have been developed and implemented before the introduction of business continuity. In this case, the teams and roles that are responsible for implementing the existing plans should be incorporated into the response structure.

Methods and Techniques

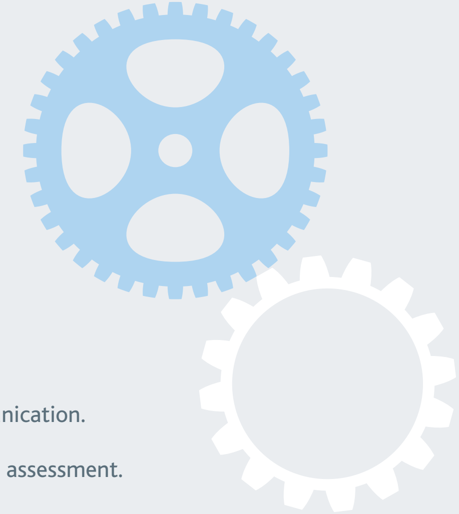
The response structure needs to include all teams and individuals that are identified in the organization's business continuity policy and programme. These teams and individuals should cover all aspects of emergency response, business continuity management, and crisis management. The response structure should consider which of these teams and individuals are competent to undertake the strategic, tactical, and operational roles.

The following should be considered:

- The existing management structure.
- The skills, competencies, and authorities of response teams and individuals.
- The communication channels and escalation process.
- The organization's size, complexity, and type, as well as process infrastructure.
- The agreed continuity solutions.

The responsibilities of the individuals and teams identified in the response structure should be documented and include:

- Team mobilisation.
- Procedure escalation.
- Plan activation.
- Command and control.
- Resource allocation.
- Cost management.
- Personnel welfare.
- Interested party communication.
- Incident monitoring and assessment.
- Changing priorities as the situation evolves.



The required competencies and skills should be identified and the appropriate training and awareness provided for those individuals with roles and responsibilities.

The strategic, tactical, and operational response levels provide a general model for all organizations, but need to be implemented in a way that fits the organization's size, complexity, and type. The table below shows how the levels might be implemented in different types of organization:

Table 11.

Strategic	Tactical	Operational
Small, single site organization In a small, single site organization, all levels of response may be implemented by one response team within a single plan, covering all aspects of the organization's response.		
Medium sized organization In a medium sized organization, the levels of response might be implemented as follows:		
A crisis management plan with a response team consisting of top management.	A single plan covering the continuity of all of the organization's operations, with a response team consisting of the functional leaders or heads of departments.	Usually covered by the tactical plan, except for ICT which, because of the technical detail required, has its own ICT service continuity plan with a technical ICT recovery team.
Large organization In a large organization, the levels of response might be implemented as follows:		
A crisis management plan with a response team consisting of top management.	Several plans, each one covering a division, product, service, or location, each with its own response team consisting of either the division head, or product or service heads responsible for the areas covered by the plan.	Usually covered by the individual tactical plans. Exceptions are the main support functions of human resources, ICT, finance, and sites or facilities. Each of these has its own specialist response team.

Table 11. cont...

Strategic	Tactical	Operational
Large multinational organization In a large multinational organization, the levels of response might be implemented as follows:		
A global crisis management plan, with a response team consisting of top management with global responsibilities, and an incident management plan for each territory, with a response team consisting of top management from those territories. Multinational organizations may also have another level of strategic plan focused on regions.	Each region or country could have several plans, each covering a major division, product, or service, with its own response team consisting of the functional leaders or divisions, or product or service heads responsible for the areas covered by the plan.	Each department or location covered by the business continuity plan may have its own detailed operational plan, with its own response team consisting of the operational managers of the department or location.

Business continuity professionals should apply a combination of general business experience, knowledge of the organization, and business continuity expertise to find the most suitable response structure for their organization. Feedback from various plan users and analysis of exercise results can also assist in further improving the response structure as part of the ongoing validation process, as described in PP6.

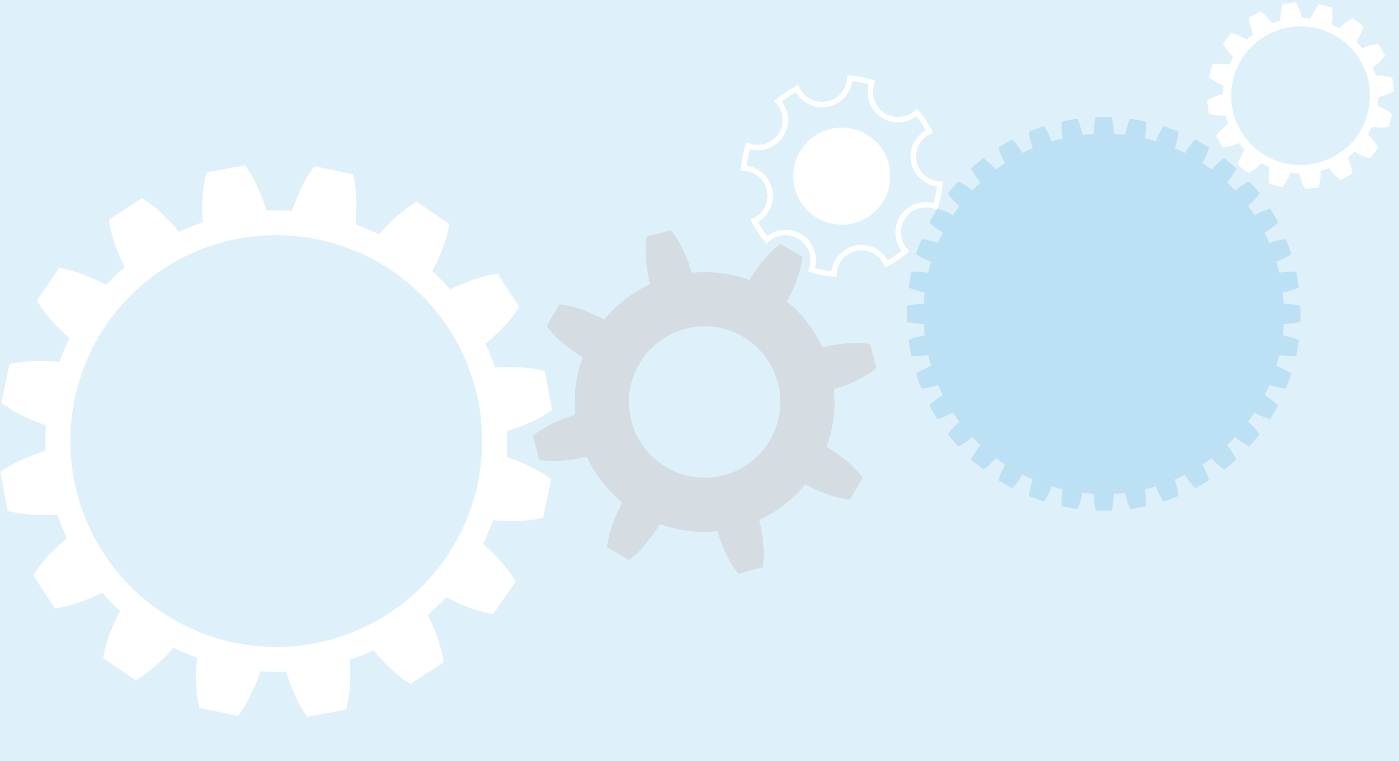
Outcomes and Review

The outcome from establishing a response structure is an organization that has the capability to implement an effective response to a disruption. The response structure should define:

- The required number and type of individuals or teams.
- The relationships between the individuals and teams.
- The roles and responsibilities of the individuals and teams.
- The documented plans required to support the response.

The response structure is necessary to support the development of the detailed response plans which should document how to implement the organization's continuity solutions.

The response structure should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.



Developing and Managing Plans

The term 'business continuity plan' is defined as "documented procedures that guide organizations to respond, recover, resume, and restore to a predefined level of operation following disruption." (Source: ISO 22301:2012)

Business continuity plans can be created to address the strategic, tactical, and operational requirements of an organization. The number and type of plans to be put in place should be determined by the response structure and the business continuity solutions agreed in the Design stage of the lifecycle. This should reflect the existing management structure as well as the size, complexity, and type of organization.

General Principles

Plans are intended to be used in high pressure, time limited situations. A user-friendly plan should be concise and easy to read. Plans are not reports and should not contain unnecessary information that is not needed during an incident.

To make the plan focused, specific and easy to use, it should be:

- **Direct;** providing clear, action orientated and time-based direction. It should provide quick access to vital information.
- **Adaptable;** enabling the organization to respond to a wide range of incidents, including those that the organization may not have anticipated.
- **Concise;** containing only guidance, information and tools that are likely to be used by the team in an incident. Anything else is unnecessary.
- **Relevant;** providing information that is current and useful to the team using the plan.

The business continuity plan should be kept up to date and be documented in a way that enables personnel to quickly access the information relevant to them.

Plans should be owned, coordinated, and maintained appropriately.

Concepts and Assumptions

Plans at all levels should contain the following:

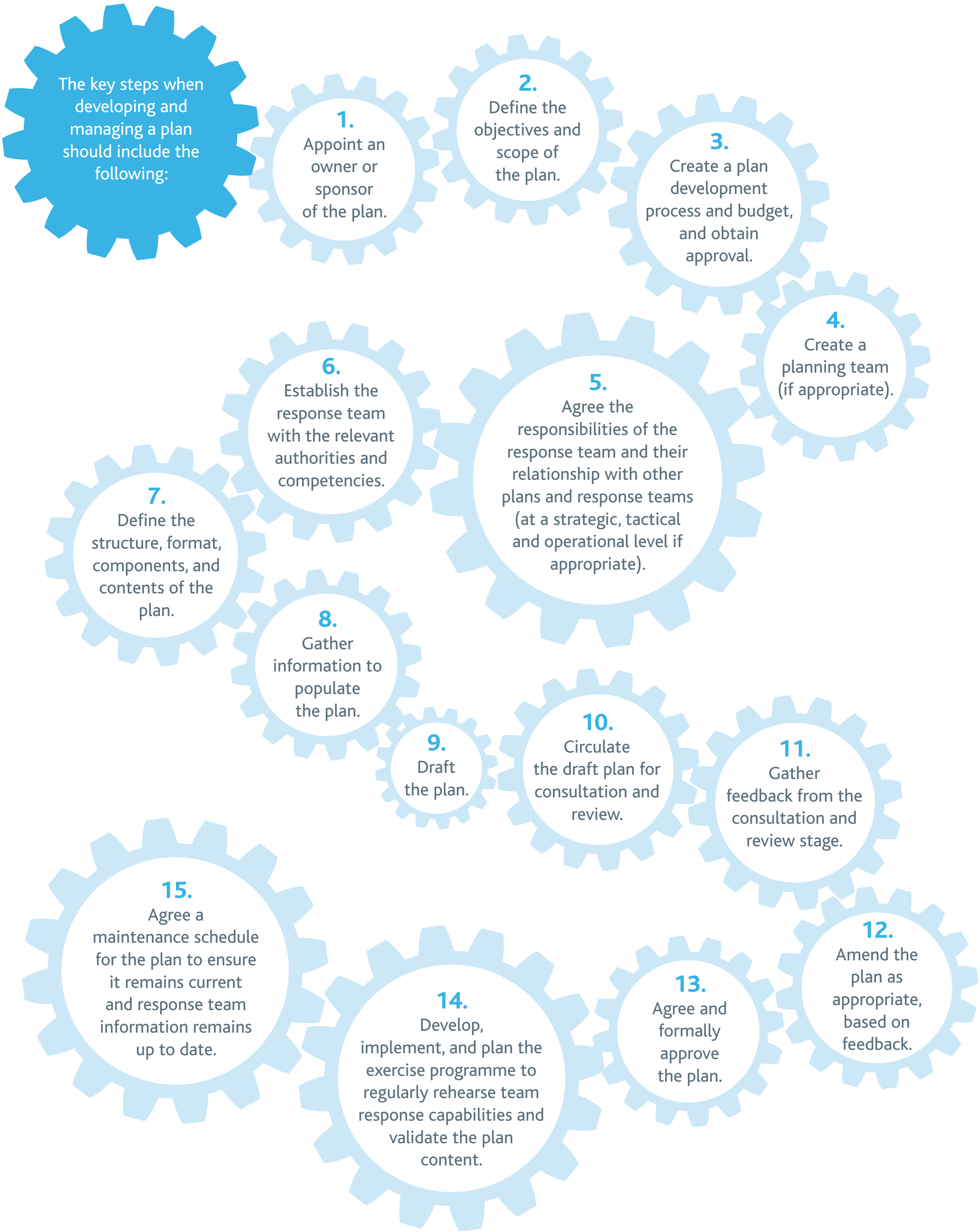
- Purpose and scope.
- Objectives and assumptions.
- The response structure which is specific to the organization.
- Plan activation criteria, procedures, and authorisation, including implementation procedures:
    - Invocation of continuity solutions.
    - Team mobilisation instructions.
- Response team roles and responsibilities (with alternates as appropriate).
- Individual responsibilities and authorities of team members.
- Prompts for immediate action and any specific decisions the team(s) may need to make, for example, whether to activate an alternate site.
- Communication requirements and procedures concerning relevant interested parties, for example, personnel, suppliers, customers, and the media.
- Internal and external interdependencies and interactions, including contact details (usually held as appendices).
- Summary information (at a level of detail appropriate to the plan) of the organization's prioritised activities and resource requirements as identified in the Analysis stage of the business continuity management lifecycle, with reference to the continuity time frames within which they are required.
- Assumptions defining the limitations of the plan relating to extent, duration, or impact of the incident.
- Decision support checklists.
- Details of meeting locations.
- Information flow and documentation processes.
- Procedures for standing down the team and organization once the incident has been resolved.
- Appendices with relevant information capture templates, for example, an action log.
- Plan approval and distribution information.

