Business Continuity Guidance

A WALK THROUGH OF THE KEY STAGES OF THE BUSINESS CONTINUITY LIFECYCLE

ecclesiastical

Contents

Introduction

Business continuity is relevant and applicable to every organisation regardless of size and complexity. An effective business continuity programme ensures that you can respond to threats and incidents effectively, continue to deliver your strategic objectives and includes:

- the identification of priorities and solutions to potential threats and disruptive events
- the creation of appropriate response structures and plans and,
- promotes validation and continuous improvement.

1 Policy and programme management

Establishing the Business Continuity Policy

The Business Continuity Policy sets the boundaries and needs of the Business Continuity Programme. It outlines the reasons for implementing business continuity and the key principles to follow. It covers how you should build and maintain the programme to ensure that you can continue to deliver your key products and services in the event of a business interruption.

When developing your Business Continuity Policy you may wish to include:	
A definition of business continuity	What is it?
A commitment from senior management	Why it is important?
Objectives	What is the desired outcome?
Scope	What is included and what is not?
Roles and responsibilities	Who is responsible and for what?
Reference to other policies	How does this link to other policies and documentation?
Stakeholders	Who should be included in the creation and sign-off of the policy?
Measurement and review	How will the Business Continuity Management (BCM) approach be measured and reviewed?
Approval	Who has final approval?
Communication	How will it be communicated?

Defining the scope of the Business Continuity Programme

The Business Continuity Policy should clearly define the scope of your Business Continuity Programme. It should clarify which products and services are included and which are not.

When determining the scope of your Business Continuity Programme you may wish to consider:	
Products and services	Which are the most important - Those that make the most income? Those which contribute to your reputation? Where are they delivered from?
Legal and regulatory landscape	What legal or regulatory requirements do you need to follow?
Contracts	What contracts do you have in place?
Physical threats	What physical threats do you face e.g. risk of flooding?

It is important to agree the scope before progressing to the **Analysis, Design, Implementation** and **Validation** stage of the business continuity lifecycle.

Establishing Governance

Good governance is a key part of business continuity management. It is important to have a central point of accountability for implementation and continuous monitoring of your activities in line with your Business Continuity Policy.

When establishing your governance activities you may wish to focus on:	
Oversight and resources	Who will provide oversight and resources to support your Business Continuity Programme?
Accountability	Who will be accountable for ensuring the Business Continuity Programme complies with the Business Continuity Policy?
Monitor and review	Who will monitor and review the Business Continuity Programme? How often will this be carried out?

Roles and responsibilities

Clearly defining roles and responsibilities e.g. management, steering group, business continuity plan owner, incident response staff etc. is a key element to support an effective Business Continuity Programme. These roles and responsibilities will have been outlined in your Business Continuity Policy.

It is important that a member of senior management has overall accountability for business continuity and its effectiveness. Having the commitment from the top will ensure that business continuity is recognised as a key activity and it will be implemented through collaboration with all parts of your organisation.

When defining roles and responsibilities you may wish to consider:	
Assigning roles	Do you have people in mind? Do they have the appropriate competencies and skills? Is additional training required?
Resilience	Do you have alternate staff in place to provide additional resilience if key business continuity staff are not available?
Monitor and review	Have business continuity responsibilities been included in relevant job descriptions? Has this been communicated to key stakeholders? Do you have a process in place to monitor and review performance?

The Business Continuity Programme

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.

It is an ongoing process which adapts in response to the changing nature of your internal and external environment. When implementing a programme for the first time you should involve all activities detailed in the Business Continuity Management (BCM) Lifecycle (see below diagram). Managing documentation is also a key element of the process.

