**Unit 2: Crisis and Disaster Management**

There is extensive research into the field of crisis management, but disaster recovery can appear to be of less interest to researchers and academics, even though it is argued that there is a symbiotic relationship between the two. In this part of the unit, we will be studying both aspects, including the journey from crisis to disaster.

The first question that should be asked is “What is meant by the term ‘crisis?’. Fink (2002) argues that Webster’s (Dictionary) defines a crisis as a “turning point for better or worse”; as a “decisive moment” or “crucial time.” It also defines a crisis as “a situation that has reached a critical phase.” Fink goes on to argue that a crisis is an unstable time or state of affairs in which a decisive change is pending - either one with the distinct possibility of a highly undesirable outcome, or one with the distinct possibility of a highly desirable and extremely positive outcome.

The International Federation of the Red Cross (2016) defines a disaster as:

...a sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community’s or society’s ability to cope using its own resources. Though often caused by nature, disasters can have human origins.

For the purposes of this training course, and from a practical, business-oriented point of view, a crisis is any prodromal situation that runs the risk of:

Escalating in intensity

Falling under close media or government security

Interfering with normal operations

Jeopardising the positive public image presently enjoyed by a company or its officers

If any or all of these developments occur, the turning point most likely will take a turn for the worse. Therefore, there is every reason to assume that if a situation runs the risk of escalating in intensity, that same situation, if caught and dealt with in time, may not escalate. It is generally agreed that there are three stages to a crisis, and ultimately its management.

**Pre-crisis**

* **Avoiding the crisis**     
  The first stage, not surprisingly, is prevention. Amazingly, it is sometimes skipped altogether, even though it is the least costly, and the simplest way to control a potential crisis. The problem may be that crises are accepted by many executives as an unavoidable condition of every day existence.
* **Preparing to manage the crisis**         
  Most executives, pre-occupied with the market pressures of the present quarter, are not inclined to pay much attention to planning for future crises. This brings us to the second stage of crisis management: preparing for that circumstance when prevention does not work - that is, making a plan to deal with a variety of undesirable outcomes.  
     
  Steve Fink, a prominent management consultant, wrote in his book Crisis Management (2002) that a survey of the Fortune 500 (USA) CEO’s found that senior managers may suffer from a severe lack of crisis preparedness, but certainly not from a lack of confidence that they can handle a crisis. Eighty-nine percent of those who responded to the survey said that crises in business, are as inevitable as death and taxes, yet 50% said that they did not have a plan for dealing with crises.
* **Recognising the crisis**  
  The third stage of crisis management is often the most challenging; recognising that, in fact, there is a crisis. Executives who refuse to face reality should be mindful of the bright, if inexperienced chemistry student who warned, “When you smell an odourless gas, it is probably Carbon Monoxide.”  
     
  In general, you need to understand how others will perceive an issue, and to challenge your own assumptions. Organisations sometimes misclassify a problem, focussing on the technical aspects, and ignoring issues of perception. However, it is often the public perception that causes the crisis.

A few years ago, petrol tanker drivers were threatening to go on strike, which caused mass public panic buying. There were huge queues at petrol stations which then ran out of fuel and had to shut, and those that still had fuel, capped the limit that users could buy.

In the end the tanker drivers did not carry out the threat to strike.

To read more about the strike threat, please [click here](https://www.theguardian.com/uk/fuel-tanker-drivers-dispute).

The problem in this stage of crisis management is that perception truly does become reality.

**Operational Crisis**

**Containing the crisis**  
The operational crisis stage is when:

* the crisis becomes a reality

This phase of crisis management requires triage. This is the phase in which the tough decisions have to be made and made fast. In the case of the discussed potential petrol tanker drivers’ strike, had the strike been carried out, senior managers would have had to make critical decisions to ensure that petrol and diesel was delivered. This would probably have meant breaking the strike by the use of the military or sub contracted drivers.  
   
Another conclusion is the value of immediately despatching the senior responsible individual to the scene of the problem-usually the CEO. The CEO may know less about the details of the situation than local management, but his or her physical presence sends two important messages: “I care, and I am accountable.”