Tactical and operational level plans may contain information about procedures which can only be developed after the continuity solutions have been agreed in the Design stage.

By contrast, the strategic level plan does not usually contain such detailed procedural information. As a result, they can be implemented at the start of the business continuity process to provide an initial response capability before the other plans are developed.

Whichever type of plan is being developed, it should not be done in isolation. To achieve a successful outcome, it is essential to involve users of the plans, including top management, in the development and implementation process.

Process



The key steps when developing and managing a plan should include the following:

1. Appoint an owner or sponsor of the plan.

2. Define the objectives and scope of the plan.

3. Create a plan development process and budget, and obtain approval.

4. Create a planning team (if appropriate).

5. Agree the responsibilities of the response team and their relationship with other plans and response teams (at a strategic, tactical and operational level if appropriate).

6. Establish the response team with the relevant authorities and competencies.

7. Define the structure, format, components, and contents of the plan.

8. Gather information to populate the plan.

9. Draft the plan.

10. Circulate the draft plan for consultation and review.

11. Gather feedback from the consultation and review stage.

12. Amend the plan as appropriate, based on feedback.

13. Agree and formally approve the plan.

14. Develop, implement, and plan the exercise programme to regularly rehearse team response capabilities and validate the plan content.

15. Agree a maintenance schedule for the plan to ensure it remains current and response team information remains up to date.

Methods and Techniques

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

Plan Management

Although some plans may be owned by specific departments, they are part of the organization's overall business continuity programme. Copies of all business continuity documents should be stored and maintained centrally to facilitate supervision of the scheduled plan review and maintenance.

All plans should be held in known and secure locations that are accessible to all team members. If plans are held electronically, the organization should ensure that they are also available in hard copy during a disruption.

Roles and Responsibilities

The personnel nominated to be members of the response team should have the necessary authority and capability to respond to an incident at the appropriate level. Alternates should be identified for each role.

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

- The team leader who ensures that the response team is activated, briefed, and properly staffed. They can nominate team members if necessary.
- People and welfare.
- Internal communication to establish and maintain contact with personnel and other response teams.
- External communication to establish and maintain contact with interested parties outside the organization, which may include the media.
- Operations, including finance.
- Technical support for example, ICT and facilities.
- Administrative support, including a record keeper to maintain a log of incoming information, decisions made and actions carried out throughout the incident.

Plans should clearly state which members have responsibility or authority for key decisions or actions, however, these procedures should also be flexible and adaptable to allow for the absence of one or more team members.

Activation and Mobilisation

The plan should document the conditions or circumstances under which the plan should be activated and the team mobilised.

Not all incidents happen suddenly. Some escalate at a slower pace before they are recognised as an incident.

For example, threats of industrial action, medical issues, and supply chain disruption or shortages due to environmental or economic impacts.

Consequently, the plan should include information about unacceptable disruption levels. This information can support incident assessment and enable timely decision making and escalation by appropriate members of the organization.

Disruption levels, or impact thresholds used in plans should be directly related to the organization's prioritised products and services and based on measures that relate to the business continuity requirements. For example:

Disruption impacting more than **(x)*** customers or users for more than **(x)*** hours or days.

Disruption to the organization's prioritised activities lasting for more than **(x)*** hours or days.

Disruption impacting the organization's prioritised ICT systems and data for more than **(x)*** hours or days.

Disruption impacting a key outsourced service provider for more than **(x)*** hours or days.

To be effective, the measures should be based on information that is likely to be easy to identify and readily available in the early stages after a disruption occurs.

Additional measures of the level of disruption that support incident assessment may be more difficult to quantify, for example, adverse impacts on:

- Personnel and other interested parties.
- The environment.
- The reputation of the organization.
- Compliance with legal or regulatory obligations.

***The organization should determine the disruption levels or impact thresholds as appropriate.**

The disruption levels or impact thresholds should be implemented in the strategic, tactical, and operational plans, so that the organization has a consistent approach to identification, assessment, and escalation of threats and incidents.

However, the strategic, tactical, and operational response teams may not always invoke their plans simultaneously. Activation may start at the operational level and escalate to the strategic level. Alternatively, activation may start at the strategic level and cascade down to the operational teams.

Plans should clearly state which members have authority to declare an incident or crisis and mobilise the team. The guidelines should be clear and direct and promote action by the team even though there may be uncertainty about the incident. It is easier to stand a team down than to mobilise it after the incident has developed beyond the organization's capability to respond effectively.

Automated notification systems can help organizations to contact and communicate with large numbers of personnel, especially in the early stages of an incident.

As the organization starts to recover from an incident and resume its operations, the disruption levels or impact thresholds can be used to decide when to declare the incident as 'resolved'. It is important that the stand down procedure is implemented at all levels, leading to a formal declaration that the incident has ended.

People Welfare

Organizations have a responsibility to safeguard the health, safety and welfare of their personnel, contractors, visitors, and customers (this is a legal requirement in some industry sectors). The business continuity plan should address personnel and welfare issues. The organization's personnel are more likely to support the extra demands placed on them in an incident if their welfare needs are met.

The issues listed below should be included in a dedicated welfare plan, or be incorporated in the body of a more general business continuity 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 help line or intranet pages.
- Contacting next of kin.
- Arranging transport assistance.

Subsequently there may be additional needs to consider, including:

- Dealing with issues relating to casualties, in consultation with the emergency services and in accordance with local regulations and customs.
- Counselling and rehabilitation services (which may be provided as part of existing personnel benefits).
- Liaison with specialist services when dealing with next of kin.
- Family support (especially where families have been affected by the incident).
- Temporary accommodation.
- Translation services.
- Access to emergency cash or facilities.
- Welfare needs at alternate locations:
    - Personal safety and security.
    - Special needs.
    - Transport and accessibility.
    - Appropriate training on replacement equipment.
    - Toilet and washing facilities.
    - Refreshments.

Team Meeting Facilities

To save time and avoid confusion during an incident, each team should know in advance the details of available meeting locations (also known as a command centre). It should also be understood which team members can decide on the most suitable meeting place based on the available information about the incident. Depending on the type of the incident, the team may work together in one place or meet periodically throughout the day.

At least two locations or options should be predefined. One should be on-site or close to the site where the response team is based with the other being at a more remote off-site location.

The off-site physical location does not have to be owned by the organization. By prior arrangement, a location that provides secure, 24-hour access, such as a hotel or serviced office may provide the required resources.

For large scale incidents or multisite organizations, a virtual incident response team with a virtual command centre may be more appropriate. An effective virtual command centre requires reliable communications capability and real time access to information by all team members.

Consideration should be given to how the following will be facilitated:

- Incoming and outgoing communication.
- Recording of incident events, team decisions, actions, and issues.
- Monitoring public information about the incident.
- Physical and information security.

The availability of the following resources should also be considered when setting up a meeting room:

- A continuously available and stable power supply.
- An appropriate number of landline telephones, as well as teleconference equipment and voice recording facilities.
- A computer and printer.
- Cell phones and mobile communicators with chargers.
- Secure access to email, internet, and fax.
- Printed copies of relevant plans and urgently required information.
- A supply of log sheet templates.
- Whiteboard/flip charts and pens for recording incident details along with actions taken and decisions made by the team.
- Access to:
    - Stationery.
    - Television and radio equipment.
    - Refreshments.
    - Transport.
    - Sleeping facilities on-site or nearby.
    - Toilet and washing facilities.

Some of the smaller meeting room equipment and resources can be stored in a 'battle box' or 'recovery box' that is kept on-site, or in a secure accessible off-site location.

Strategic Plans

A strategic level, or crisis management plan is a high level plan that defines how strategic issues resulting from a crisis or incident should be addressed and managed by top management. It has some special characteristics which differentiate the document from the tactical and operational plans.

Some crises or incidents do not involve physical disruption to the organization and may not require invocation of a business continuity plan, however, they still require a strategic level response, for example, fraud or negative media exposure that threatens the organization's reputation.

This type of incident may result in the mobilisation of the teams with responsibility for managing the area of the business affected and the potential reputational damage. In these situations, it is almost always necessary to involve the strategic level team, if only to make them aware of the situation in case it escalates.

General Principles

A strategic level plan should provide high level information and guidelines to support top management or the crisis management team. It should address strategic issues that impact the organization's core objectives, and its prioritised products and services.

The strategic-level plan should also address the need to communicate with, and control activity between, all involved, or impacted interested parties. The content of a strategic level plan should be relevant to the size, complexity, and type of organization.

The strategic plan should be designed as a high level, generic plan. It should contain summary information on different parts of the organization and generic organization-wide response procedures. The aim is not to encourage micro-management of an incident but to provide the strategic team with summary information to assist assessment and decision making.

Concepts and Assumptions

During a crisis or incident, the strategic level team are accountable for the organization's stability, continuity, and reputation. They are responsible for implementing and adapting response activities to achieve the best possible outcome for the organization. **Specific responsibilities of the strategic level team that should be captured in the plan include:**

- Establishing the strategic objectives of the crisis or incident response.
- Devising short, medium, and long-term strategies, depending on the type of crisis or incident.
- Managing communications with all involved interested parties, including the media.
- Approving external statements before they are issued and monitoring and adjusting the communications strategy, as necessary.
- Monitoring the overall response to the crisis or incident.
- Resolving implementation issues or resource conflicts during the response.
- Ensuring the response and recovery is in line with the long term objectives of the organization and meets the organization's legal and regulatory requirements.
- Identifying and maximising opportunities or advantages arising from the crisis or incident.
- Approving significant expenditure.
- Monitoring the financial health of the organization.
- Identifying and declaring when the incident or crisis is over, directing the individuals and teams to stand down, and clearly communicating the end of the incident or crisis to all interested parties.

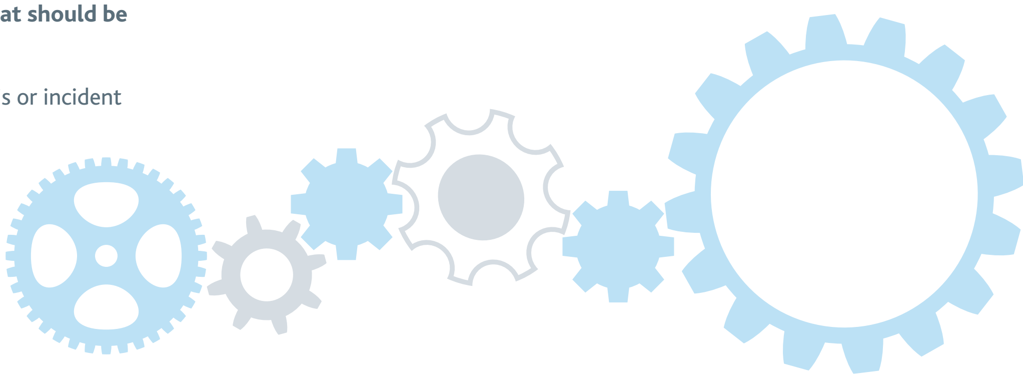
Communication and Media Liaison

The communication response during a crisis or incident is usually guided by top management, working with specialist communication teams within the organization.

Depending on the organization's response structure, there may be a separate communication plan or it may be included as part of the strategic plan.

The communication plan should:

- Address how communications should be managed with internal and external interested parties.
- Identify these internal and external interested parties, record their contact details and where possible, define each group's communication requirements or expectations.
- Define the available methods and channels for communicating with each interested party, for example, social media, email, radio, and newspapers.



- Include a selection of communication methods and channels, so that the team can guarantee availability of at least one method or channel.
- Identify the group or individual in the organization who has the responsibility, authority, and technical knowledge to deliver communications via each of the available methods and channels. Where possible, existing methods should be used to communicate with interested parties.
- Decide in advance who the organization's spokesperson should be and then ensure that:
    - The spokesperson has been trained in their role and is available at the location or can get there at short notice during an incident or crisis.
    - The process to create and issue media statements is known, including how they should be approved internally prior to release.
    - There are individuals available to brief the media at a central location as well as representatives who can be on-site of a local incident or crisis.
    - There is a designated technology proficient spokesperson if appropriate.
- Assign responsibility for monitoring and reviewing the interested party response to communications to assess and adjust as required.

The organization may choose to work with specialists such as public relations organizations to develop the media response. Some organizations may also benefit from developing relationships with key media organizations.

The volume, type, and urgency of communications after an incident can vary significantly. The communications plan can accelerate the response if it includes pre-formatted messages or pre-written statements. The communication plan can:

- 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 or crises.
- Contain a general background statement about the organization which can be distributed in public statements.
- Include development of a website or web pages which can be activated during an incident or crisis and be used as a focus point to communicate specific and relevant information.

Media Liaison

The strategic level plan should address how the organization manages communication with the media. The strategic plan should ensure that only appropriately trained personnel liaise with the media and communicate with interested parties.

All plans should include instructions for personnel on what they should do if approached by the media during an incident or crisis.