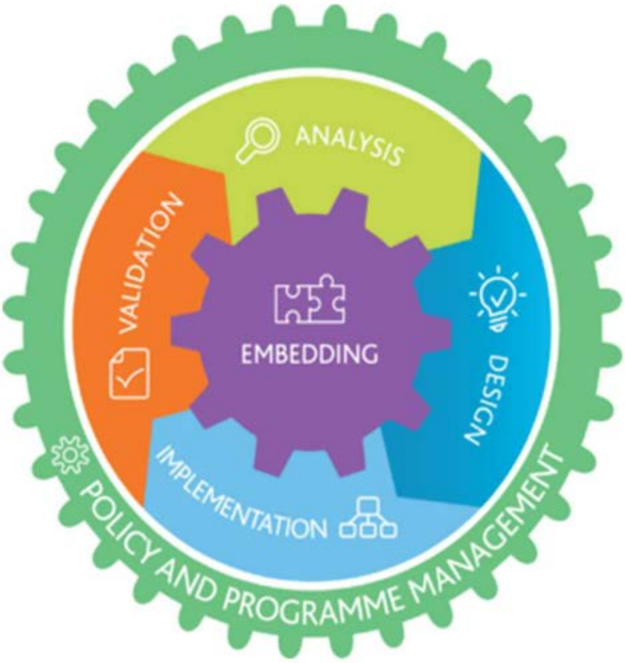

Image taken from BCI Good Practice Guidelines - 2018 Edition: The global guide to good practice in business continuity

A flexible and comprehensive programme is needed to ensure you maintain business continuity capability and continue to develop organisational resilience.

When developing your Business Continuity Programme you may wish to consider:	
Business Continuity Policy	Does your Business Continuity Programme support your Business Continuity Policy?
BCM Lifecycle	Has sufficient time and resources been allocated to work through the whole BCM Lifecycle?
Documentation	Do you have in place an agreed approach to manage your Business Continuity Programme documentation e.g. Business Continuity Policy, Business Continuity Programme of activities, Business Impact Assessment (BIA) information, Risk Assessments, Business Continuity solutions, Response structure, Business Continuity Plans, Crisis management plans, Exercise and review documents?
Adaptability	Is your Business Continuity Programme ongoing and adaptable to deal with changes to your organisation's internal and external environment?

2 Embedding

Understanding and influencing organisational culture

Successful embedding of an effective Business Continuity Programme may require changes in the culture of your organisation. Senior management and the business continuity professional need to work together to ensure that business continuity is seen as a priority, is aligned to strategic objectives and is integral to how you operate.

When thinking of your organisational culture/embedding business continuity you may wish to consider:	
Strategic planning	How does business continuity align/support strategic planning?
Operational procedures	How is business continuity embedded into operational procedures?
Meetings	Does business continuity feature as a standing agenda item at relevant meetings?
Induction	Is business continuity a key part of your induction programme?
New products or services	Is business continuity considered at the planning stage when entering into new products or services?

Competencies and skills

It is important that staff with responsibility for business continuity have the appropriate training and experience required to develop and implement your Business Continuity Policy and Programme. Senior Management should provide appropriate resources to cover current and ongoing training to ensure relevant skills and competencies are maintained.

When thinking about the competencies/skills for business continuity you may wish to focus on:	
Skills and competencies	Have the skills/competences for business continuity roles been identified?
Resources	Have appropriate levels of resources been assigned to support your business continuity programme?
Budget	Has a budget been allocated to support business continuity?
Training	Has a budget been allocated to support business continuity training?

3 Analysis

Business Impact Analysis (BIA) – Products and Services, Processes and Activities

BIA is the main technique used by organisations to determine their business continuity requirements. If you have not completed one already, an initial BIA should be undertaken to determine your key products, services, processes and activities. Once complete you may wish to undertake more detailed analysis through either a product and services BIA, a processes BIA or an activity BIA. No one approach is better than another and a combination may be more appropriate, depending on the size and complexity of your organisation.

Further details on the different types of BIA can be found on the Business Continuity Institute (BCI) Website **https://www.thebci.org**/ and BCI Good Practice Guidelines 2018 Edition: The global guide to good practice in business continuity **https://www.thebci.org/resource/good-practice-guidelines--2018-edition-.html.**

The BIA should identify all critical products and/or services and the impact of not providing them over time due to an incident. It should also determine the tolerable downtime and the minimum resources required to get those products and/or services back up and running.

An example BIA template (using a combined approach) can be found at Appendix A.