**Post Crisis Legitimation**

**Resolving the crisis**   
In this phase, speed is of the essence. A crisis simply will not wait. It is during this phase that maximum resources are utilised to end the crisis. Are they justified; are they legitimate. This also refers to the legitimacy of the management structures, including senior personnel responsible for managing the crisis.

Once the crisis is under control, those responsible for its management need to carry out a post mortem, to try to understand what lessons can be learned from how the crisis evolved, and how it was brought under control.

A screenshot of a cell phone

Description automatically generated

**The Crisis Management Plan (CMP)**

According to the **British Standard 11200**, which is the recognised global standard for Crisis Management, the Crisis Management Plan (CMP) is a response document and may set out the following key information:

* Who has authority and responsibility for key decisions and actions in a crisis;
* Key contact details -  how staff are to be contacted in the event of a crisis;
* Crisis communications (internal and external);
* The activation mechanism for a crisis and how it works in practice;
* Details of levels of response across the organisation (i.e. who is to be contacted for what level of problem) and a flow chart showing the sequence of actions;
* The structure and role of the CMT and what is expected of it;
* Where the CMT is to meet (with alternative locations) and what equipment and support are required;
* Key templates (such as CMT meeting agenda and logbook including log-keeping guidance; a situation report template which is to be used across the organisation).

The CMP should be as concise as possible to ensure that:

* It is read and exercised before it is needed, and
* It can be understood and actually used when a crisis breaks.

If required, the plan can be developed to set out the policy and more procedural elements about how the CMT works and the necessary training and evaluation arrangements, but this should not clutter the plan itself.

The CMP should be focused on the provision of a generic response capability. It should not be scenario-specific, as a plan for every possible contingency would be unwieldy, potentially suppress flexible thinking and action, and miss the point that many crises are essentially unforeseeable and impossible to plan for in precise detail.

The following tools and templates support the crisis management plan:

* Aides-memoire and checklists of key decision points and required actions;
* Defined roles and responsibilities;
* Draft holding statements;
* Guidance for call takers and switchboards;
* Up-to-date fact sheets and press kits;
* A list of items necessary for a practical response;
* Tools and systems to help manage social media monitoring and engagement;
* A list of interested parties and a management matrix;
* 24/7 contact information for resources, including spokespeople; and
* Locations for press conferences.

The CMT should generally be formed from the main board or operate with the authority of the board, as this provides strategic vision and the authority to make decisions in crisis situations and enact its leadership function. Individuals with the appropriate level of authority, experience and capabilities should be appointed to the CMT.

Beneath the CMT should be a hierarchy of teams as appropriate, but good practice has established the norm as a strategic CMT, supported by a tactical team(s) and operational team(s). Some small organizations do not need this, but it allows the CMT to remain strategic in its thinking and approach, giving direction to the tactical team for the planningand then the operational team for active implementation.

The size of the CMT varies according to the size of an organization, but typically consists of representatives from top management and key business areas. In the event of an actual crisis, the team may be expanded to include other department heads from those areas more directly affected. Potential roles include the following.

**Chair**

responsible for leading the CMT and acting as the primary contact for the operational elements of the crisis response. The chair should be a strong, authoritative, respected senior executive with a long-term perspective, who is trusted and decisive without being impulsive. It is important to maintain a balance of top management within the CMT that does not leave the wider business without normal leadership whilst the crisis is resolved.

**HR**

ensures that people issues are being addressed. This role-holder should have broad HR expertise or be able to contact an appropriate resource. They should be able to provide quick access to employee data, such as next of kin, and might need to address crisis counselling.

**Operations**

ensures that delivery of the ongoing business priorities is maintained and coordination of this with the crisis response is managed. This function should be able to apply priorities across the organization as needed and allocate additional resources if required.

**Legal**

provides legal counsel to the team and arranges for external legal support as necessary, participates in communication preparation, and advises on other crisis-specific issues, such as ex gratia payments.

**Communications**

coordinates the media response and incorporates legal advice for all public communications. The communications lead is responsible for internal communications and developing press and other media releases, and has a key role in protecting the brand and reputation of the organization.