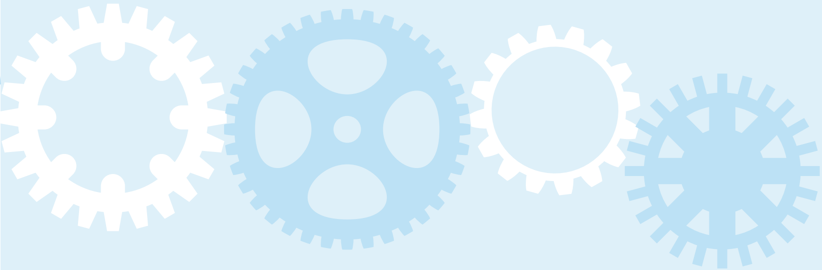
Plans should also contain information on what actions the organization's personnel should take if they are involved in an incident which has, or is likely to attract media attention, and who they should escalate media attention to.

Outcomes and Review

The outcomes of developing the strategic level business continuity plan include:

- A plan that can support top management during an incident or crisis.
- A plan for managing interested parties and media communications during an incident or crisis.
- Documented evidence of the organization's preparedness which is available to interested parties.
- A plan that complies with legal and regulatory requirements.

The strategic level plan should be regularly reviewed in line with the tactical and operational-level plan reviews at pre-agreed intervals or following significant change as defined within the business continuity policy.



Tactical Plans

Tactical level plans focus on coordinating the response to an incident and facilitating the continuity of prioritised activities. Tactical plans should provide guidelines to help the tactical team analyse the impact of the incident, implement the appropriate solutions from those available in the plans, ensure the continuity of prioritised activities, and provide progress updates to the strategic team.

General Principles

The tactical plans should be based upon the agreed business continuity solutions and address the incident response from the initial alert, to the point at which disrupted activities are restored. The tactical plan should focus on coordinating the activities of the involved response teams to ensure they work together effectively. Where resources are limited, the tactical plan should provide information to help the tactical team allocate available resources to the prioritised activities identified in the Analysis stage.

> Where there are multiple operational level plans, one of the roles of the tactical response team is to prioritise response activities to ensure that the response remains focused and is coordinated. The tactical response team may alter the agreed priorities and business continuity solutions if directed by top management.

Concepts and Assumptions

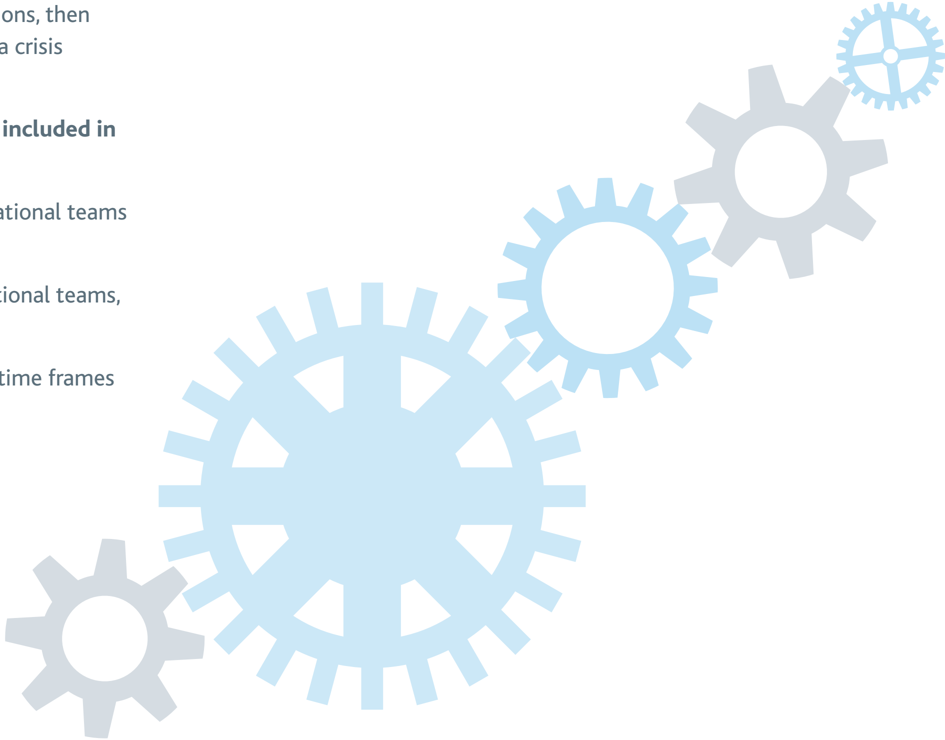
Tactical plans should contain assumptions relating to the scale of the incident in terms of extent, duration, and operational or personnel impact. If the scale of the incident exceeds the assumptions, then this should be escalated to the strategic level team and a crisis management response should be considered.

Specific responsibilities of the response teams to be included in the tactical plans include:

- Coordinating and monitoring the response of the operational teams involved in the incident.
- Monitoring the support services provided to the operational teams, such as ICT, human resources, facilities, and finance.
- Allocating available resources based on quantities and time frames agreed in the Analysis stage.
- Amending the agreed priorities and response actions to take into account the current situation, business conditions or based on direction from the strategic level team.
- Requesting or receiving progress updates and other information from the operational teams.
- Reporting to the strategic level team.
- Mobilising specialist service providers, for example, damage management or salvage companies, data recovery, or counselling services, as required.
- Ensuring the individuals and teams stand down when directed.

The tactical plan should include detailed information about the resources required by the organization, the time frames and quantities in which they are needed, and how they are sourced (as identified in the Analysis stage). Relevant resources may include:

- Personnel.
- Welfare services.
- Alternate locations.
- Security services.
- Technology, communications, and data.
- Transportation and logistics.
- Alternate suppliers of priority services.
- Contact information to access those resources.
- Resource requirements for the continuity of each prioritised activity.



Other details to be included in the tactical plan might include:

- Organization contact information.
- Key interested party information and contact details, including customers, clients, and service providers.
- Secure location of legal documents, for example, contracts, service level agreements and insurance policies.
- Details of contracted work area recovery space, and how and when it will be made available to response teams.
- Procedures for obtaining emergency funds.

Suppliers and business partners

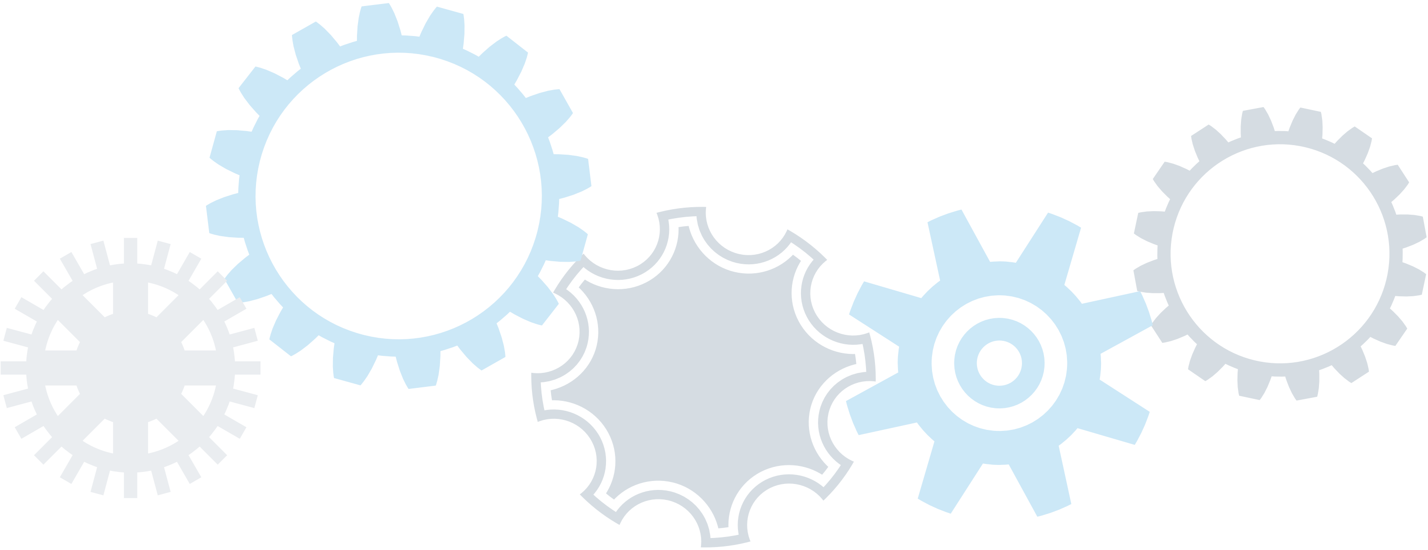
Tactical plans should consider aspects of the business continuity solution that may involve prioritised activities and resources available outside the organization. The plan should consider key suppliers to the organization's supply chain and other business partners who are able to support the continuity solution and response activities.

If a proposed solution relies on access to resources from an outsourced service provider, it is important that a service level agreement is in place for the arrangement and that the arrangement is reviewed and validated in line with the tactical plan review process. It is important that such arrangements are included the exercise programme.

Emergency services liaison

If the organization is responsible for its own site or premises, personnel with an appropriate level of capability and authority should be appointed to liaise with emergency services throughout the incident or crisis. As the tactical team has a central coordinating role, this emergency services liaison role is often assigned to this team.

During an incident, the emergency services will require information on the location of any casualties, the current status of the incident or crisis, and any known hazards they may encounter. They may also need access to a dedicated contact person from the organization to update and obtain further information from.



Outcomes and Review

The outcomes of developing the tactical level business continuity plan include:

- Documented business continuity plans to support tactical teams during an incident or crisis.
- A framework for coordination of response activities and resource allocation between the strategic and operational teams.
- Guidelines for coordinating continuity solutions and response activities with interested parties.

The tactical level business continuity plan should be regularly reviewed in line with the strategic and operational-level plan reviews at pre-agreed intervals or following significant change as defined within the business continuity policy.

Operational Plans

Operational level plans determine the individual departments or business units involved in the incident response. Lower level plans are likely to become complicated if all continuity procedures for an organization are included in a single document. When this is the case, the response procedures of each business unit may be separated into one or more plans that each become the responsibility of the related business unit.

General Principles

Operational level plans should support the continuity of the organization's prioritised activities, from the beginning of the incident through to the recovery of agreed levels of service and the return to business as usual. They should be based on the agreed continuity solutions and the resource requirements identified in the Analysis stage of the lifecycle.

Operational level plans should include departments that manage the organization's infrastructure, for example, ICT services and other specialist services that support the organization during an incident. These operational level plans provide a structure for restoring key support services or providing alternate facilities that support the continuity of other departments.

Concepts and Assumptions

The complexity and prioritisation of the organization's products, services and processes should determine whether one departmental plan can cover several activities or if an operational plan is needed to cover a single activity in detail. If required, these more detailed plans may contain information and response procedures for specific locations, systems, or equipment.

Business continuity professionals should carefully consider the organization's need for detailed operational plans before they are produced. Situations where detailed plans are beneficial include:

- Where manual workaround procedures are to be used as a continuity solution for partially or fully automated procedures.
- Where alternate ICT systems or processing equipment are to be used in place of disrupted ICT systems or unavailable equipment.
- Where the personnel responsible for implementing the continuity solutions are likely to be unfamiliar with the procedures they have to follow, or the systems and equipment they have to use.

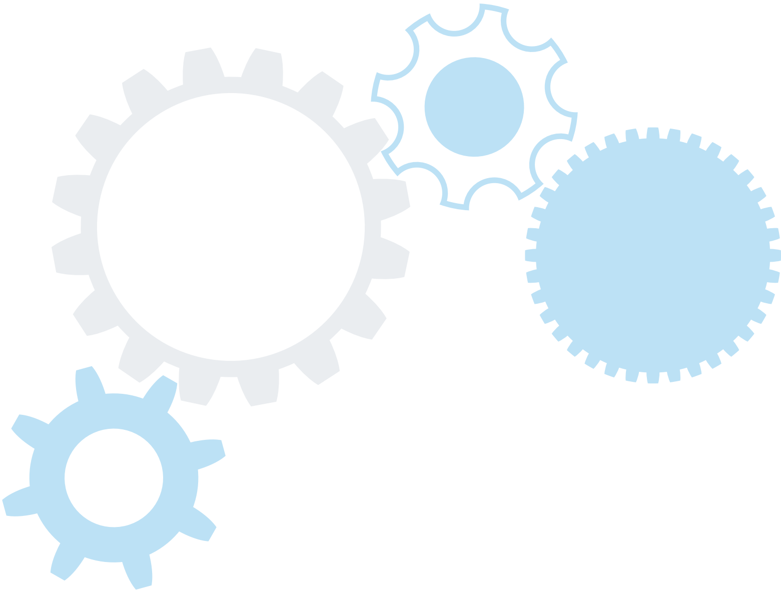
Examples of operational level plans include:

- A department or business unit plan.
- Specific procedures implemented in response to an incident, such as equipment salvage and document restoration.
- An ICT department's response to the loss and subsequent recovery of ICT applications and services.

Because of the links between the tactical and operational plans, the tactical plans should be written, at least in outline, before the operational plans are finalised.

Development of operational plans should consider the following:

- Appointing a representative within each business unit to develop their plan.
- Developing a planning process and scheduled programme. Where possible, begin with the plans for the highest priority activities.
- Using a plan template to encourage standardisation of documentation but allowing variations where appropriate.
- Documenting communication and information interdependencies between the tactical and operational level plans, for example, where an operational team relies on a tactical team for a key decision or approval to proceed with a response procedure.
- Ensuring business units nominate competent individuals to fulfil key roles within their plans.
- Circulating the draft plan for consultation with members of each business unit for review and feedback.
- Circulating the draft plan outside the business unit (if appropriate).