When conducting your BIA (whatever approach you use) you may wish to consider:	
Key product and services	Do you have a list of your key products and/or services?
Processes and activities	Do you understand which processes and activities support your key products and/or services?
Impact	Are you clear what the impact would be if the key product and/or service was not delivered?
Maximum Tolerable Period of Disruption (MTPD)	Have you defined your MTPD - the maximum time period in which you must recover your product or service to avoid adverse impact?
Minimum Business Continuity Objective (MBCO)	Have you defined your MBCO - the minimum level of service/and or product that is acceptable to achieve business objectives during a disruption?
Recovery Time Objective (RTO)	Have you defined your RTO - the time period in which you aim to recover your key products and/or services in line with your MBCO?
Resource requirements	Have you identified the resources required to support those processes/activities linked to your key products and/or services?
Internal or external dependency	What internal/external services and/or products are necessary for the delivery of your key products and/or services?

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.

Risk and threat assessment

A risk and threat assessment considers the risk of disruption due to various threats. The risk assessment typically involves methods to identify, analyse and evaluate a range of risks relevant to you.

If you have an established risk management function, information may already be available that will support this part of the process.

When conducting your risk and threat assessments you may wish to consider:	
Internal and external threats	Have these been identified?
Impact	Have you assessed the impact of each threat on your organisation?
Probability	Have you determined the probability of the threat occurring?
Threat score	Have you calculated the threat score e.g. impact x probability (use your existing risk matrix)
Prioritise	Have you prioritised the threats based on your risk score?
Share findings	Have you shared the output of the Risk and Threat Assessment with key stakeholders?
Information	Have you used 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?

4 Design

Designing Business Continuity Solutions

The BIA and outcomes from the Risk and Threat Assessment should inform your Business Continuity Solutions (or strategies). Your Business Continuity Solutions will identify how your organisation is going to continue to operate following a disruption.

There are a number of well-established Business Continuity Solutions:

- Diversification
- Replication
- Stand-by
- Post incident acquisition
- Doing nothing.

The above list has been taken from the BCI Good Practice Guidelines - 2018 Edition: The global guide to good practice in business continuity.

Organisations will usually find the best outcome stems from combining a mixture of business continuity solutions, so the solutions reflect the priority and recovery time objectives of the processes and activities.

Further details on the different types of solutions can be found on the Business Continuity Institute (BCI) website **https://www.thebci.org/** and BCI Good Practice Guidelines 2018 Edition: **https://www.thebci.org/resource/good-practice-guidelines--2018-edition-.html**

When designing your Business Continuity Solutions you may wish to consider:	
BIA	Have you used the information from your BIA to inform your Business Continuity Solution?
Threat and Risk assessment	Have you used the information from your Threat and Risk assessment to inform your Business Continuity Solution?
Business Continuity Solutions	Are you clear what Business Continuity Solutions are available?
Cost vs benefits	Have you carried out a cost benefit analysis to inform your choice of Business Continuity Solutions?

Risk and Threat mitigation measures

Mitigation measures should be identified and implemented to reduce the impact of any disruption to your prioritised activities. Measures selected should be targeted at unacceptable levels of risk, any single points of failure, and the main threats to your prioritised activities. All of these are identified in the **Analysis** stage of the Business Continuity Management Lifecycle.

When considering your Risk and Threat mitigation measures you may want to consider:	
Costs	Are the costs acceptable when looking at the benefit gained?
Targeting	Are you targeting mitigation measures at unacceptable levels of risk and any single points of failure?
Mitigation measures	Have you thought through what measures can be put in place to reduce the risk or threat e.g. physical security to prevent theft and unauthorised entry, information security to prevent loss of data, monitoring systems to provide warning of fire and equipment failures and sprinkler and fire suppression systems to prevent fire from spreading?

5 Implementation

Response structure

It is important to have a response structure in place should an incident occur. The response to an incident (regardless of its cause) should be clearly documented and well understood. The response structure establishes command, control and communication systems to help you manage an incident and minimise the impact of any disruption.

The response structure should be closely aligned with your existing management structure as this will help embed business continuity into the organisation.

There can be different types and levels of response teams in an organisation's response structure. Response teams should address the strategic, tactical and operational levels which are appropriate to you.

Strategic team	▪ The strategic team focuses on strategic issues that impact your core objectives, and products and services and is usually led by management ▪ The strategic team is often called a crisis management team and has primary responsibility for addressing any crisis impacting the organisation .
Tactical team	▪ The tactical team manage and co-ordinate 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.
Operational team	▪ 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 immediate effects of an incident by containing it where possible and managing the direct consequences.

