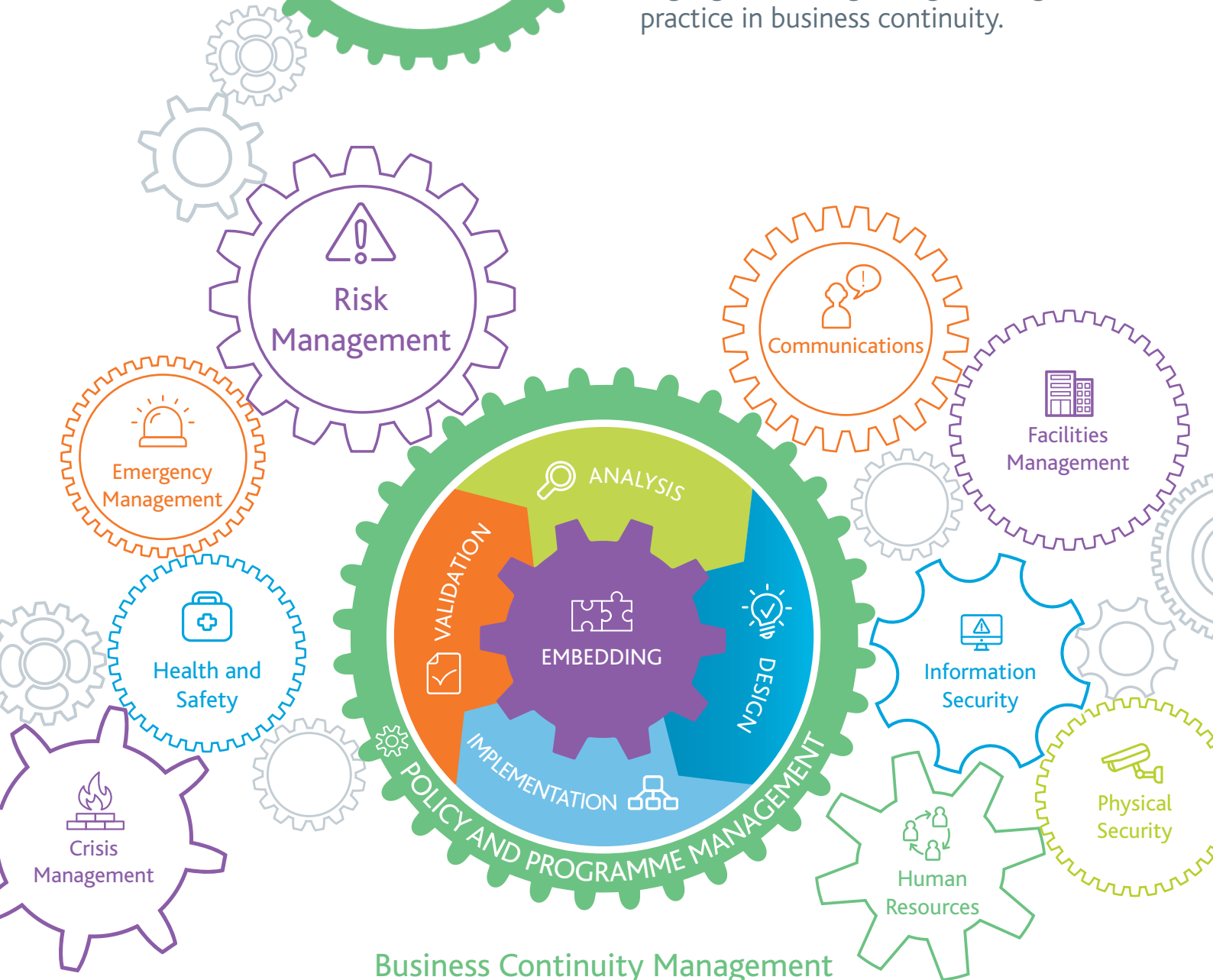




Good Practice Guidelines

2018 Lite Edition

Highlights of the global guide to good practice in business continuity.



Business Continuity Management (BCM) Lifecycle

Building organizational resilience

COPYRIGHT PROTECTED DOCUMENT

© BCI/BCI Forum Limited. Published 2018. All rights reserved.