Methods and Techniques

Operational level plans may include a wide variety of detailed information regarding:

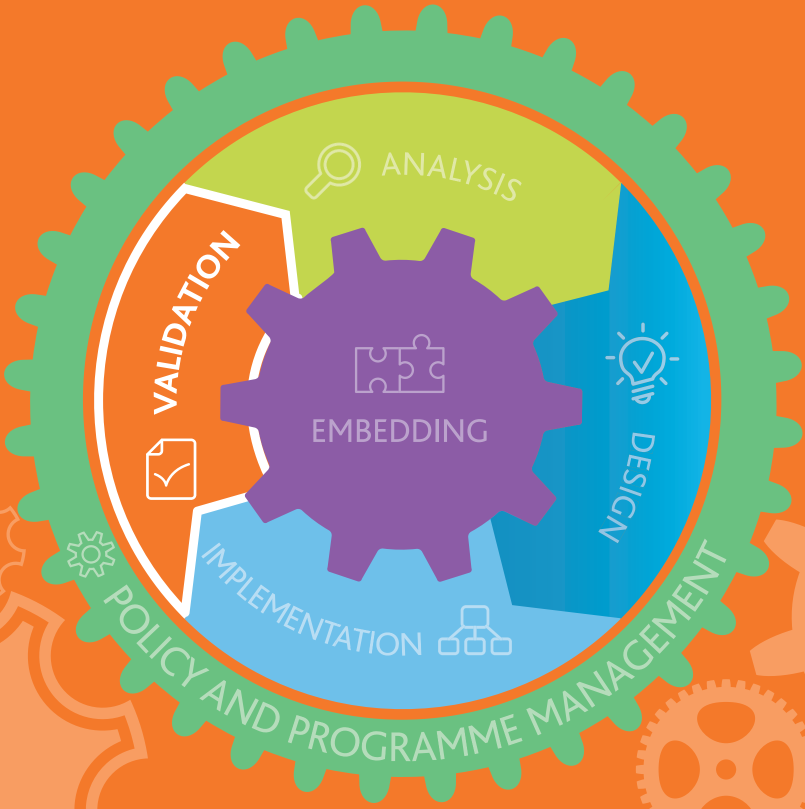
- Human resources and people welfare.
- Access to, and use of facilities.
- Departmental activities (listed in order of priority).
- Liaison with ICT service continuity teams.
- Mobilisation of teams and allocation of resources.
- External support.
- Building evacuation and shelter-in-place procedures.
- Location and layout of evacuation points.
- Security.
- Accounting for personnel.
- Health and safety.
- Escalation procedures to advise top management about unexpected issues.
- Initial response and activation.
- Methods to contact team members.
- Resolving work in progress issues.
- Special or non-standard procedures.
- Redeployment of personnel and visitors.
- Personnel contact numbers.
- Other key interested party contacts.
- Communications with personnel following plan activation.
- Space, seating, and resource requirements.
- A list of ICT equipment and software required.
- Details of off-site data with document storage and access instructions.
- Restoration instructions that a technical person unfamiliar with the system(s) can use.
- Salvage arrangements and contracted assistance.
- Stand down procedures.
- Counselling and rehabilitation resources.

Outcomes and Review

The outcomes of developing the operational plan include:

- Documented business continuity plans to support the continuity of prioritised activities by department following an incident.
- Documented business continuity plans for the continuity of the organization's infrastructure and other specialist support services.

The operational level business continuity plan should be regularly reviewed in line with the strategic and tactical-level plan reviews at pre-agreed intervals or following significant change as defined within the business continuity policy.


ANALYSIS
DESIGN
IMPLEMENTATION
VALIDATION
EMBEDDING
POLICY AND PROGRAMME MANAGEMENT

BCI Professional Practices

PP6

Validation

Validation is the Professional Practice within the business continuity management lifecycle that confirms that the business continuity programme meets the objectives set in the policy and that the plans and procedures in place are effective.

The purpose of Validation is to ensure that the business continuity solutions and response structure reflects the size, complexity, and type of the organization and that the plans are current, accurate, effective, and complete. There should be a process in place to continually improve the overall level of organizational resilience.

Introduction

Validation is achieved through a combination of the following three activities:

- **Exercising:** A process to train for, test, assess, practise, and improve the business continuity capability of the organization.
- **Maintenance:** A process to ensure that the organization's business continuity arrangements and plans are kept relevant, up-to-date, and operationally ready to respond.
- **Review:** A process for assessing the suitability, adequacy, and effectiveness of the business continuity programme and identifying opportunities for improvement.

Developing an Exercise Programme

An organization's continuity capability cannot be considered reliable or effective until it has been exercised. No matter how well designed a business continuity solution or business continuity plan appears to be, realistic exercises should be used to help identify issues and validate assumptions that may require attention. The goal of exercising is the continuous improvement of business continuity management capabilities and readiness by ensuring that lessons learned are integrated into prevention, mitigation, planning, training, and future exercising activities.

General Principles

Exercising aims to achieve various outcomes, including:

- Evaluating the organization's capability to undertake continuity activities and achieve the expected RTOs.
- Validating the business continuity solutions and the assumptions on which they are based.
- Verifying that the documented procedures in the business continuity plan are relevant, complete, and current.
- Verifying the adequacy and practicality of resources that support the continuity solutions.
- Identifying areas for improvement or missing information.
- Validating competency and building confidence in personnel with relevant roles and responsibilities.
- Developing team work.
- Raising awareness of business continuity throughout the organization as described in PP2.

Exercising is not a one-time activity. It should be scheduled and programmed into a series of events and activities that allow the organization to gradually improve capability over time. An exercise programme should ensure the desired level of capability by:

- Rehearsing all plans.
- Verifying all business continuity solutions.
- Verifying all information contained in plans.
- Exercising all relevant personnel (including alternates).

The exercise programme should begin with simple activities to raise general levels of awareness and understanding, and escalate gradually in terms of complexity and challenge. The programme should use a combination of exercising methods and techniques to ensure that the planned outcomes are achieved across the whole organization over the duration of the programme.

The exercise programme should include suitable exercising of the following elements:

- **Technical:** Do all the required systems and equipment work?
- **Procedures:** Are the procedures and plans correct?
- **Logical:** Do the procedures work together in a logical manner?
- **Timeliness:** Can the procedures achieve the required recovery time objective for each activity?
- **Administrative:** Are the procedures manageable?
- **Personnel:** Are the most suitable individuals involved and do they have the required competencies, skills, authority, and experience? Does everyone know their role and responsibility?
- **Resources:** Are the right resources identified in appropriate quantities from known and reliable sources?
- **Information:** Is all necessary information available to implement the plan?

The frequency of exercising is determined by the exercise schedule in the business continuity programme and may be influenced by the size, complexity, and type of organization.

Prioritised products and services, processes and activities, and every member of the organization's incident response teams should be involved in exercises in line with the planned exercise schedule.

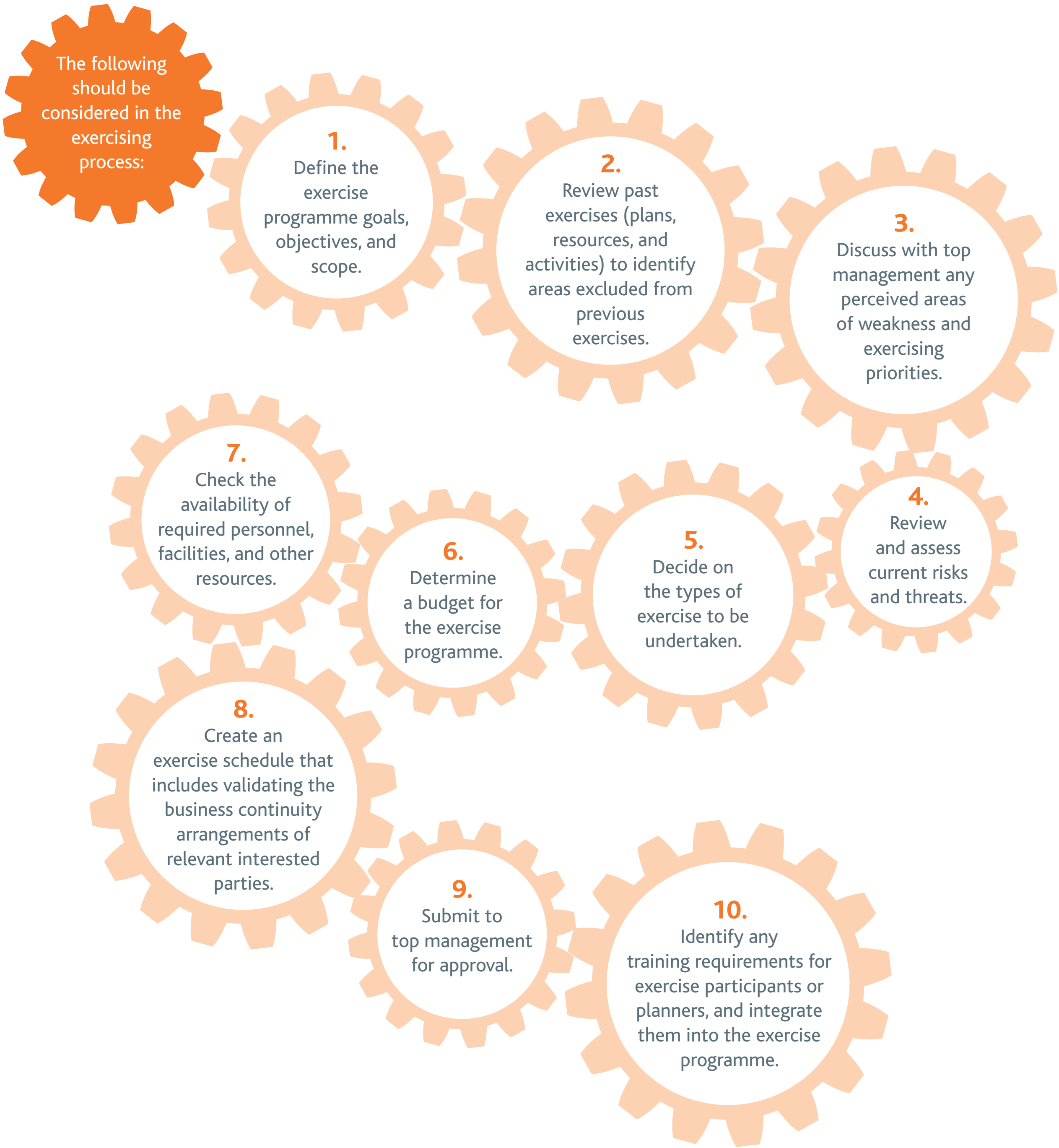
Concepts and Assumptions

The organization's business continuity policy and programme establishes how the exercise programme is to be planned and managed, as well as any training to be undertaken and necessary resources to be identified.

An exercise is defined as "a process to train for, assess, practice, and improve performance in an organization." (Source: ISO 22301:2012)

Where the delivery of a product or service has been outsourced, the responsibility for exercising remains with the organization that owns the product or service. The organization should make sure, through exercising, that the outsourced company can continue to meet its obligations in the event of a disruption. 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 of the business continuity management lifecycle, they should be asked to demonstrate their own business continuity capability through their own exercises.

Process



The following should be considered in the exercising process:

1. Define the exercise programme goals, objectives, and scope.

2. Review past exercises (plans, resources, and activities) to identify areas excluded from previous exercises.

3. Discuss with top management any perceived areas of weakness and exercising priorities.

4. Review and assess current risks and threats.

5. Decide on the types of exercise to be undertaken.

6. Determine a budget for the exercise programme.

7. Check the availability of required personnel, facilities, and other resources.

8. Create an exercise schedule that includes validating the business continuity arrangements of relevant interested parties.

9. Submit to top management for approval.

10. Identify any training requirements for exercise participants or planners, and integrate them into the exercise programme.

Methods and Techniques

Types of Exercise

There are many names given to different types of exercises, but in principle they fall into the following five categories. These exercise types have common features, and organizations may find it appropriate to combine elements from different exercise categories to achieve their exercise objectives.

• Discussion-based exercises

These exercises are the simplest to organize and to facilitate and the least time consuming of the exercise types. They are structured events where participants can explore relevant issues and walk through plans in a low pressure environment. This type of exercise can focus on a specific identified area for improvement with the aim of finding a preferred solution.

• Scenario exercises

A scenario exercise is a commonly used discussion based activity, using a relevant scenario with a time frame. The exercise may either run in real time or include time 'jumps' to allow different phases of the scenario to be exercised. A scenario exercise is usually conducted in a tabletop environment. Participants are expected to have some familiarity with the plans being exercised and are required to demonstrate their understanding of how the plans work as the scenario unfolds. They can involve some practical rehearsal of relevant response activities, such as completing assessment checklists or use of log sheets.

Scenario exercises can be a realistic, cost effective and efficient method. This type of exercise can be enhanced using media and other injects which can make a scenario more realistic. Practical outputs such as media releases or employee communications may be produced by the response teams during the exercise.

• Simulation exercises

Simulation exercises are more elaborate and can involve teams at a strategic, tactical, or operational level. Participants can be located across the whole organization, all working from their usual locations. During a simulation exercise, participants are given information in a way that simulates a real incident. Scenario details and questions from interested parties such as personnel, customers and the media can be introduced into the exercise using various platforms, for example, phone calls, emails, social media, and TV news.