The above table has been taken from the BCI Good Practice Guidelines - 2018 Edition: The global guide to good practice in business continuity.

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

When considering your response structure you may want to consider:	
Management structure	Is your response structure aligned to your existing management structure?
Skills and competencies	Do you have the appropriate skills and competencies within your response structure team(s)?
Communication	Are communication channels clear?
Escalation	Do you know when to escalate between response teams?
Size and complexity	Is your response structure in line with the size and complexity of your organisation?
Continuity solutions	Are your response team(s) clear on the agreed Business Continuity Solutions to deal with each threat?

Developing and managing plans - Strategic, Tactical and Operational

Business Continuity Plans should be created to address your strategic, tactical and operational requirements. The number and type of plans to be put in place should be determined by the response structure and Business Continuity Solutions agreed.

Plans are intended to be used in high pressure, time limited situations and should be direct, adaptable, concise and relevant.

Strategic	▪ Supports management during an incident or crisis ▪ Manages interested parties and media communications during a crisis ▪ Documents your approach to business continuity at a strategic level ▪ Ensures compliance with legal and regulatory requirements.
Tactical	▪ Supports tactical teams during an incident or crisis ▪ Provides a framework for co-ordination of response activities and resource allocation between strategic and operational plans ▪ Provides guidelines for co-ordinating Business Continuity Solutions and response activities with interested parties.
Operational	▪ Supports the continuity of prioritised activities at an operational/ departmental level following an incident ▪ Documented plans for the continuity of key infrastructure and support services e.g. technology, equipment, facilities and resources.

The above table has been taken from the BCI Good Practice Guidelines - 2018 Edition: The global guide to good practice in business continuity.

When developing your plans you may want to ensure they contain:	
Purpose and scope	Why are you doing this? What products and services are included or excluded?
Objectives and assumptions	What do you hope to achieve? What assumptions are you making?
Plan activation criteria	How will the plan be activated? Do you have an agreed procedure in place? Has the procedure been communicated and fully understood?
Meeting locations	Where will the response team meet? What location and room? On site? Off site? Does the site and room have all the equipment you may need to use?
Roles and responsibilities	Have roles and responsibilities been clearly defined during an incident? Are people clear what they need to do?
Prompts for immediate action	Is there a set of prompts to refer to for immediate action during that first hour of an incident - often referred to as the golden hour? **See Appendix B.**
Communication requirements	Is there a crisis communication plan in place which outlines how you should communicate during and after a crisis or incident?
Internal and external interdependencies	Are you clear what internal and external interdependencies are linked to your key products and services? Do you have a Plan B to deal with these e.g. alternative suppliers?
Summary of the organisation's prioritised activities and resource requirements	Are you clear what products and services are a priority and the processes and activities required to support them? Are you clear what resource requirements are needed to ensure these prioritised products and services are maintained during a disruption?
Agreed Business Solution (or strategy)	Are you clear what Business Solution has been agreed to deal with each of the key threats you face?
Decision support checklists	Do you have a list of tasks/actions to support the agreed Business Solution that can be followed (as a guide) during a disruption?
Standing down	Is there a procedure in place to stand down the team and organisation once the incident has been resolved?
Supporting appendices	Do you have access to additional information e.g. Site Plans, Disaster Recovery Plan, Communications Plan, Internal and External Contact Details, Action Log
Plan approval and distribution	Has the plan been formally approved with an agreed distribution list?

Communications

The communication response during a crisis or incident is usually guided by management, working with specialist communication teams within an organisation. Depending on your response structure you may have a separate communications plan.