**Finance**

assesses the financial impact of the crisis and the organization’s response, monitors developments, and advises on/authorizes contingency budgets and emergency spend.

**Log Keeper**

an essential part of the crisis team who maintains a log of all decisions and actions for later reference and use in insurance, liability issues or potential enquiries.

**Business Continuity**

advises on appropriate recovery or contingency plans and alternative resources.

**Other business Teams**

additional support for the core team is provided by internal specialist teams, such as facilities, security, information security and IT, which assess damage and advise on the appropriate recovery plans and available facilities.

**Support Teams**

depending on the extent of the crisis, the chair and CMT could require administrative support, which might include record keeping, tracking documents, updating team members and monitoring information channels.

**Command and Control**

Command and control is a term used to describe the management of an occurrence when there may be danger to life or destruction of property. Most Emergency Service institutes tend to use the Gold, Silver and Bronze approach, which identifies the level of emergency service response required. For instance, a perceived low-level incident, such as a domestic fire, would probably be required to be controlled by the Bronze Teams. Whilst a terrorist attack would instigate the response from a Gold Team.

In all command and control situations, internal and external communications are critical.

Figure 1 below illustrates the operational, tactical and strategic approach to the mentioned command structure.

Figure 1: Gold, Silver and Bronze

Figure 1 below illustrates the operational, tactical and strategic approach to the mentioned command structure.



Figure 1: Gold, Silver and Bronze

**Respond Recover**

**Respond (the CMT in action)**

Given the dynamic and complex nature of crises, it is difficult to predict exactly what actions will be required of the CMT. While certain generic actions will be required (see 1-11 below), crisis management is not a linear activity. Activities might be concurrent, their relative importance can change with events and all should be subject to continuous and rigorous review.

   
Achieving situational awareness, with the team confirming their (individual and shared) understanding of the situation and its dynamics, and continuously reviewing it.

 Defining (and continuously reviewing) the strategic direction of the response.

 Identifying issues, making decisions, assigning actions and confirming the implementation and results of actions.

 Setting an operating rhythm for the response, so that meetings, briefings, information dissemination, press releases, conferences, etc., can be arranged coherently.

 Managing meeting agendas and ensuring brevity.

 Confirming, monitoring and reviewing internal and external communications and strategy.

 Reviewing and monitoring the work of the crisis management organization as a whole, to ensure that priorities are understood clearly and that its performance, and the flow of information, are appropriate to the demands of the situation.

 Examining the impact and management of the crisis on business as normal.

 Carrying out a continuously reviewed analysis of interested parties, to ensure that the right people receive the right messages and information, and that their views, advice and assistance are actively sought.

 Monitoring and reviewing continuously the objectives and effectiveness of any teams managing incidents at other levels of the response, with particular focus on making sure that their activities are in harmony with the strategic crisis response and conflicts of interest or resource are managed.

 Ensuring that strategic planning for recovery starts as early as possible.

**Recover**

The recovery phase involves dealing with the long-term effects or impacts of a crisis and how to return to the new “normal”, or adapt to new circumstances, particularly if major change has taken place in the days, weeks and sometimes months following the crisis. This stage contains many risks and can even lead to another crisis if not well managed.

**Plans and protocols** lans and protocols should recognize the importance of a definitive transition and handover marking the progress from the response phase to the recovery phase of crisis management. Recovery planning could be directly affected by decisions made as part of the response, and longer-term recovery objectives and issues may inform response managers who are making decisions on immediate issues. The recovery team should be led by a member of the CMT and resourced adequately.

There are likely to be ongoing issues which can run for a considerable period of time, often characterized by reputational damage, investor concerns and ongoing legal and insurance challenges. The recovery needs to be funded and could affect earnings, cash flows and debt ratios. In parallel, the organization faces the potential for high-performing individuals leaving whilst at the same time it is trying to introduce changes or reaffirm its strategic direction. The recovery effort might be long term, and it should be expected to consume resources long after the response phase is over.