The use of roleplay can bring an additional level of reality to the exercise by simulating the interests of key interested parties, for example, customers, personnel, the media, regulators, and suppliers.

The exercise participants are asked to deal with the updates or requests for information as if it were a real incident, and develop and implement a suitable response to the unfolding scenario. Simulation exercises also allow the participants to rehearse relevant procedures in detail, for example, notification and escalation, decision making, communication, media response and team coordination, in addition to testing command centre equipment and other resources required to support the team.

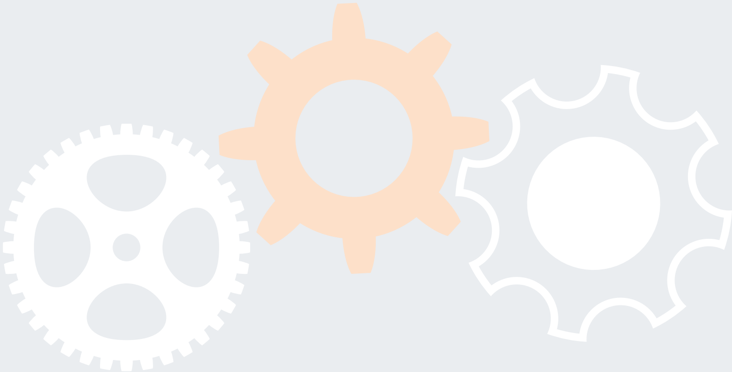
• Live exercises

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 are designed to include everyone likely to be involved in that part of the response.

Live exercises are particularly useful 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 fully evaluated. They are the most realistic way to train individuals and exercise the plans. However, there are several challenges that may mean a live exercise is not the most appropriate exercise format. For example, the resources required can be significant and there may be financial implications. Care should be taken to avoid disruption to the organization's business as usual tasks and any reputational impacts should be considered.

• Test

A test is defined as "a unique type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned." (Source: ISO 22301:2012) It is usually applied to equipment, recovery procedures or technology, rather than teams or individuals. For example, the rebuilding of a server from back-up tapes within a predefined time frame.

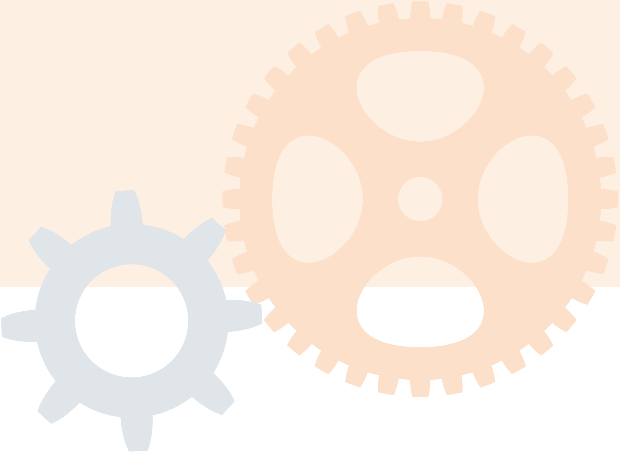


Outcomes and Review

The outcomes of developing an exercise programme are as follows:

- A complete exercise programme which defines:
    - The objectives to be achieved.
    - The methods required to achieve the objectives.
    - Defined resource requirements (including budget).
    - Proposed timing, and training requirements.
- Improved organizational resilience, with a demonstrable capability to respond to, and recover from, an incident or crisis over time.

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



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. The exercise development process should be approached like a project, using the appropriate planning steps and controls associated with good practice in project management.

Concepts and Assumptions

Realism: Exercises should be as realistic as possible. They should be carried out using the same procedures and methods as would be used in a real event. This is the ideal, but it may not be practical to run certain exercises without considering the limitations.

Setting a realistic business scenario helps to ensure that the participants accept and engage fully in the exercise and benefit from the experience. The selection of a realistic scenario should also help prove the validity of plans. It is essential that the person coordinating the exercise works with facts to ensure participants gain the most from the exercise through the realism of the scenario and supporting material.

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

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

The introduction of 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: Exercising should focus on maximising benefits and minimising the impacts of disruption. Exercising can sometimes cause disruption to business as usual activities. Those responsible for planning and managing exercises should ensure:

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

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 business as usual 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 when preparing an exercise is to determine the objectives and outcomes. Criteria should be defined for measuring the effectiveness of the exercise.

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

Examples of measures that can be used during an exercise are as follows:

- Can the appropriate personnel initiate the alert, invocation, and escalation process?
- Can the on-duty manager activate the callout procedure?
- Is the incident manager able to call an initial management meeting?
- Have response team members demonstrated effective decision-making capabilities?
- Have key personnel established and maintained an incident log?
- Can a priority system be recovered and restored within the expected recovery time objective?
- Can a department resume services from the alternate site using the resources available?
- Was the response structure established as defined within the business continuity plan?
- Were roles and responsibilities allocated as per the business continuity plan?
- Were lines of communication established with interested parties?

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

Although it is often appropriate for existing personnel to develop and run exercises, there are other options which can involve the engagement of external parties. For example, the emergency services may be willing to be involved in some types of exercises 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 nominated to run the exercise. This individual or team should manage the exercise in accordance with the exercise plan and schedule, initiating and controlling the various stages as the exercise progresses.

Participants: Those involved in exercises may include:

- Facilitators.
- Umpires.
- 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

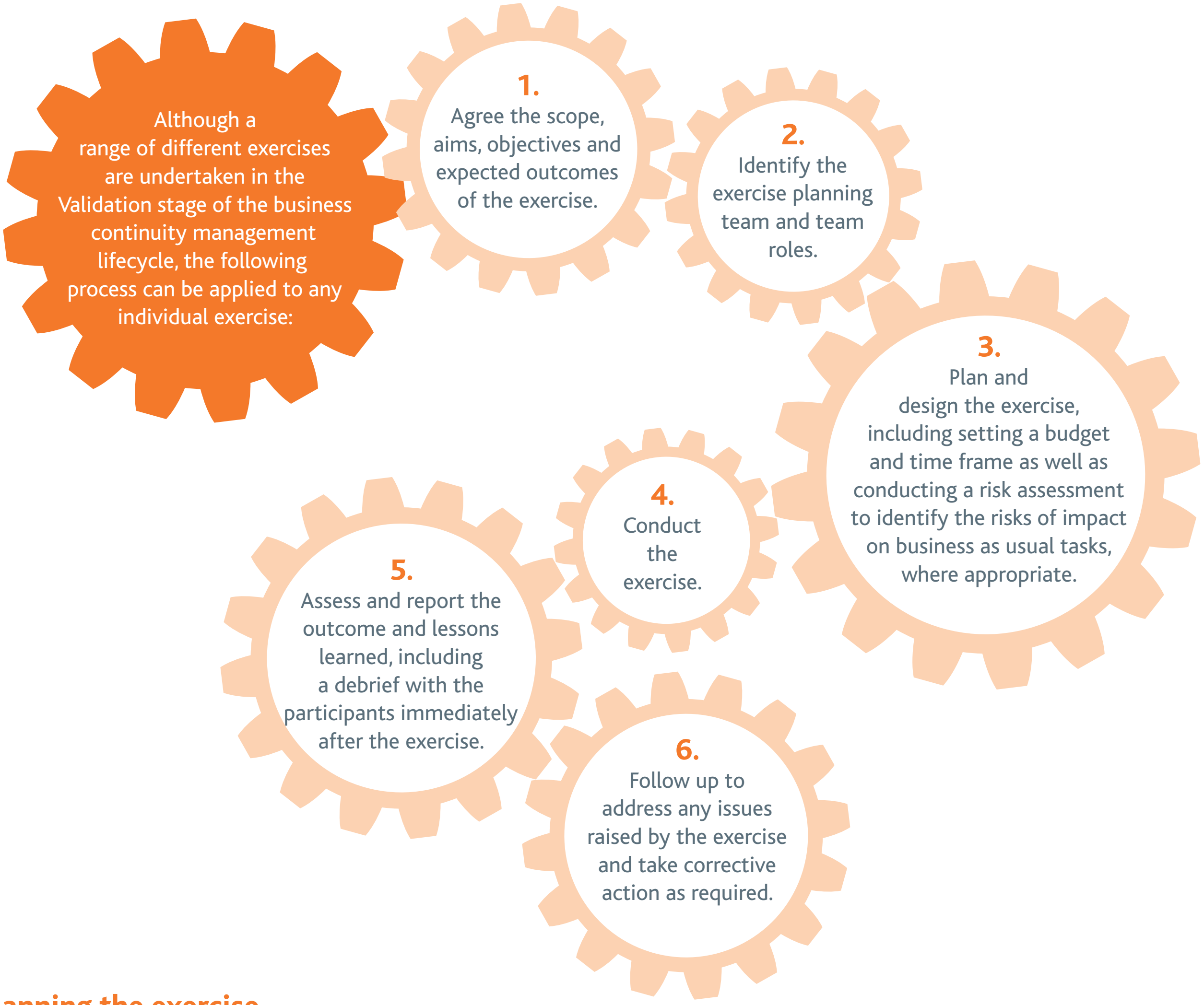
As the organization's exercise experience and business continuity management capability increases, it may be appropriate to consider involving a wider range of interested parties in the exercises. For example, customers, suppliers, regulators, statutory and professional bodies, agencies, emergency services, and the voluntary sector.

The continuity capability of suppliers and outsourced activities that have been prioritised should be considered an important part of validating the organization's business continuity 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. The organization should consider any operational or reputational risks involved with external participation together with 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. The warning time and the number of pre-warned participants may reduce as the organization becomes more confident in its business continuity capability.

Process



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

1. Agree the scope, aims, objectives and expected outcomes of the exercise.

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 risk assessment to identify the risks of impact on business as usual tasks, where appropriate.

4. Conduct the exercise.

5. Assess and report the outcome and lessons learned, including a debrief with the participants immediately after the exercise.

6. Follow up to address any issues raised by the exercise and take corrective action as required.

Planning the exercise

The individuals planning the exercise should prepare a schedule that demonstrates 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 schedule can also list the anticipated participant response to an event, especially if this is defined in the business continuity plan. The individuals coordinating or facilitating the exercise use the schedule to ensure the exercise runs as planned and to prompt participants to refer to specific business continuity plan content or procedures so that they can be validated.

Individual scheduled exercise 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.
- Delivery method of the inject.
- Participants or teams who should receive the inject.
- Expected responses from the participants or teams, reflecting the business continuity plan, where relevant.

Prior to the exercise starting: 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. It is essential the briefing does 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.
- Roles and responsibilities during the exercise.
- Information, communication tools, and technology to be used.
- Action in the event of unforeseen circumstances.
- Post-exercise activities.

To prevent misunderstanding or unintended organizational disruption, it is essential that participants and the wider organization are 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 notice or there is 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, emails etc. 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. 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 is making decisions that would not be appropriate in the given scenario, or to re-focus if the exercise participants have become distracted from the main exercise objectives. Taking time out can also be a useful learning opportunity to discuss exercise decisions or concerns, or to 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 in extreme cases, terminated.

Ending the exercise: The decision to end the exercise should rest with the individual or team managing the exercise. Consideration should be given as 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 to take place.

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

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

It is important 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 gives the participants the opportunity to highlight a variety of immediate issues and concerns.
- **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 as well as 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 review.
- **Interviews:** These should be held within one week of the exercise. The interview could be conducted one to one or with a small group of participants.
- **Post-exercise report:** The results of the debriefing should be used to prepare a post-exercise report including recommendations for improvement.

To ensure any lessons identified are accepted and addressed by the organization, the post-exercise report should be distributed to all exercise participants, other relevant personnel and interested parties.

It is essential that there is a management process to ensure that the findings of the post-exercise report are included in the organization's review and considered in the business continuity programme update. The organization should create and seek top management approval for action plans to implement the recommendations, as they may involve changes to the wider business continuity programme.

If significant issues have been identified in an exercise, the organization should consider repeating the exercise, after corrective actions have been put in place.

Outcomes and Review

The outcomes of the exercise development and delivery process are:

- An exercise plan or brief which outlines the objectives, scope, roles and responsibilities, and approach of how the exercise should be conducted.
- 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 include:

- Confirmation that personnel are familiar with their roles, responsibilities, and authority in response to an incident.
- Validation of the technical, logistical, and administrative aspects of the business continuity plan.
- Validation of suitability of the continuity infrastructure (command centres, work areas, technology, and telecommunications resources).
- Confirmation of the availability of personnel and processes for relocation.
- Enhanced awareness of business continuity, crisis management, and emergency response procedures.
- An increased awareness of the significance of business continuity.
- Ideas for further exercises and scenarios relevant to the organization.

The exercise development process should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Maintenance

Maintenance of the business continuity programme keeps the organization's business continuity arrangements up to date. This ensures that the organization remains ready to respond to, and manage the impacts from incidents effectively, despite periodic organizational change.

General Principles

To be effective, maintenance activities should be embedded within the organization's business as usual processes rather than being a separate activity that may be overlooked.

Most of the maintenance required will be the result of internal 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 within an organization, a time frame should be agreed to implement any changes in the business continuity programme.

Requirements for maintenance activities can be identified using the following:

- Lessons learned through exercising.
- 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.
- A real incident, where lessons learned can be incorporated.
- Changes or updates in the business continuity management lifecycle, such as the BIA or continuity solutions.