No part of this publication may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from BCI at the address below:

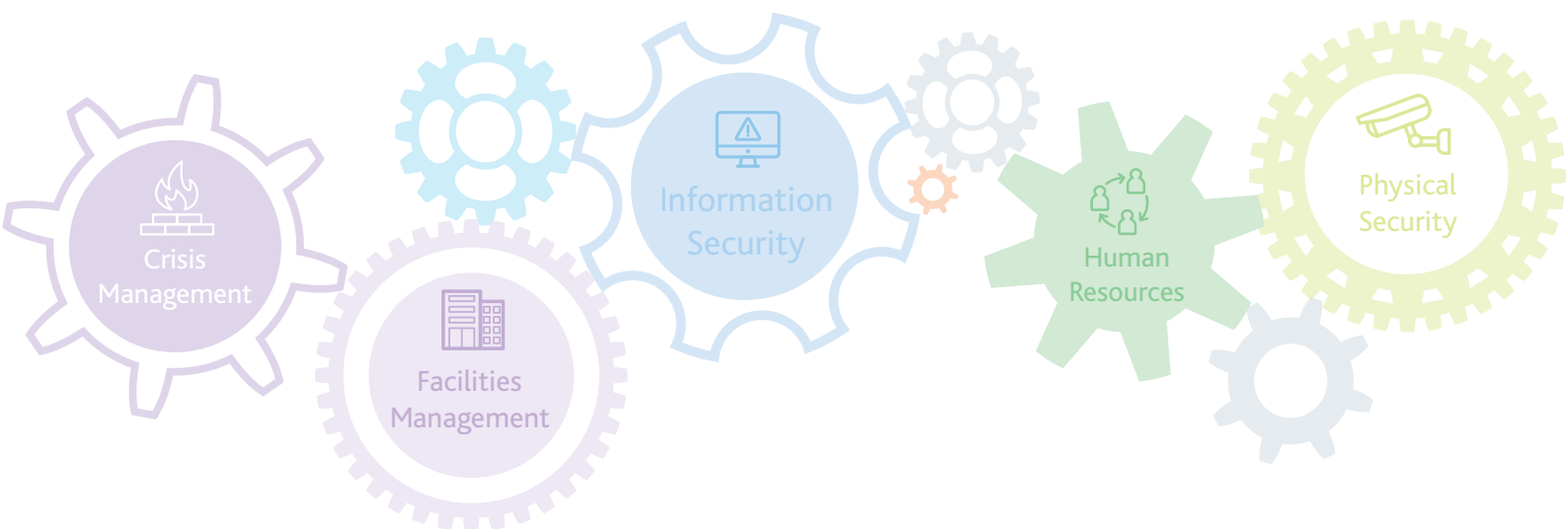
BCI Copyright

bci@thebci.org

10-11 Southview Park, Marsack Street, Caversham, Berkshire, RG4 5AF, UK.

www.thebci.org

For those intending to take the Certificate of BCI (CBCI) examination, the full version of the GPG 2018 should be studied.



contents

Introduction to BCI's Good Practice Guidelines 2018 Lite Edition	4
About BCI	4
What is Business Continuity?	4
What is the Good Practice Guidelines 2018 Lite Edition?	4
Who is the Good Practice Guidelines 2018 Lite Edition for?	5
What to do next	5
The BCM Lifecycle: Building organizational resilience	6
The Professional Practices 2018	6
Glossary of Terms	7
PP1 Policy and Programme Management	9
PP2 Embedding Business Continuity	11
PP3 Analysis	13
PP4 Design	15
PP5 Implementation	17
PP6 Validation	19
Next steps	21
CBCI Classroom Course	21
CBCI Online	21
CBCI Exam	21
Additional training courses	21



Introduction to BCI's Good Practice Guidelines 2018 Lite Edition

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.

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 BCI.

The business continuity management lifecycle is central to improved organizational resilience. Through collaboration with other management disciplines, for example, risk management, communications, emergency management, crisis management, health and safety, facilities management and human resources, BCI aims to promote and create a more resilient world.

About BCI.

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.

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

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 BCI's process of continual improvement and ongoing development of our body of knowledge to remain relevant to professionals worldwide.