**Ongoing issues** There are likely to be ongoing issues which can run for a considerable period of time, often characterized by reputational damage, investor concerns and ongoing legal and insurance challenges. The recovery needs to be funded and could affect earnings, cash flows and debt ratios. In parallel, the organization faces the potential for high-performing individuals leaving whilst at the same time it is trying to introduce changes or reaffirm its strategic direction. The recovery effort might be long term, and it should be expected to consume resources long after the response phase is over.

Social cost

he social cost should not be ignored, with employees, customers and key stakeholders all affected. Apart from the physical rebuilding or replacement of nfrastructure that might be necessary, the organization could be required to support investigations or enquiries by the police or regulatory authorities. The CMT should also be mindful of sensitivities attached to the natural processes of healing and grieving, where individuals and their families have been directly affected by the events.

**regenerate, restructure or realign**

Finally, recovery presents an opportunity to regenerate, restructure or realign an organization. The essence of recovery is not necessarily a return to previous normality. It might mean moving towards a model of business and organizational structures that represent a new normality, confronting harsh realities and realizing potential opportunities that might have been revealed by the crisis.

**Review and learn**

Crises serve as a major learning opportunity for both individuals and organizations as a whole. Therefore, the overall management process should include a review of the crisis and an evaluation of the response, the plans and procedures, and the tools and facilities, to identify areas for improvement. Following the evaluation and the identification of lessons, recommendations should be made for change, and responsibilities and timelines assigned to drive that change forward and ensure it is carried out. Too often, lessons are identified but not actually addressed, so that mistakes are repeated in future events. Learning from a crisis should result in change for the organization, its people, plans and procedures that make it more resilient and better prepared for the future.

Capturing organizational learning from a crisis occurs by conducting thorough operational debriefs and extensive follow-up communication with all those individuals, teams and interested parties involved in the actual crisis. This might identify and mitigate any effects of the event on those individuals, personally and professionally.

Learning the lessons from a crisis or planned exercise is an essential element of crisis management. It requires commitment of time, resources, attention and energy towards the end of a difficult and challenging experience. However, not reflecting and acting on lessons not only allows latent problems and vulnerabilities to remain in an organization, it also predisposes the organization to future crises if it emerges that no action, or insufficient action, was taken in response to such problems in the past.

*Business Continuity Planning and Management- ISO 22301*

Business Continuity Planning and Management is a relatively new area of professional activity, but also am area of academic study and research, which aims to facilitate the mitigation of emergencies, crises and disasters in organisations. One theorist argues that, business continuity planning may in fact be defined as:

**thinking the unthinkable, or mitigate the unthinkable"**

**- Ginn, 1992**

The most serious risk that can be posed to any organisation is survival. The area of increasing concern is referred to as ‘business continuity’ or ‘contingency management’; also, sometimes as ‘crisis management’. The need for improved business continuity management (BCM) is increasingly accepted as sensible and pragmatic (Rolfer et al., 1998). This has been accompanied by the emergence of a number of practitioner-based associations. For example, the Business Continuity Institute has a large and rapidly growing membership in over 20 countries, which are graded in accordance with perceived ability and experience (Borodzicz, 2005).

BCM is about prevention, not just cure. It is not just about being able to deal with incidents, as and when they occur, and thus prevent a crisis and subsequent disaster, but it is also about establishing a culture within the organisation that seeks to build in greater resilience, in order to ensure the continuity of operations to deliver key products and/or services to clients and customers. Tony Blair, former UK Prime Minister added BCM to the political arena, when he called for a joined-up approach to face the threat of the millennium computer bug.

**Case Study - Gulf of Mexico**

The Gulf of Mexico disaster of 2010 was a classic example of what can go wrong when the senior management mishandles a crisis. The share price fell by 54% in three months, and two years later was still 23% below the price prior to the disaster. The CEO was fired and the company was forced to sell off many of its assets, to set aside funds to cover claims that in 2011 exceeded £35 billion.  
In addition, a lucrative deal with the Russians was lost to another international company.

**Business Impact Analysis**

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios which should be considered.