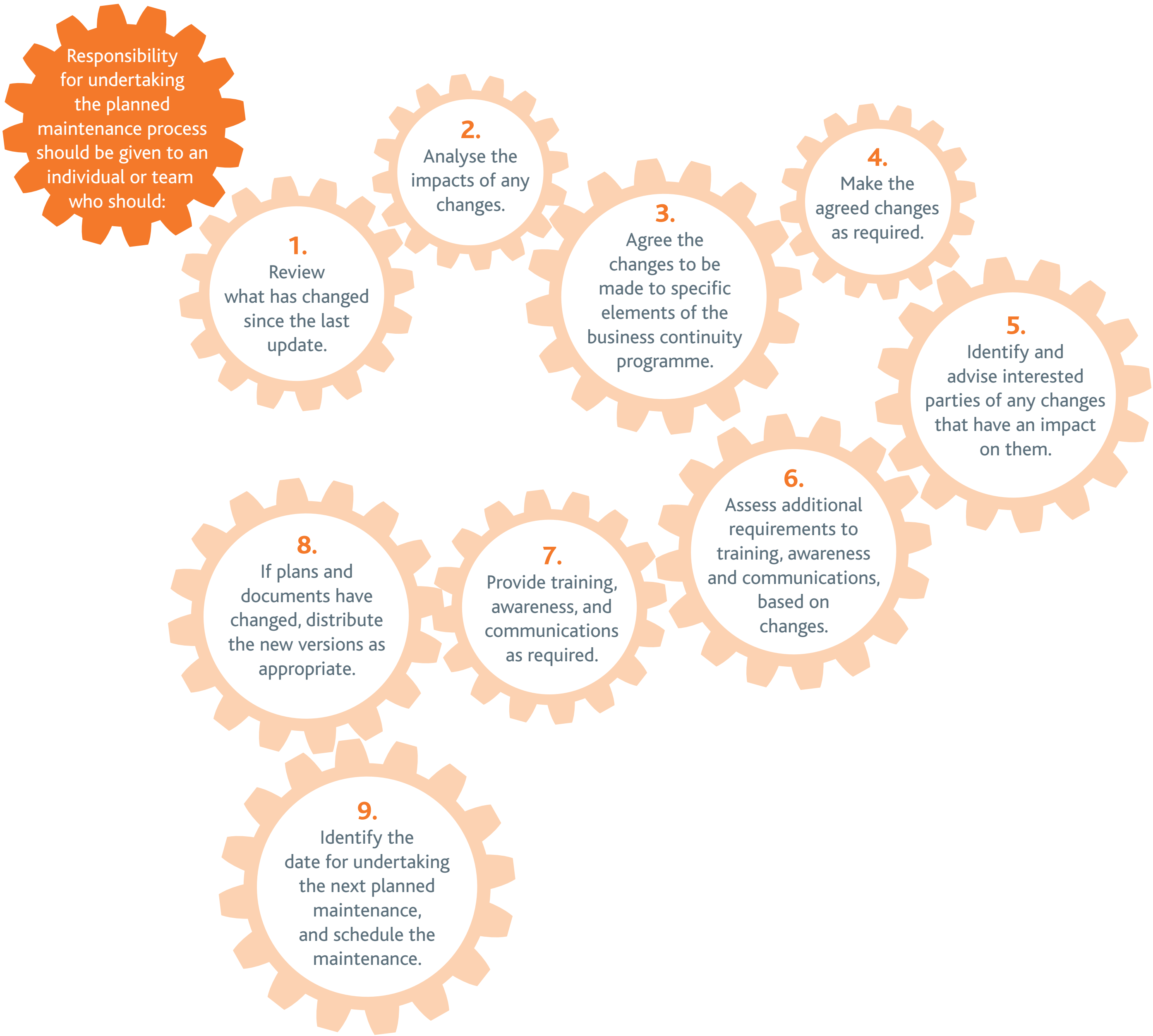
Concepts and Assumptions

Although the need for maintenance may be triggered by any or all of the requirements, regular and planned maintenance is required for the entire business continuity programme. This involves establishing a schedule for carrying out specific maintenance activities, for example, planned updates, checking of backup equipment and review of contracts, that are undertaken at specified intervals over an agreed time frame.

Process

A formal process for maintaining the business continuity programme needs to be established. 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 activity being maintained.

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



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

1. Review what has changed since the last update.

2. Analyse the impacts of any changes.

3. Agree the changes to be made to specific elements of the business continuity programme.

4. Make the agreed changes as required.

5. Identify and advise interested parties of any changes that have an impact on them.

6. Assess additional requirements to training, awareness and communications, based on changes.

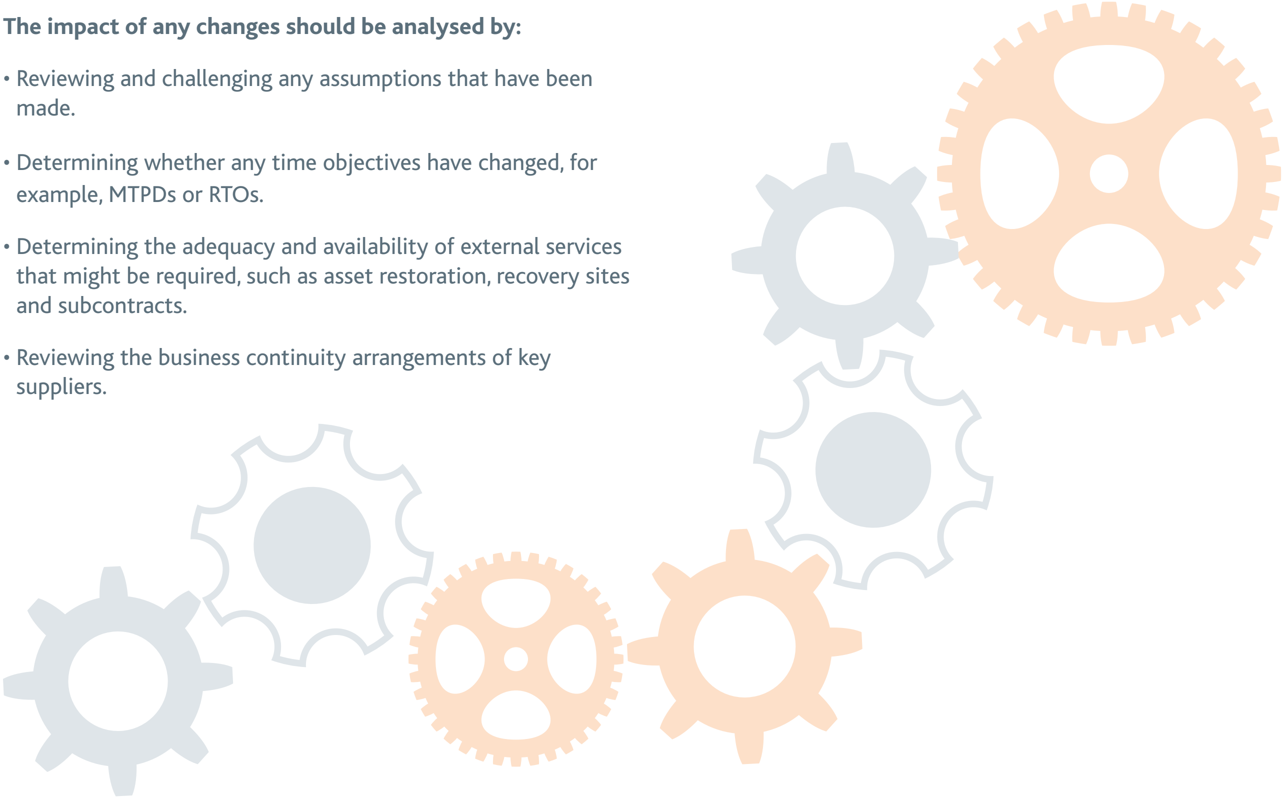
7. Provide training, awareness, and communications as required.

8. If plans and documents have changed, distribute the new versions as appropriate.

9. Identify the date for undertaking the next planned maintenance, and schedule the maintenance.

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 business continuity arrangements of key suppliers.



Methods and Techniques

Responsibility for maintenance should be given to the departmental representative for business continuity, although plan distribution can be handled by a central individual or team. For example, a departmental representative can be made 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.

If it is to achieve its purpose, maintenance needs to be managed in a timely manner. This requires regular reports which identify progress of planned maintenance, highlight areas of weakness, and make recommendations for improving the process.

Proprietary software can be very effective in managing documentation by using systems which contain follow-up, tracking, reporting and reminders to ensure that maintenance takes place as and when planned.

Outcomes and Review

The outcomes of maintenance of the business continuity programme include:

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

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

Review

The purpose of a review is to evaluate the business continuity policy and programme for continuing suitability, adequacy, and effectiveness.

General Principles

There are six basic types of review:

- **Audit** (internal and external): A formal, impartial review process that measures an organization's business continuity programme against a pre-agreed standard.
- **Self-assessment:** An assessment of the organization's programme by those involved in the management and implementation of the business continuity programme.
- **Quality Assurance (QA):** A process that ensures that the various outputs from the business continuity programme meet the defined requirements.
- **Performance appraisal:** A review of the performance of individuals tasked with roles and responsibilities.
- **Supplier performance:** A review of a key supplier's business continuity programme or their recovery services.
- **Management review:** A review by top management of the organization's business continuity programme to ensure it aligns with organizational objectives.

Methods and Techniques

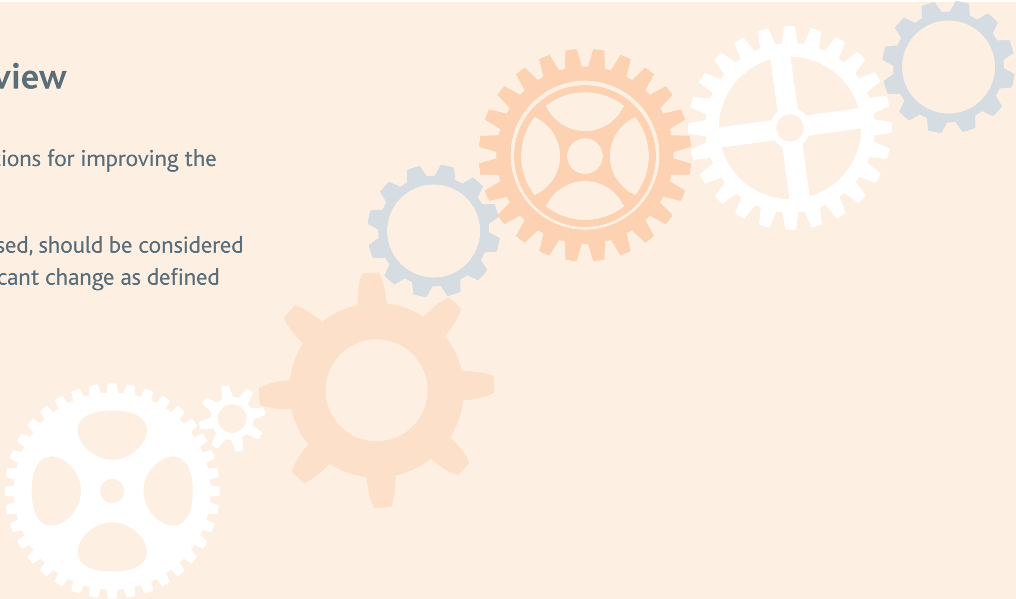
The following criteria can be considered for assessment to support the review of the organization's business continuity programme:

- Whether the programme is up to date and aligned to the organization's:
  - Governance structure and strategic objectives.
  - Culture and operating environment.
  - Technology systems (primarily ICT specific business applications and critical operating systems).
  - Other prioritised resource dependencies (non-ICT specific).
  - Business continuity policy.
- The effective use of resources and procedures, for example, systems, tools, and response and recovery procedures etc. within the business continuity programme.
- The alignment and integration of the business continuity programme in relation to other organizational response procedures which may include:
  - Emergency management procedures.
  - Health and Safety procedures.
  - Security procedures.
  - ICT recovery plans and processes.
- The frequency and effectiveness of training and awareness sessions and whether these enhance the overall level of awareness and understanding of business continuity.
- An assessment of the competency of the individuals assigned roles in the business continuity programme (including alternates).
- The frequency and effectiveness of exercising and whether it is used to validate the effectiveness of the business continuity programme.
- The performance of the personnel who are directly accountable for management of the business continuity programme.

Outcomes and Review

The outcomes of the review should be options for improving the organization's level of resilience.

The effectiveness of the types of review used, should be considered at pre-agreed intervals or following significant change as defined within the business continuity policy.



Audit

General Principles

Auditing is designed to verify that the business continuity process has been followed correctly, not that the solutions adopted are necessarily correct.

The purpose of a business continuity management audit is to analyse an organization's existing business continuity programme and verify it against predefined standards and criteria to deliver a structured audit report.

Audits should be conducted at planned intervals to confirm that the organization is conforming with its own business continuity policy or the organization's audit and governance policies where relevant.