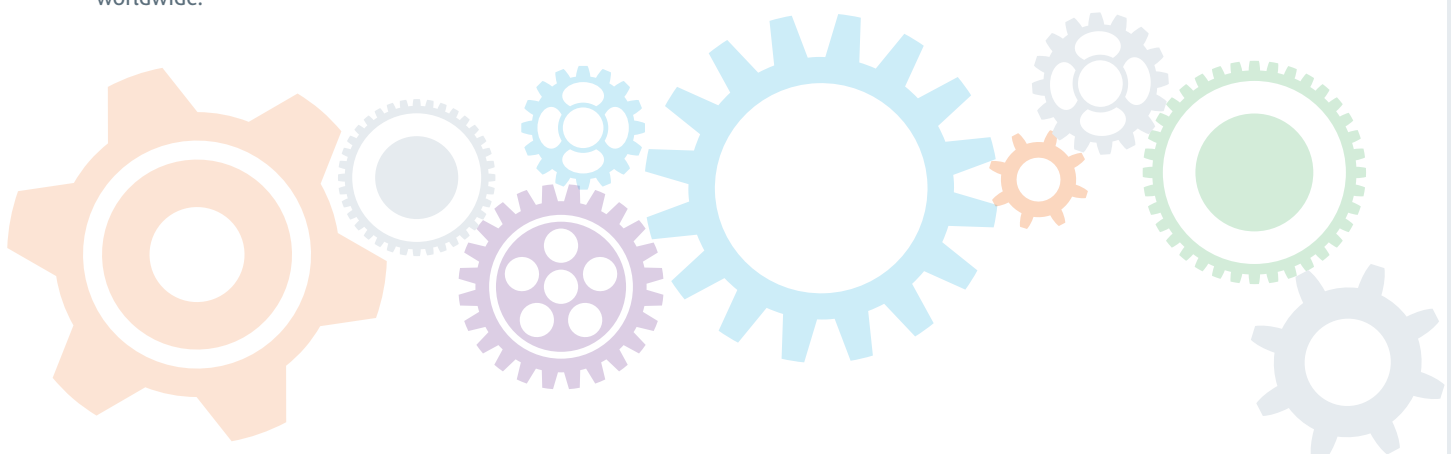
What is Business Continuity?

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. An effective business continuity programme supports the strategic objectives of the organization and proactively 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.

What is the difference between the Full and Lite Editions of the Good Practice Guidelines 2018?

The Good Practice Guidelines 2018 Edition provides a full and comprehensive breakdown of business continuity management. The business continuity management lifecycle provides a framework to structure the approach to business continuity. It gives readers the understanding and knowledge to sit our Certificate of BCI (CBCI) examination and progress their careers within business continuity and the wider resilience landscape.

The Lite Edition provides you with an overview of the six Professional Practices. It is the perfect tool for organizations to inform staff of good practice, and for professionals to understand the Professional Practices before they enroll on the full CBCI course.



Who is the Good Practice Guidelines 2018 Lite Edition for?

The GPG 2018 Lite Edition is for any professional or organization looking to take their first steps towards improved organizational resilience. The GPG and GPG Lite are relevant to anyone with a business continuity or 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 to do next

Once you have read the Good Practice Guidelines 2018 Lite Edition, you will have an understanding of the business continuity management lifecycle which will help you to progress to the full CBCI course and exam.

Our CBCI exam tests your knowledge of the Good Practice Guidelines 2018 Edition and can be taken in two ways; in person or online.

BCI has a selection of other resources available, ranging from sector specific training courses to mentoring and networking opportunities.

Once you are a certified member of BCI, you will gain a post nominal designation of CBCI which demonstrates your knowledge of the Professional Practices. You can also explore your personalised member area and benefit from BCI's extensive range of resources.

Further information on our range of resources is available at the end of this document.



The BCM Lifecycle: Building organizational resilience.

The following Professional Practices form the basis for the business continuity management lifecycle. These are the stages required to improve organizational resilience.



The Professional Practices 2018

Management practices

- PP1 Policy & Programme Management
- PP2 Embedding

Technical practices

- PP3 Analysis
- PP4 Design
- PP5 Implementation
- PP6 Validation

Once you understand the purpose of these Professional Practices, you can read the Good Practice Guidelines 2018 Edition in full to understand how to review or revise an existing programme as well as initiate a new business continuity programme.

To reflect the evolving business continuity discipline, the use of terminology in the GPG 2018 Edition has been carefully considered and in most cases BCI has adopted ISO terms and definitions.