When considering communications in a crisis you may wish to consider:	
Management	Which member of the management team will oversee your response to communications during a crisis?
Internal or External	How will communications be managed during a crisis e.g. internal (staff, volunteers and senior management/board) or external (customers, shareholders, media, neighbours)?
Crisis Communications Plan	Do you have a crisis communications plan you can refer to? Do you have guidelines for dealing with the media? **See Appendix C.**

6 Validation – Exercising, maintaining and reviewing

Developing an Exercise Programme

Your business continuity capability can only be considered reliable or effective following some kind of exercise or test. Testing your plan will demonstrate how effective your strategies are and how prepared your key people are to respond. Gaps and weaknesses will be present in even the most comprehensive plans: testing reveals where the strengths and weaknesses are and supports continuous improvement. There are numerous ways to exercise or test your plans:

Discussion based exercises	These exercises are the simplest to organise 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.
Scenario exercises	A scenario exercise is a commonly used discussion based activity, using a relevant scenario with a time frame (usually table top). This exercise may either run in real time or include time jumps to allow different phases of the scenario to be exercised.
Simulation exercises	Simulation exercises are more elaborate and can involve teams at a strategic, tactical and operational level. Participants can be located across the whole organisation, all working from their usual locations. During a simulation exercise participants are given information in a way that simulates a real incident.

Live exercise	Live exercises can range from a small scale rehearsal of one part of the response e.g. an evacuation, to a full scale rehearsal of the whole organisation, potentially involving interested parties in real time. Live exercises are designed to include everyone likely to be involved in that part of the response.
Test	A test is defined as a 'unique type of exercise' which incorporates an expectation of a pass or fail element. It usually is applied to equipment, recovery procedures or technology.

The above table has been taken from the BCI Good Practice Guidelines - 2018 Edition: The global guide to good practice in business continuity.

Maintenance

Maintenance is an important part of the Business Continuity Programme. It will ensure your plans are up-to-date and ready to respond to and manage a business interruption. To be effective, maintenance activities should be embedded within your business as usual processes rather than being a separate activity that may be overlooked.

Plans should be updated following any exercise, test or live incident to incorporate lessons learned and reflect any resultant changes in your organisation's structure or operating environment. You will need to maintain your plans following any exercise or test, if there are any changes to your organisation's structure or operating environment, following a review or audit or after a real incident where lessons learned can be incorporated.

Review

The purpose of the review is to evaluate the suitability, adequacy and effectiveness of your Business Continuity Policy and Programme. A review can take many forms e.g. audit, self-assessment, quality assurance, performance appraisal, management review. The outcome of any review will lead to an action plan for improvement of the Business Continuity Programme and an enhancement of your resilience level.

When validating your business continuity approach you may want to consider:	
Exercising	Are you clear what approach you will use to exercise or test your plan?
Maintenance	Are you clear how you will maintain your plan as part of normal business processes?
Review	Have you agreed an appropriate method of review to evaluate your Business Continuity Policy and Programme?

Appendices

Appendix A: BIA example template /example template completed

Appendix B: Risk categories

Appendix C: Crisis response checklist

Appendix D: Glossary of terms

Appendix A: BIA example template

Product or service	▪ Identify and prioritise your key product or service.
Processes / Activities	▪ Identify the processes and/or activities required that support your key product or service.
Impact if Product or Service lost over time	
First 24 hours	▪ Identify impact if lost over time e.g. legal, financial, reputational.
2-3 days	▪ As above.
Up to 1 week	▪ As above.
Up to 2 weeks	▪ As above.
Maximum Tolerable Period of Disruption (MTPD)	Consider the impacts above and determine the MTPD - the maximum time period in which you must recover your products or services to avoid an adverse effect on your business (often driven by customer feedback).
Minimum Business Continuity Objective (MBCO) - quantity	Consider the impacts above and determine the minimum level of service/and or products that is acceptable to achieve business objectives during a disruption.
Recovery Time Objective (RTO) - time	Consider the impacts above and determine the RTO – the time you aim to recover your key products or services in line with your MBCO (less than the MTPD).

Resource requirements to support those processes or activities linked to the key product or service (in line with the MBCO and RTO)					
Time	No. of staff	Data/IT	Buildings	Equipment	Other e.g. Finance
First 24 hours					
2-3 days					
Up to 1 week					
Up to 2 Weeks					

Appendix A: BIA example template (completed)

Product or service	▪ Customer service centre.
Processes / Activities	▪ Answering calls (both internal & external) ▪ Responding to queries on the website ▪ Responding to queries on social media.
Impact if Product or Service lost over time	
First 24 hours	▪ Limited or no customer interaction.
2-3 days	▪ Limited or no customer interaction ▪ Minor loss of revenue ▪ A few customer complaints.
Up to 1 week	▪ Limited or no customer interaction ▪ Moderate loss of revenue ▪ Significant number of customer complaints ▪ Reputation impact.
Up to 2 weeks	▪ Limited or no customer interaction ▪ Major loss of revenue ▪ Increasing number of customer complaints ▪ Loss of customers ▪ Reputation damage.
Maximum Tolerable Period of Disruption (MTPD)	2-3 days.
Minimum Business Continuity Objective (MBCO) - quantity	50% capacity.
Recovery Time Objective (RTO) - time	First 24 hours.