Concepts and Assumptions

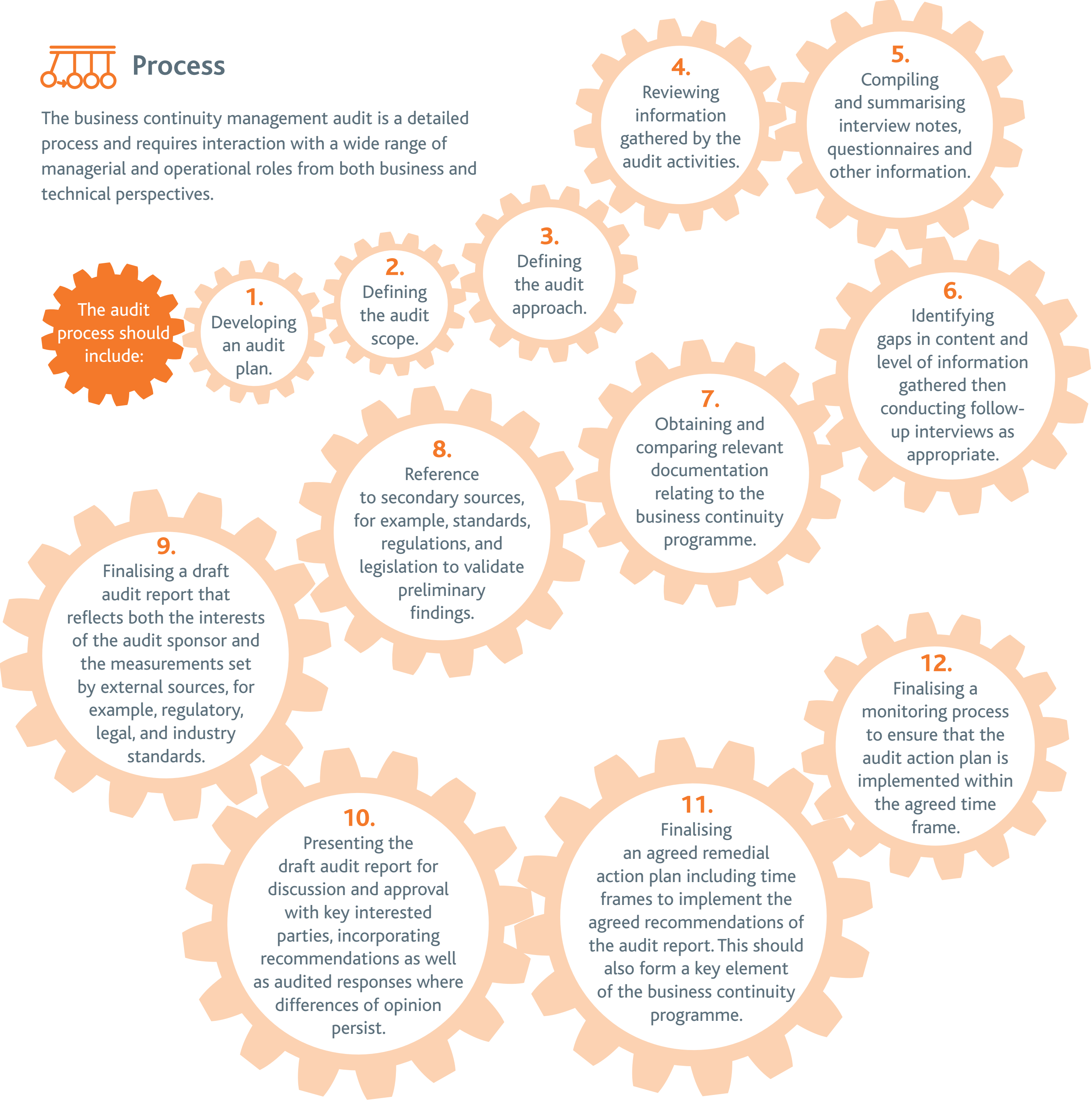
An audit assumes that if the process is undertaken correctly and properly applied, then the outcome should provide evidence of an effective programme. It also assumes that the method adopted by the organization is effective and provides a suitable framework for audit.

The assessment method adopted by the organization should have been defined in its business continuity policy document.

The person carrying out the audit should have the relevant competencies and skills to perform this task.

Process

The business continuity management 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:

1. Developing an audit plan.
2. Defining the audit scope.
3. Defining the audit approach.
4. Reviewing information gathered by the audit activities.
5. Compiling and summarising interview notes, questionnaires and other information.
6. Identifying gaps in content and level of information gathered then conducting follow-up interviews as appropriate.
7. Obtaining and comparing relevant documentation relating to the business continuity programme.
8. Reference to secondary sources, for example, standards, regulations, and legislation to validate preliminary findings.
9. Finalising a draft audit report that reflects both the interests of the audit sponsor and the measurements set by external sources, for example, regulatory, legal, and industry standards.
10. Presenting the draft audit report for discussion and approval with key interested parties, incorporating recommendations as well as audited responses where differences of opinion persist.
11. Finalising an agreed remedial action plan including time frames to implement the agreed recommendations of the audit report. This should also form a key element of the business continuity programme.
12. Finalising a monitoring process to ensure that the audit action plan is implemented within the agreed time frame.

Methods and Techniques

The methods used for auditing should be determined by those undertaking the audit and should comply with the organization's business continuity policy, as well as the organization's established auditing procedures where relevant.

A business continuity management audit plan should include identification of:

- The audit objectives, which in part should be driven and governed, or restricted by, legal or regulatory requirements. This includes key issues of high priority.
- A standard audit framework (where appropriate) which is to be used. 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:

- The auditing activities that should be undertaken, for example, questionnaires, face to face interviews, document reviews, and solution reviews.
- An activity timetable and due dates.
- Identification of the audit evaluation criteria.
- Any requirements for specific subject expertise or outsourced service provider assistance to conduct the audit.

Outcomes and Review

The outcomes of a business continuity management audit include:

- An independent business continuity management audit report.
- A remedial action plan that is agreed and approved by top management.
- The outcome of an unfavourable performance rating, which should be:
    - Acceptance of the plans by management as 'inadequate'.
    - The initiation of a review conducted by a business continuity professional to assist the team in improving their position.

The auditing process should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Self-Assessment

General Principles

The purpose of self-assessment is for an organization to review its implementation of the business continuity programme with a view to creating an action plan for improvements.

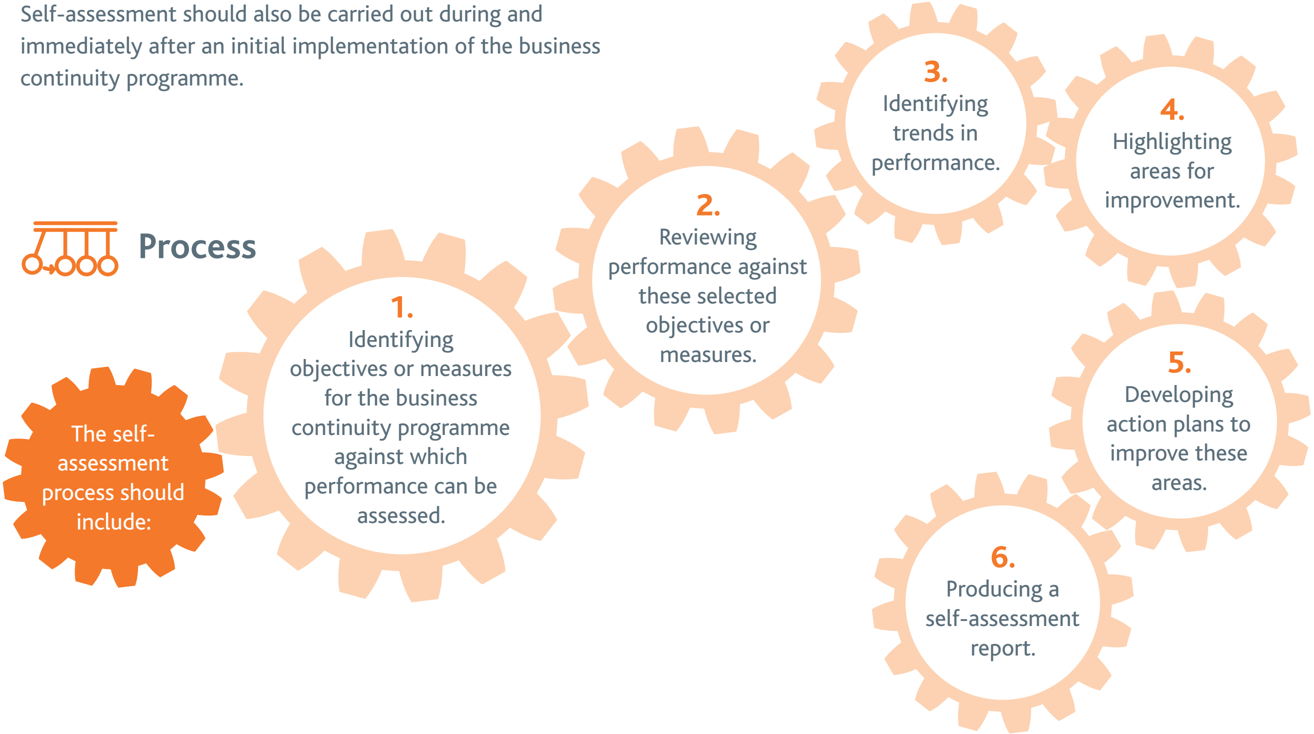
Self-assessment can be carried out between audits to identify progress against audit recommendations.

Self-assessment should also be carried out during and immediately after an initial implementation of the business continuity programme.

Concepts and Assumptions

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

Process



The self-assessment process should include:

1. Identifying objectives or measures for the business continuity programme against which performance can be assessed.

2. Reviewing performance against these selected objectives or measures.

3. Identifying trends in performance.

4. Highlighting areas for improvement.

5. Developing action plans to improve these areas.

6. Producing a self-assessment report.

Methods and Techniques

Objectives or measures to be used in self-assessments include:

- Project milestones for the business continuity programme.
- Percentage of plans maintained by the scheduled date.
- Percentage of members on response teams involved in an exercise each year.
- Number of lessons learned from exercises still not addressed.
- Extent of completion of the BIAs.

An existing maturity model can be used or can be developed to evaluate progress and can 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 business continuity programme.
- 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 business continuity policy.

Quality Assurance

General Principles

Quality Assurance is the process of determining whether the outputs from the business continuity programme meet the organization's requirements and expectations, which may or may not have been formally defined.

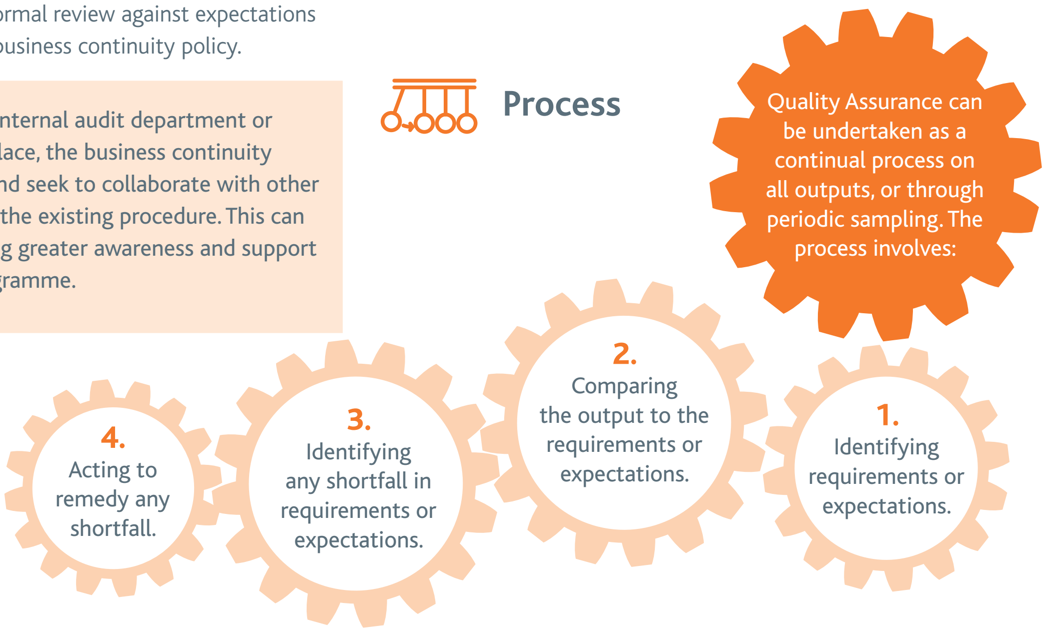
For organizations that are certified against international or national standards, this should be a formal and documented process. For other organizations, this should be an informal review against expectations and intentions as expressed in the business continuity policy.

> If there is already an internal audit department or reporting process in place, the business continuity professional should recognise and seek to collaborate with other departments and contribute to the existing procedure. This can have the added benefit of raising greater awareness and support for the business continuity programme.

Concepts and Assumptions

Quality Assurance is an ongoing process throughout the business continuity management lifecycle. It assumes that the requirements for the outputs of the business continuity programme have been identified.

Process



Quality Assurance can be undertaken as a continual process on all outputs, or through periodic sampling. The process involves:

1. Identifying requirements or expectations.

2. Comparing the output to the requirements or expectations.

3. Identifying any shortfall in requirements or expectations.

4. Acting to remedy any shortfall.

Methods and Techniques

Requirements can be identified by reviewing the business continuity programme, however identifying expectations involves interviewing personnel and interested parties.

The organization can use the following questions when comparing business continuity programme outputs to the requirements or expectations and identifying shortfalls:

- Does a document conform to the document control standards?
- Has the plan been verified by its owner?
- Does a BIA identify the MTPDs of all prioritised activities?
- Have the appropriate details (quantity, time frame, and source) of required resources for continuity and recovery of an activity been identified?
- Have the recommended continuity and recovery solutions been agreed by top management?
- Does the business continuity plan have an agreed scope signed off by top management?
- Have any previous quality assurance reports been reviewed and actions or recommendations addressed?