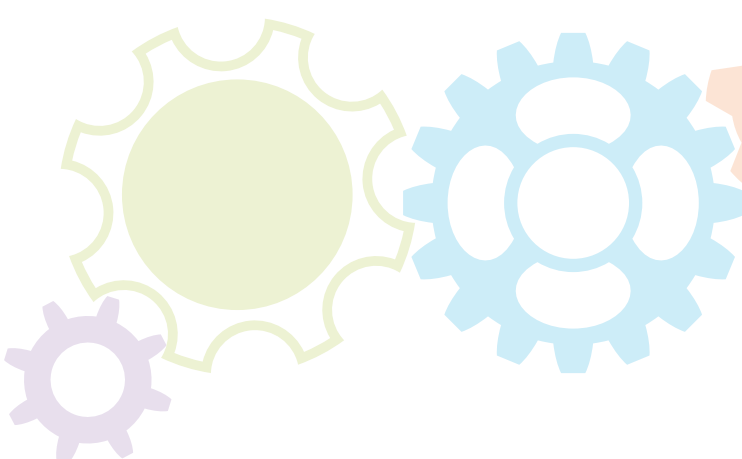
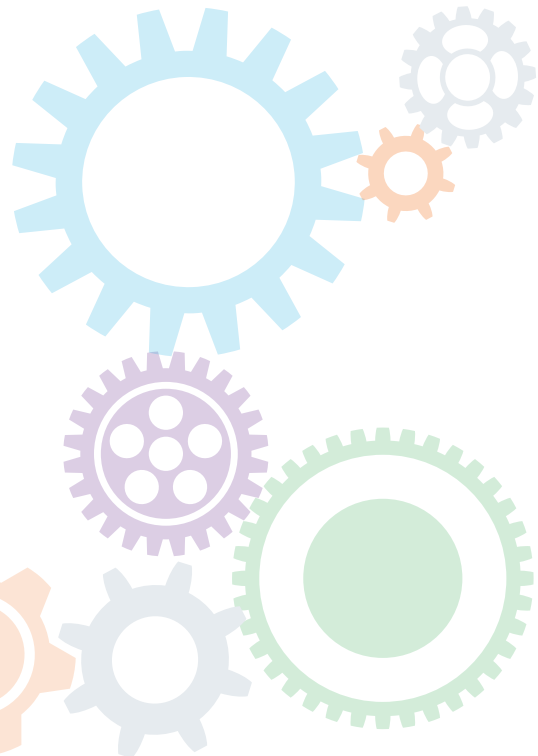
Permission to reproduce extracts from ISO 22301:2012 and ISO/TS 22317:2015 is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop:

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

The following terms may not be present in the GPG 2018 Lite Edition; however, they are relevant to all professionals looking to improve resilience capabilities.

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 pre-defined 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 pre-defined 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

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.





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.

Successfully establishing the business continuity programme is the result of several planning stages as defined below.

Establishing the Business Continuity Policy

This sets the boundaries and requirements for the BC programme and states the reasons why it is being implemented. It defines the guiding principles which the organization measures its performance against, as well as defining how to continue delivering products and services in the event of an incident.

Defining the Scope of the Business Continuity Programme

This includes consideration of the organization's products and services to be included in the programme.

Establishing Governance

This activity provides a central point of accountability for implementation and continuous monitoring of an organization's activities in accordance with the business continuity policy.

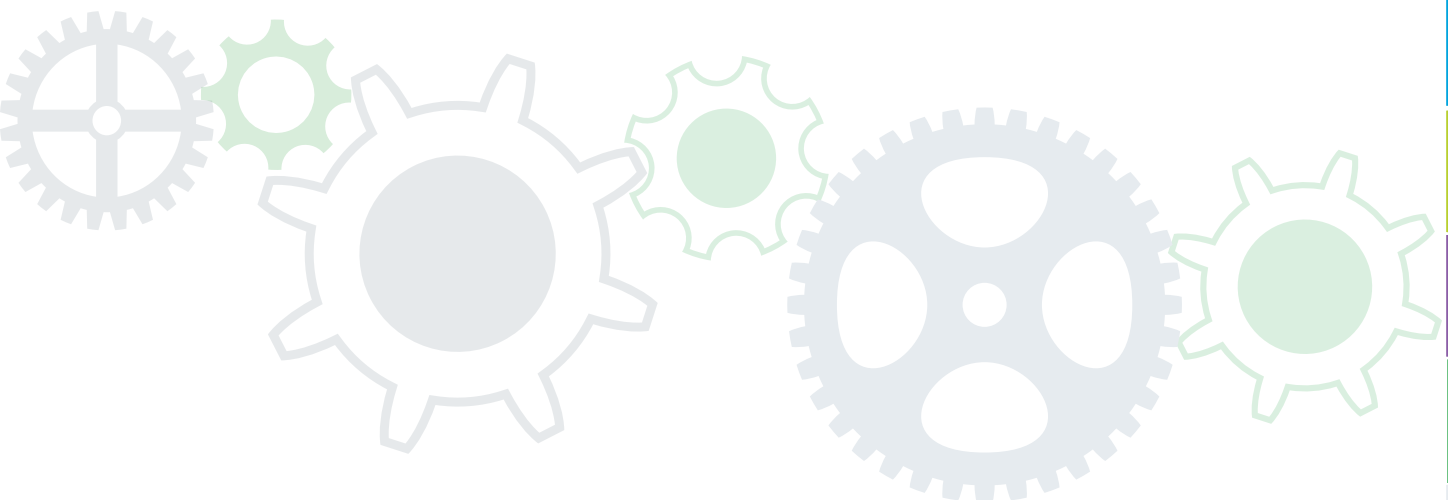
Assigning Roles and Responsibilities

This is the early identification of roles, responsibilities, and authorities required to manage the programme.