Table continued below

Resource requirements to support those processes or activities linked to the key product or service (in line with the MBCO and RTO)					
Time	No. of staff	Data/IT	Buildings	Equipment	Other e.g. Finance
First 24 hours	2 Call handlers	Remote access to network	Alternative site or home	2 x Desk, Chair Laptop, Mobile phone	
2-3 days	4 Call handlers	As above	As above	4 x Desk, Chair Laptop, Mobile phone	Access to H&S officer
Up to 1 week	Beyond MTPD				
Up to 2 Weeks	Beyond MTPD				

Appendix B: Crisis response checklist (The golden hour)

Action	Completed
▪ Determine nature of incident and extent of impact.	
▪ Evacuate if necessary e.g. alarm, assembly points.	
▪ Check that all employees, volunteers, contractors and any visitors have been evacuated from the building(s) or site and are present/in a safe place.	
▪ Treat any casualties e.g. use of trained first aiders, safe location (report to HR).	
▪ Agree location of the Crisis Management Team meeting venue.	
▪ Call up members of the Crisis Management Team to attend the meeting venue.	
▪ Identify and invoke the relevant Business Continuity Solution for the incident e.g. Loss of Site.	
▪ Implement the relevant Plan for the incident – focus on maintaining those critical activities identified in the BIA process.	
▪ Open an incident log to record key actions and decisions taken.	
▪ Liaise with Emergency Services.	
▪ Consider any hazardous substances e.g. asbestos in buildings, release of chemicals.	
▪ Liaise with utilities e.g. electricity, gas, water.	
▪ Contact key suppliers, customers and/or partners.	
▪ Protect property (if safe to do so) e.g. site security to be arranged.	
▪ Consider both internal and external communications e.g. social media, telephone, email, message on incoming phone line, intranet, website.	
▪ Deal with the media – refer to crisis response plan if appropriate.	
▪ Notify the Insurance Broker/Insurance Company of the incident e.g. location, nature, time of occurrence, details of circumstances, extent of damage, current situation.	
▪ Agree frequency of regular meetings/briefings.	

NB. This list is not exhaustive

Appendix C: Crisis communications checklist

No	Action	Completed
1	Do you understand what has happened?	Before you begin talking to the media and your customers, there needs to be clarity on what has taken place? You need to be exactly sure what has happened so far.
2	Is everyone on your crisis team aware?	It's important to contact all members of your crisis team as soon as possible. They will have been allocated certain roles in the event of a crisis or incident.
3	Do you have holding statements you can use?	Getting messages out promptly, even if initially through a simple holding statement, will show that you are in control of the situation and are taking it seriously. But always stick to what you know at the time. It will also help prevent the spread of speculation and rumour.
4	Are you logging media interest?	It's important to record where media interest is coming from and what is being reported. This will help you to challenge inaccuracies, identify themes, understand where information is coming from and know what needs to be covered in future statements and media interviews.
5	Other organisations?	If other organisations are involved in the crisis do you know who the relevant communications people are? Are they aware of the situation? Have you agreed messages and an approval process? How will any joint approval process work with your own internal sign off?
6	Are you keeping information flowing?	In the high pressure atmosphere of a crisis it can be tempting to view the media as the enemy and try to say as little as possible. Your holding statement is only going to last for so long - so make sure you are on the front foot by continuing to release details and information at regular intervals. Let journalists and your customers know when and where then can expect updates and you'll find it eases the pressure on the communications team. Failure to provide regular updates will only see the media fill the void.
7	Are you showing you care?	You need to show your customers and potential future customers that you understand the severity of what has happened and the impact it has had. Ensure all your communications show compassion, concern, honesty and empathy.
8	Have you identified your spokespeople?	It is often assumed that the most senior member of staff will front a crisis, but they may not always be the best person to put in front of the media. Depending on the situation you may require an individual with more specialist knowledge on the type of incident.