Identifying and evaluating the impact of disasters on business provides the basis for investment in recovery strategies as well as investment in prevention and mitigation strategies.

The BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes. Impacts to consider include:

* Lost Sales and Income
* Delayed Sales or Income
* Increased Expenses (e.g: overtime labour, outsourcing, expediting costs, etc.)
* Regulatory Fines
* Contractual Penalties or Loss of Contractual Bonuses
* Customer Dissatisfaction or Defection
* Delay of New Business Plans

The BIA is an integral part of ISO 22301, which requires an organisation to ‘establish, implement and maintain a formal and documented process for business impact analysis that:

1. Establishes the context of the assessment, defines criteria, and evaluates the potential impact of a disruptive incident.
2. Takes into account legal and other requirements to which an organisation subscribes.
3. Includes systematic analysis, prioritisation of risk treatments and their related costs.
4. Defines the required output from the business impact analysis.
5. Specifies the requirements for this information to be kept up to date and confidential.
6. **The Business Drivers**
7. Although it is widely accepted that the protection of brand, reputation and image is paramount for any organisation, other external drivers may have greater influence over the introduction of BCM (see figure 1).
8. A close up of a logo

   Description automatically generated
9. Industry regulations and legal requirements are driving organisations to establish BCM.
10. Today there is greater awareness among regulators that organisations should have effective BCM in place for the protection of customers and the community. Since the attacks against the World Trade Centre in New York on 11 September 2001, and the global financial crisis of 2008, finance regulators across the world have set out conditions for BCM that they expect firms they regulate to follow, in some cases, these conditions are mandatory. In others, they provide strong guidance.
11. Figure 1 below depicts some key business drivers.
12. In the UK, the Civil Contingencies Act 2004 requires local government bodies, the National Health Service (NHS) and the emergency services to put in place effective BCM to ensure that they can continue to perform their functions in the event of an emergency. They have to ensure they can mobilise the functions they need to deal with the emergency, minimise the impact on the responder’s day-to-day activity, and maintain vital services for the community at an appropriate level. In addition, local authorities have the responsibility of promoting business continuity to businesses and appropriate voluntary bodies in support of the concept of a resilient community.
13. Insurance companies are having an increasing influence. Business interruption insurance is seen as a way of covering the revenues lost following a major disruption. Until recently, insurers linked business interruption insurance to building insurance. They now look to sever this link as business interruption losses have increased dramatically. Underwriters are looking for evidence that effective BCM is in place to reduce their risk exposure to business interruption.
14. In the UK, public authorities and the emergency services are driven by the Civil Contingencies Act and are now the biggest drivers of BCM down the supply chain. Increasingly they are seeking evidence that their partners and suppliers have effective BCM; in many cases suppliers cannot tender unless they have implemented business continuity.
15. Time has also become a key driver for BCM. The speed of business has changed, and there is very often little time to allow for gradual recovery. The emergence of e-commerce and the lack of loyalty among customers changed the need for recovery to one of availability. Organisations for which this is vital have to ensure that their services are available 24 hours a day, seven days a week, 365 days a year. Customers will not wait if a call centre is not answering or a website is not available to place an order; they will go elsewhere. Failures can be the result of technical problems, high demand when a site opens for the first time or, more seriously, denial of service attacks by malicious individuals or organisations.
16. **Tickets for the 2012 Olympics in London were sold in various tranches over the internet. The demand for tickets was so great, that when the official website opened it was swamped, and crashed on several occasions. The media had extensive coverage of the failures, and of applicant’s disappointment.**
17. Implementing BCM can bring real benefits to an organisation aside from meeting the regulatory or legal requirements.
18. Competitive advantage can be gained for organisations that are able to demonstrate to potential customers that they have proven plans to continue supply in the face of disruption. Certification against, or compliance with ISO 22301, can be used as part of a marketing package to attract new customers as well as providing existing customers with a positive reason to renew contracts.
19. Financial benefits will occur when areas of weakness within the organisation are eliminated. Within processes, duplications and omissions exist that are wasteful in time and resources. Every failure that occurs has a cost to the organisation, even if it does not result in a disruption. By eliminating these weaknesses, the organisation becomes more resilient and more cost effective. More than 80% of insurance brokers state that premium discounts are given if business continuity plans are in place (British Insurance Brokers and UK Cabinet Office, 2012).
20. **Continuity Planning**
21. The first action for many organisations in establishing BCM has been to create a hostility produced Business Continuity Plan, with giving a great deal of thought to the critical preparatory planning required. The danger in taking this approach is that it will not result in a true understanding of the organisation and how it delivers key products or services. Consideration of various strategies, and their resource requirements mat have been missed. As a result, the plan produced may not be fit for purpose, and may not offer the protection and benefits that may have been possible.
22. To read more about Incident Response and Management, please [click here](http://www.emergency-response-planning.com/blog/incident-management-and-business-continuity-go-hand-in-hand).
23. Experience shows that organisations can be disrupted for many reasons. Business continuity planning has traditionally been based on known threats: loss of IT, loss of buildings through fire, flooding, etc. In recent times however, the UK has experienced some unexpected disruptions, including a widespread outbreak of foot and mouth disease, extensive disruptions to the rail network, a national shortage of oil based fuels, the loss of water supplies for weeks, and a volcanic ash cloud. In most cases existing plans did not cover these disruptions, and the impacts they had on the day to day operations of organisations.
24. When developing plans, it is important that all elements of the organisation are involved (see figure 2). If this does not happen, assumptions may be made about the ability of other parts of the organisation to respond and meet the needs of the plan. For example, if the plan calls for members of staff to work from home, then the IT department must confirm that technical arrangements have, or can be made to enable this to happen. The HR department may need to adjust its policies to accommodate remote working, and health and safety policies may have to be modified.
25. Incident and continuity plans are used under challenging and stressful circumstances; they should be concise, simple and easy to follow. In addition, plans should ensure the organisation maintains compliance with applicable laws and regulations during the period of their implementation.
26. Figure2:   The BCP contents
27. A screenshot of a cell phone