The Business Continuity Programme

Once the scope, governance, and roles and responsibilities are defined, the BC programme is put in place.

Further information on these activities can be found in the Good Practice Guidelines 2018 Edition.



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.





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.

Successfully embedding business continuity is the result of the following activities;

Understanding and Influencing Organizational Culture

This includes considering your current capabilities and ensuring an understanding of current practice and what skills are required to improve the organization's culture.

Competencies and Skills

This means ensuring all staff with business continuity related roles have appropriate education, training and experience to develop and implement the BC policy.

Training and awareness

This involves responding to the competencies and skills identified, and ensuring training and awareness requirements are responded to.

Further information on these activities can be found in the Good Practice Guidelines 2018 Edition.



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.





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:



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.

The following are general principles to analysis;

Business Impact Analysis

The BIA can initially help to clarify the scope of the business continuity programme, and then be used to determine and select business continuity solutions.

Risk and Threat Assessment

This is used to identify unacceptable levels of risk and single points of failure. Risk and threat assessments enable effective solutions and mitigation measures to be designed.

Final Analysis and Consolidation

Once all BIAs have been undertaken, final analysis and consolidation is used to validate the information.

Further information on these activities can be found in the Good Practice Guidelines 2018 Edition.



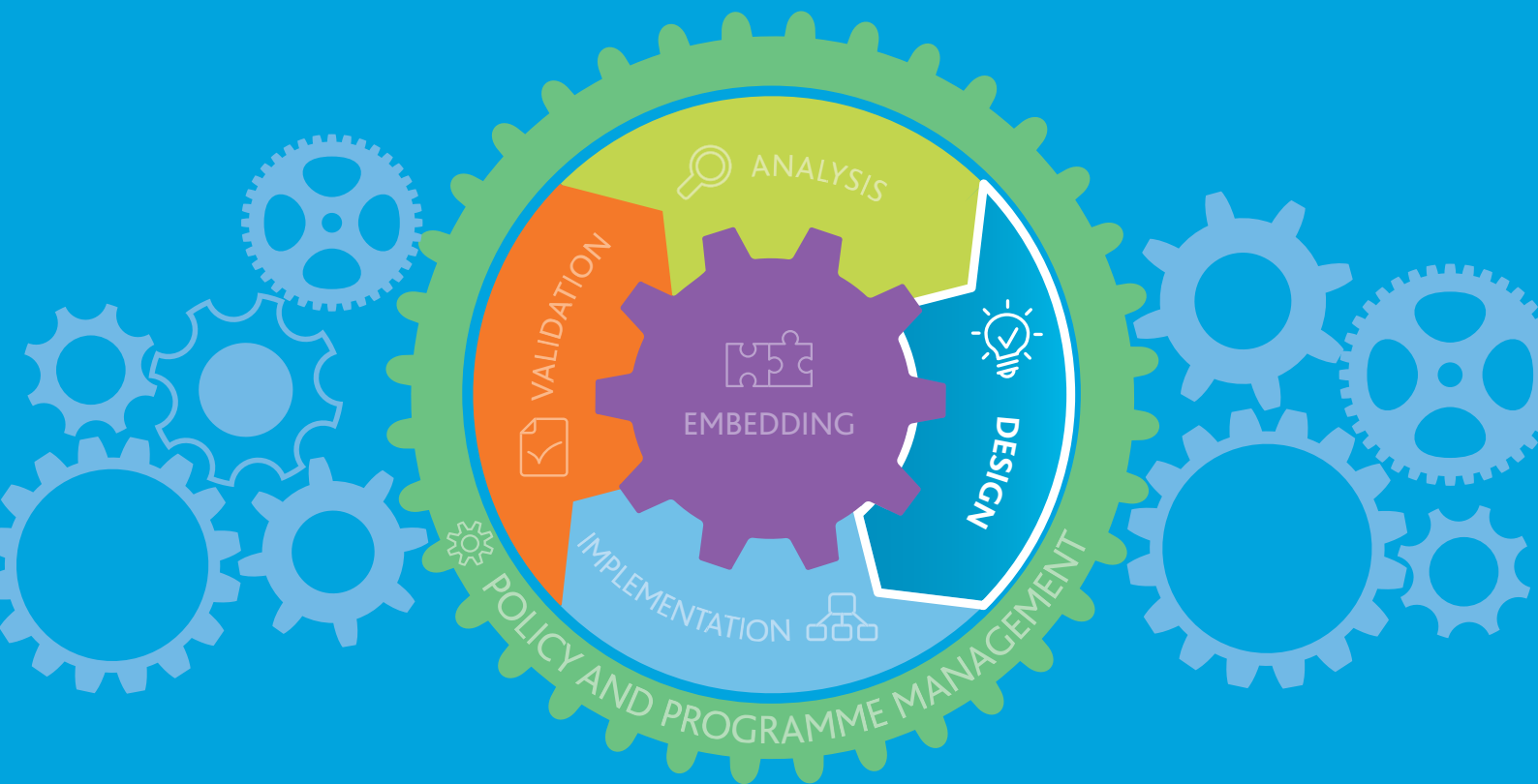
BCI Professional Practices

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.