9	Do you require a regional spokesperson?	If the crisis centres on a regional centre, using a media trained spokesperson from that site may be beneficial. Not only are there logistical benefits but it can help you engage and win the trust of the audience and show a commitment to the area and the people who live there.
10	What is being said on social media?	As well as meeting the demands of the media, you are now faced with a range of extra channels to monitor, manage and feed. The huge growth in social media also means a crisis is likely to reach the mainstream media much quicker than before. Your customers will start tweeting and posting information about your crisis as soon as it happens and journalists will quickly get a lead for a story. As with mainstream media, you need to monitor what is being said effectively, respond quickly, provide regular updates and again communicate with compassion, concern, honesty and empathy.
11	Press Conference?	If your crisis attracts a lot of media attention and you want to hold a press conference do you have a suitable venue in which to do so? Does it have a clear escape route for your spokesperson at the end of proceedings? Is there adequate parking for journalists? Effective crisis communication training often includes press conference training so make sure your team is fully media trained.
12	Out of hours contacts?	There's every chance a crisis may strike outside normal working hours or that media interest continues beyond the traditional working day. Do the media know how to contact you out of hours? Is this contact information available on your website?
13	Are you communicating internally?	It can be all too easy to focus on your external messages during a crisis and forget about your internal communications. But your employees are ambassadors and can be strong advocates. Ensure staff know what you are doing to deal with the situation before they hear about it in the media. Be honest and ensure visible leadership. An engaged workforce is less likely to give potentially damaging information to a journalist or post something unhelpful on social media. Make sure they know what to do if approached by a reporter.
14	What can you learn from the crisis?	After a crisis it is important to look at what worked well and where improvements could be made. Would you do things differently if faced by a similar situation in the future? Would you use the same spokesperson? Do your spokespeople need more media training? Do you need to look at different social media monitoring?

NB. This list is not exhaustive

Appendix D: Glossary of terms

Term	Definition	Source
Activity or activities	One or more tasks undertaken by, or for an organisation, that produces or supports the delivery of one or more products or services.	Good Practice Guidelines (GPG) 2018
Business Continuity (BC)	The capability of the organisation to continue to delivery products or services at acceptable pre-defined.	ISO 22300:2012
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational 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 Plan (BCP)	Documented procedures that guide organisations 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 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
Incident	A situation that might be, or could lead to, a disruption, loss, emergency or crisis.	ISO 22300:2012
Interested party	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.	ISO 22301:2012

NB. This list is not exhaustive

Term	Definition	Source
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.	ISO 22301:2012
Minimum Business Continuity Objective (MBCO)	The minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption.	ISO 22301:2012
Policy	The business continuity policy provides the intentions and direction of an organisation as formally expressed by its management.	ISO 22301:2012
Process	A set of interrelated or interacting activities which transforms inputs into outputs.	ISO 22301:2012
Products and Services	Beneficial outcomes provided by an organisation 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, premises and supplies that an organisation 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	Co-ordinated activities to direct and control an organisation.	ISO/IEC Guide 73
Threat	A potential cause or an unwanted incident, which can result in harm to individuals, the environment or the community.	ISO 22300:2012
Test	An exercise whose aim is to obtain an expected, measureable pass/fail outcome.	ISO 22300:2012

This guidance is provided for information purposes based on Enterprise Risk Management best practice and is general and educational in nature.

It does not constitute legal advice. You are free to choose whether or not to use it and it should not be considered a substitute for seeking professional help in specific circumstances.

You acknowledge that over time, this guidance may become out of date and may not constitute best market practice.

Accordingly, Ecclesiastical and its subsidiaries shall not be liable for any losses, damages, charges or expenses, whether direct, indirect, or consequential and howsoever arising, that you suffer or incur as a result of or in connection with your use or reliance on the information provided in this guidance except for those which cannot be excluded by law.

Ecclesiastical Insurance Office plc
Benefact House
2000 Pioneer Avenue
Gloucester Business Park
Brockworth, Gloucester GL3 4AW
www.ecclesiastical.com

Our Enterprise Risk Management (ERM) support is a non-regulated activity providing optional support to you outside of our insurance products.