Outcomes and Review

The outcome of Quality Assurance should be:

- An improvement in the way the outputs from the business continuity programme meet the organization's requirements and expectations.

The Quality Assurance process should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Performance Appraisal

General Principles

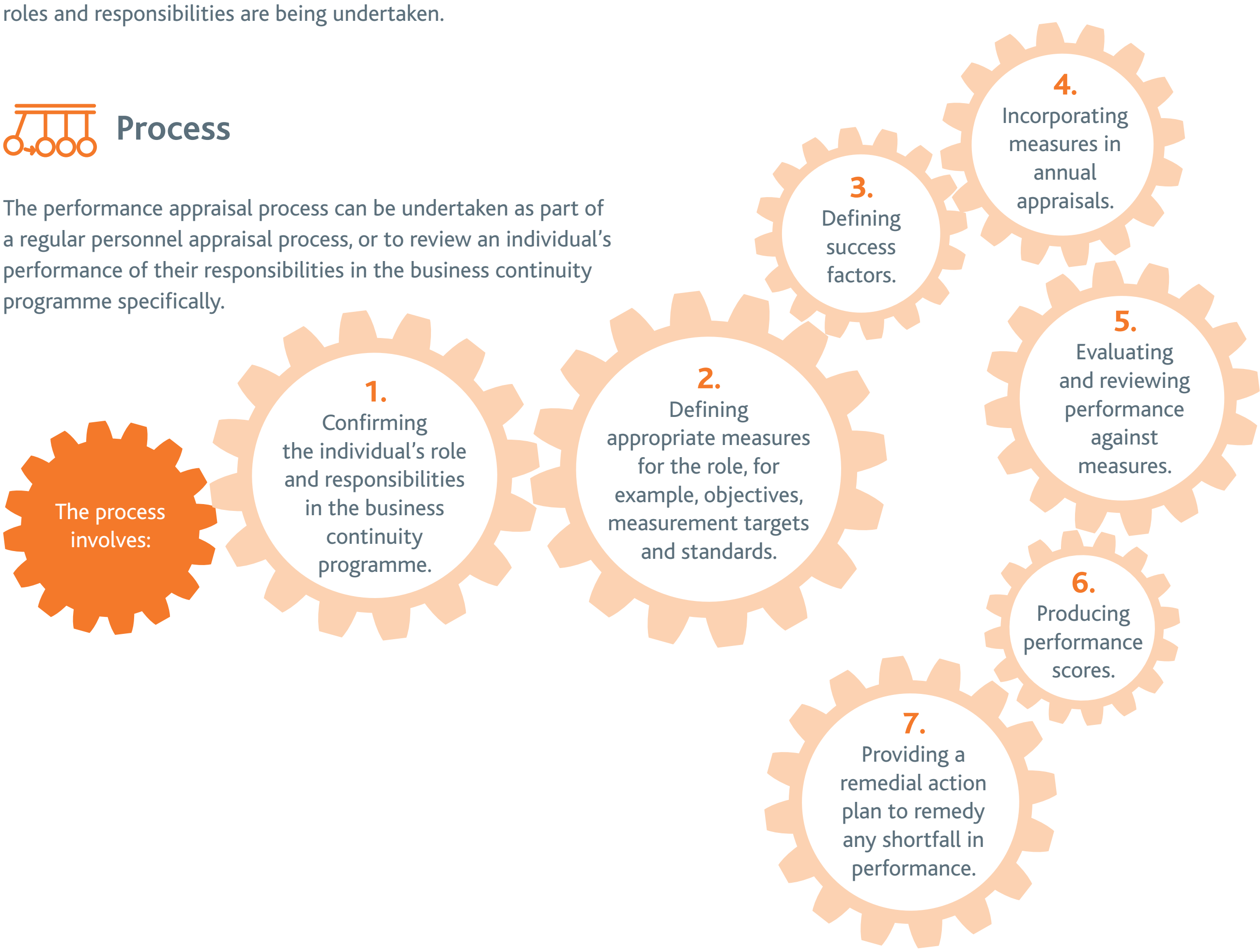
Roles and responsibilities for the business continuity programme should have been defined as part of business continuity policy. Performance appraisals should be used to check how well those roles and responsibilities are being undertaken.

Concepts and Assumptions

An organization's performance appraisal process assumes that the roles and responsibilities for business continuity 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 business continuity programme specifically.



The process involves:

1. Confirming the individual's role and responsibilities in the business continuity programme.
2. Defining appropriate measures for the role, for example, objectives, measurement targets and standards.
3. Defining success factors.
4. Incorporating measures in annual appraisals.
5. Evaluating and reviewing performance against measures.
6. Producing performance scores.
7. Providing a remedial action plan to remedy any shortfall in performance.

Methods and Techniques

Measures could include:

- Number of times scheduled plan maintenance dates were met.
- Percentage completion of the BIAs.
- Number of exercises undertaken as planned.
- Number of plans completed.
- Number of outstanding issues resulting from incidents, exercises, and audits.
- Expenditure against budget.

Outcomes and Review

The outcome of a performance appraisal should be an improvement in the way in which an individual tasked with a role in the business continuity programme:

- Carries out their role.
- Undertakes their responsibilities.
- Meets their objectives.

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

Supplier Performance

General Principles

The review process of the business continuity programme of any supplier on which the organization depends should be similar to the process employed for reviewing the organization's own programme.

Concepts and Assumptions

The supplier performance review assumes that the suppliers on which the organization depends have been identified, and the expectations of their business continuity programme defined.

Process

The process for reviewing key suppliers' business continuity programmes and reviewing suppliers of recovery services should be defined in their contracts. The business continuity programme of key suppliers should be reviewed as if they were part of the organization itself. This is in the same way that the business continuity arrangements of any internal department, location, or outsourced service provider that provides products and services would be reviewed.

Methods and Techniques

Supplier performance should be reviewed against contractual service level agreements (SLAs), which in the case of key suppliers should relate to their business continuity programme.

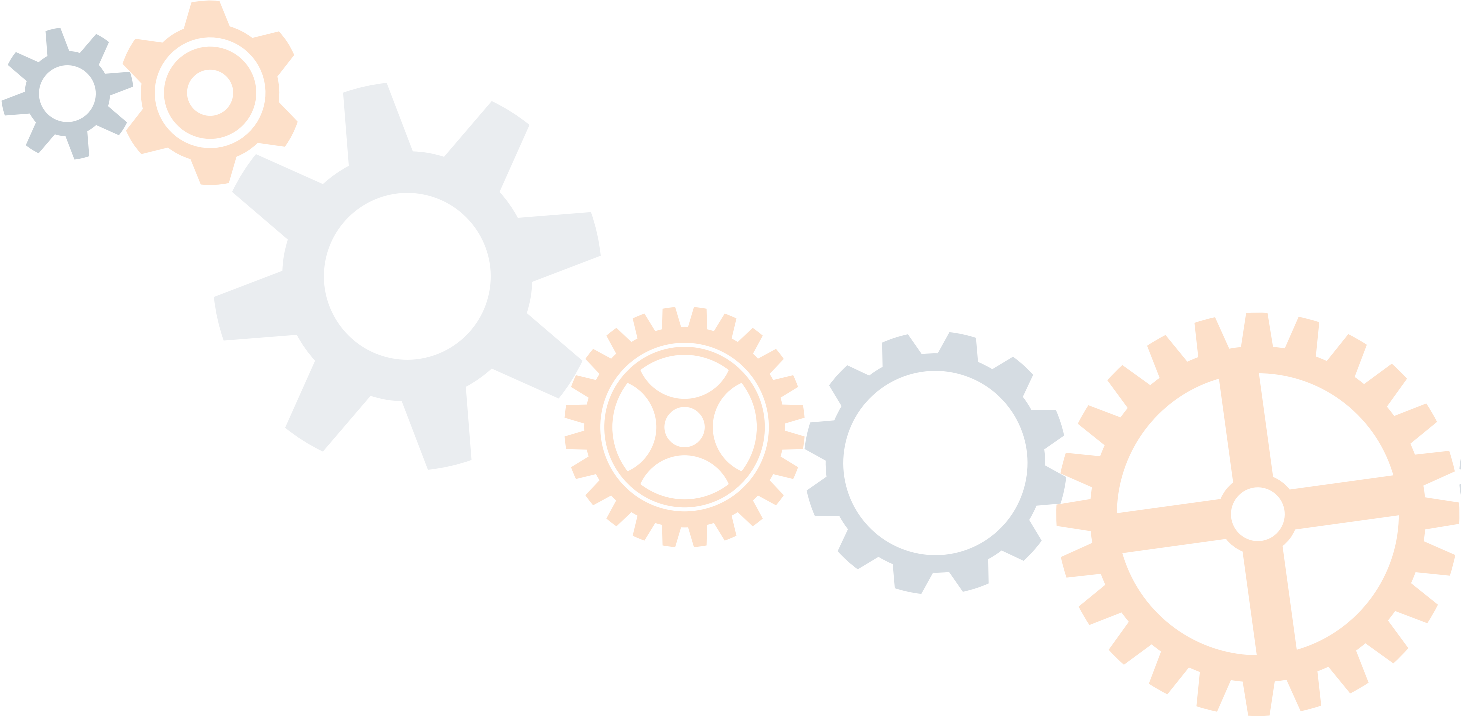
Increased supplier performance and capability can be achieved by including and assessing their exercise activities.

Outcomes and Review

The outcomes of reviewing supplier performance include:

- A performance rating against service level agreements.
- An understanding of the supplier's business continuity programme.
- An action plan for improving supplier performance.
- Increased readiness and assurance of prioritised supplier activities.

The performance of the supplier's business continuity programme should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.



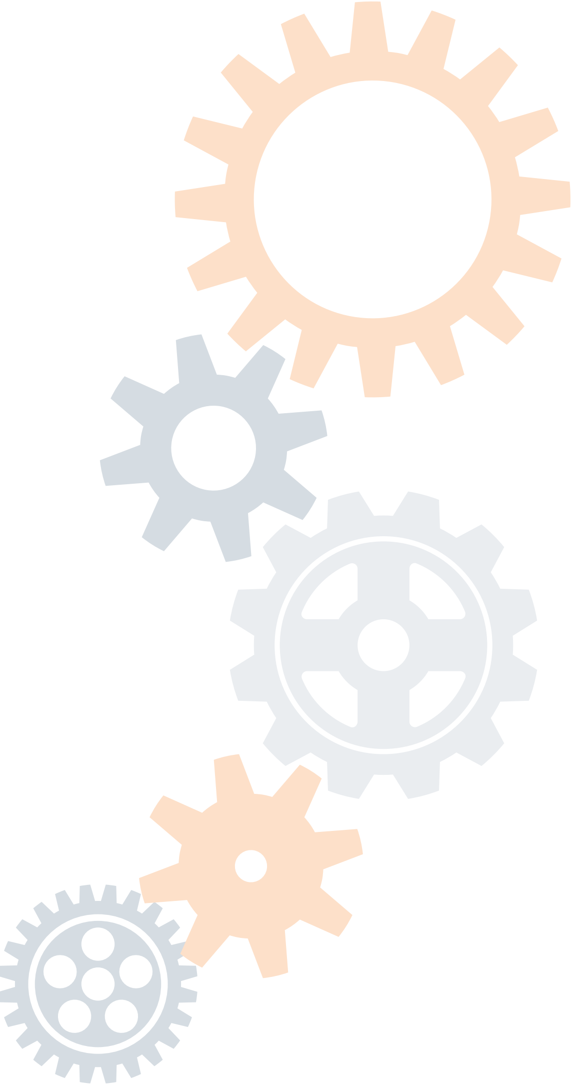
Management Review

General Principles

A management review provides opportunities for top management to understand the performance of the business continuity programme. 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 Assumptions

A management review assumes that the intentions and directions of the organization as identified in the business continuity policy are effectively adhered to.



Methods and Techniques

A management review should include information relating to the following:

- The status of actions from previous management reviews.
- Changes to the internal and external environment, if relevant to the organization's business continuity programme.
- Information regarding the performance of the programme 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 exercising.
- Risks or issues not adequately addressed in the programme.
- Adequacy of the business continuity policy.

Outcomes and Review

The outcomes of the management review include:

- An action plan for improvements.
- **Continual improvement of the business continuity programme.**
- An enhancement of the organization's level of resilience.

The management review process should be regularly reviewed at pre-agreed intervals or following significant change as defined within the business continuity policy.

Find out more
www.thebci.org

Leading the way to resilience.

Membership

Industry leading thought leadership

Events and Awards

Networking

Corporate partnership

Award winning training

bci Leading the way to resilience

Find out more
www.thebci.org

BCI Membership Grades

Affiliate Student
CBCI
AMBCI
MBCI
FBCI

Leading the way to resilience

Good Practice Guidelines

2018 Edition

The global guide to good
practice in business continuity.

Central Office

The BCI

10-11 Southview Park,
Marsack Street,
Caversham,
Berkshire
RG4 5AF, UK

Tel: +44 (0) 118 947 8215

www.thebci.org

BCI Offices and Contact Information

communications@thebci.org
subscriptions@thebci.org
membership@thebci.org
education@thebci.org
advertising@thebci.org
events@thebci.org
research@thebci.org

ISBN: 978-0-9932110-8-9

Correct at November 17