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, as identified in the Analysis stage.

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.

The following should be considered when designing business continuity solutions;

Designing Business Continuity Solutions

These solutions are based on the outcomes of the risk and threat assessments. Price versus performance and cost versus benefit are often used when designing solutions.

Risk and Threat Mitigation Measures

These are identified and implemented to reduce the impact of a disruption to the organization's prioritised activities. Collaboration with risk, physical security, and information security professionals should be undertaken at this stage.

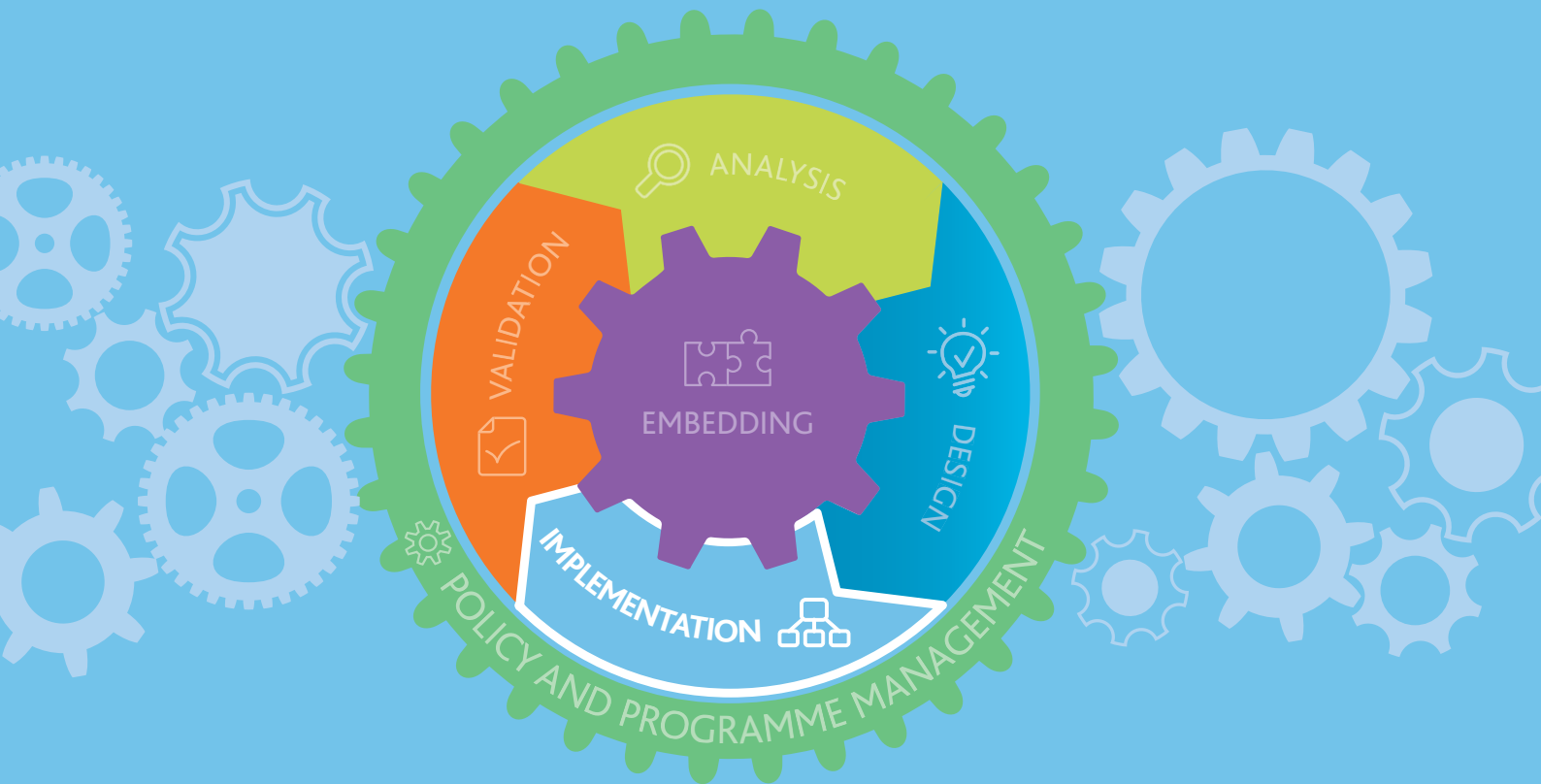
Further information on these activities can be found in the Good Practice Guidelines 2018 Edition.