    Description automatically generated

Business Continuity Plans should provide answers to the following basic questions:

* What is to be done?
* When?
* Where are the alternative resources located?
* Who is involved?
* How is continuity to be achieved?

In any organisation, there may be a suite of interconnecting plans, covering:

* Crisis Management
* Emergency Management
* Business Continuity
* Incident Management
* Disaster Recovery

The plans should be appropriate for the organisation, and compatible with each other.

1. **Plan contents**
2. The following sections discuss the recommended elements of incident response and business continuity plans.
3. –
4. **Roles and responsibilities**
5. The plan should identify the roles and responsibilities of those post holders who will be involved in delivering the plan. It will identify the team leader, key team members and their deputies, to be assembled at the time of invocation. It will set out their levels of authority, and to who they must report their actions. It will also set out the point at which the responsibility for incident or continuity management must pass to a higher level in the organisation. There may be separate teams responsible for incident and continuity plans.

**Invoking a plan**

The plan must indicate the circumstances under which it is to be invoked, and who can authorise the invocation. It must also include details of how to manage a disruption, and its impact on the organisation.

**Command Centyre**

* Details of the main and secondary locations where the team should proceed to, in order to manage the disruption.

**Alternate locations**

Details of all stand by locations should be included.

**Contact details**

The plan should include contact details of all team members and their deputies.

**Vital documents and resources**

A list of vital documents and resources needed for continuity and recovery for each critical activity must be included along with details of where these are located.

**Checklist**

A simple checklist or action card may be included to ensure the team completes mandatory tasks.

**Incident log**

With any major disruption, there may be a requirement for post event enquiry and audit.

**Communications**

Details of what will be communicated, and to whom, must be included, together with details of those who are responsible for delivery of the message.

**Salvage**

This is an area frequently omitted from the BCM. If the organisation has suffered fire, flooding or other damage to its buildings, then it is important to ensure that, when safe to do so, arrangements are made to recover important documentation and equipment.

**Returning to normal**

A process must exist for standing down the incident and continuity tams, and returning to normal once the disruption is over.