PP5

Implementation

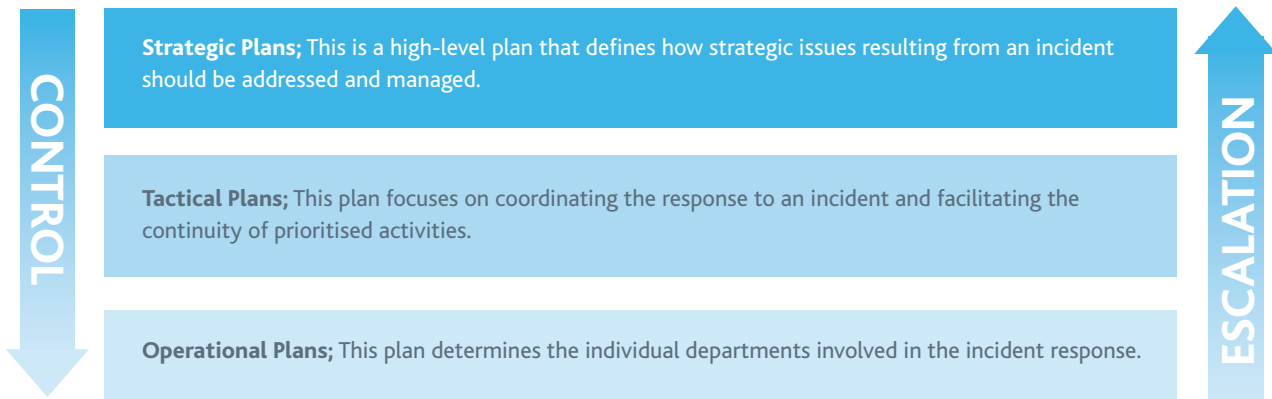
Implementation is the Professional Practice within the business continuity management lifecycle that implements the solutions agreed in the Design stage. Implementation is achieved by developing business continuity plans to meet the organization's agreed business continuity requirements and solutions 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 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 three levels of plans are as follows;



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.

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.

The following are elements of the Implementation stage;

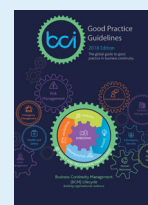
Response Structure

This process established command, control and communication systems to ensure that the organization has a clearly documented and well understood mechanism for responding to an incident, regardless of its cause.

Developing and Managing Plans

Business continuity plans can be created to address the strategic, tactical, and operational requirements of the organization. The plans should be determined by the response structure and business continuity solutions agreed in the Design stage.

Further information on these activities can be found in the **Good Practice Guidelines 2018 Edition.**