**Implementation**

Having completed the plans, they must be implemented. Those who hold key positions that are named in the plan must be made aware of their role, and have appropriate training to enable them to fulfil their responsibilities.

**Excercising and testing**

BCM requires that effective plans be established to ensure an organisation can respond to any incident, but the process does not stop at the planning stage.

Plans may be worthless unless they are exercised. Many examples exist where organisations have had business continuity plans in place, but the plans failed because they had not been exercised and tested. In the UK, research has shown (Chartered Management Institute, 2012) that only half of those organisations with plans, exercise or test them, at least on an annual basis. Whilst 18% never exercise their plans at all (see figure 3).

Figure 3: Frequency (in percentage terms)with which UK organisations exercise Business Continuity Plans

A picture containing door

Description automatically generated

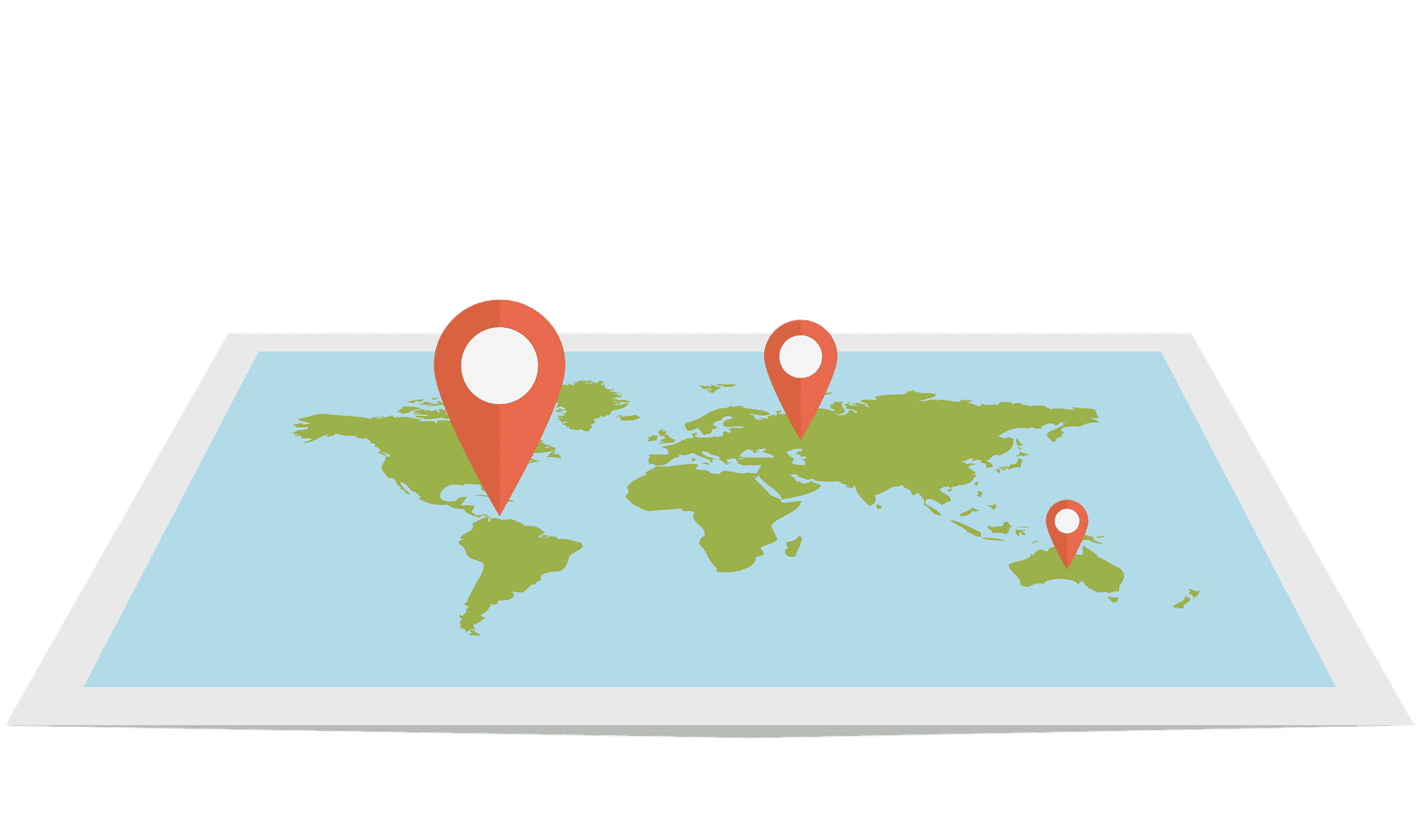
Exercising helps to build confidence in team members by clarifying roles and responsibilities, and supplying practical training and awareness, as well as providing valuable experience of responding to an incident.