BCI Professional Practices

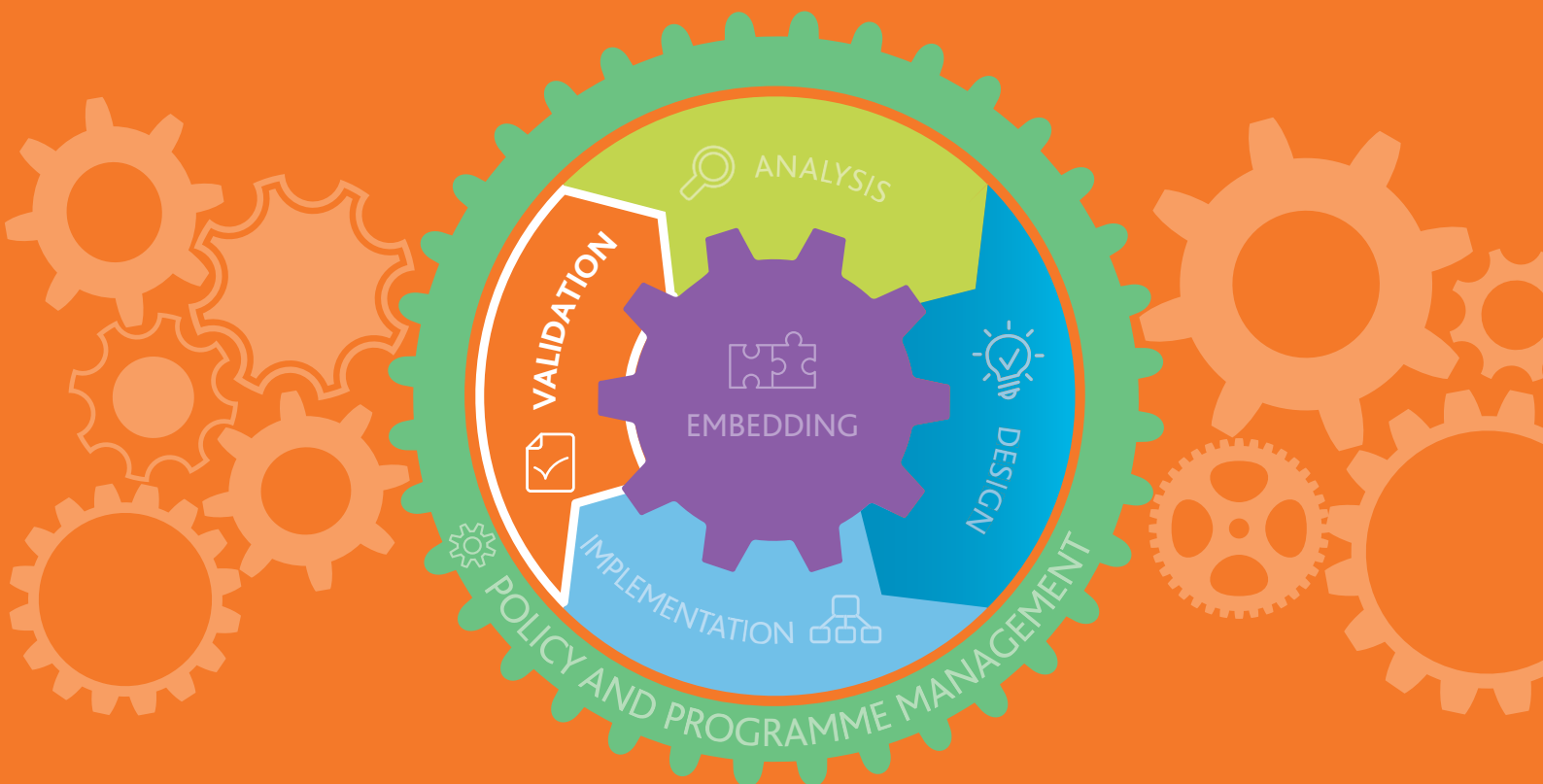
PP6



Validation

Validation is the Professional Practice within the business continuity management lifecycle that confirms 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.





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

Exercising

A process to train for, test, assess, practice, 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.

The following are key activities in the Validation stage;

Developing an Exercise Programme

In order to be validated, the selected solution or plan must be exercised. The goal is continuous improvement of business continuity management capabilities through ongoing validation.

Developing an Exercise

Individual exercises within the exercise programme should be planned like a project, to justify the resource requirements.

Maintenance

Maintenance of the business continuity programme ensures that the organization remains ready to respond to incident, despite organizational change over time.

Review

This stage evaluates the business continuity policy and programme for continuity suitability, adequacy and effectiveness.

Further information on these activities can be found in the Good Practice Guidelines 2018 Edition.



Next steps

Now you have an understanding of the business continuity management lifecycle, you can progress onto the full Good Practice Guidelines 2018 Edition for more in-depth understanding.

Sitting BCI's Certificate of BCI exam provides you with a reputable post nominal designation which is recognised by organizations on a global basis.

The following options are available to students looking to advance their understanding of business continuity and organizational resilience;

CBCI Classroom Course

This classroom course lasts between 4 and 5 days and can be sat with one of our training partners around the world.

CBCI Online

This 8-week course runs in collaboration with Bucks University on an interactive e-learning system. You will receive 32 hours of training with an expert tutor.

CBCI Exam

You can sit the exam in person at the end of the CBCI Classroom course or from the comfort of your own home.

Additional training courses

We offer Professional Practice specific training courses, all delivered by experts in their field. Topics include;

- IT Disaster Recovery
- Introduction to Business Continuity
- Introduction to Organizational Resilience
- Incident Response and Crisis Management
- Business Impact Analysis
- Designing and Delivering Effective Exercises
- Supply Chain Resilience
- Designing Continuity Strategies
- Developing and Managing a Business Continuity Plan



Find out more
www.thebci.org



BCI Membership Grades





Good Practice Guidelines

2018 Lite Edition

Highlights of the global guide to good practice in business continuity.



Central Office

BCI

10-11 Southview Park,
Marsack Street,
Caversham,
Berkshire
RG4 5AF, UK

Tel: +44 (0) 118 947 8215

www.thebci.org

bci@thebci.org