There are various forms of exercise, but it is important to:

* Test the systems
* Exercise the plans; and
* Rehearse the people

Despite the increased use of BCM in organisations, there are still managers who continue to dismiss the need for continuity management, even in the face of such major disruptions as the 2007 floods, and 2010/2011 bad winters in the UK. Many have a strong belief that insurance will provide cover for any loss that they may suffer. This is not the case; as losses are not restricted to material damage, but also include loss of reputation, revenues and customers.

Organisations can be disrupted in many ways. Incidents include fire, flood, water shortages, storm damage, internal and external vandalism or fraud, the failure of systems and loss of data, computer hacking, machinery break down, breaches of physical and system security, and staff losses. These are only some examples. Added to this is the climate in which todays organisation has to operate. The intolerance of customers and clients to failure, their lack of loyalty and the demands of the banks for financial visibility and considerable pressures at a time of disruption. If the organisation is unable to manage disruption correctly, and in appropriate time, then the situation will rapidly decline to a crisis, and then a disaster; and the organisation may fail.



**As recent disasters around the world have demonstrated, it is not possible to predict all possible events that can seriously disrupt an organisations ability to maintain continuity of operations. Because the unexpected will always occur, there is a clear need to protect organisations by forward planning (Sharp, 2012)[1]**

[1] Sharp, J. (2012) The Route Map to Business Continuity London; The British Standards

**Contingency Planning**

Activity undertaken to ensure that proper and immediate follow-up steps will be taken by a management and employees in an emergency. Its major objectives are to ensure (1) containment of damage or injury to, or loss of, personnel and property, and (2) continuity of the key operations of the organisation.

Business Directory .com, 2018

As with the Business Impact Analysis (BIA), which will be described later, contingency planning is an integral part of any Business Continuity Plan (BCP) and alludes to need for what is often referred to as a ‘plan B’. If the initial phases of the BCP are unsuccessful, a contingency plan will be required.

In the current political genre, the UK Government has put forward to the UK Parliament a proposal (plan) for exiting the European Union, and this will be democratically voted on to decide if is acceptable. If it is unacceptable, the UK Government will be expected to offer a contingency plan (plan B) for BREXIT.

A disaster is generally defined as:

**"A sudden accident or a natural catastrophe that causes great damage or loss of life."**

**- The Oxford English Dictionary (2018)**

What should be taken from the above definition, is the fact that a disaster is normally unforeseen, at least until it is too late; it can be natural or man-made, and it causes a great deal of damage, including loss of life.

**Case Study - Grenfell Tower**

At 0400hrs on 14 June 2017, a multi-story block of flats in Central London was engulfed in a blaze of fire that was to consume the lives of at least eighty of its inhabitants; inclusive of men, women and children. The above photographic montage illustrates the speed at which the fire took control of the building. The fire was reported at the 24-storey block in North Kensington at 00:54 BST (23:54 GMT), leading to 40 fire engines and more than 200 firefighters tackling the blaze. It took until 01:14 BST the following day to get it under control, with the fire affecting most floors of the building and destroying 151 homes, both in the tower and surrounding areas.

Police said that 71 people died as a result of the fire. By 12 July 2017, Westminster Coroner Dr Fiona Wilcox reported that only 34 victims had been identified. The Metropolitan Police say it believed there were about 255 survivors from the fire.

"Extensive investigations" have led them to conclude 350 people should have been in the tower block on the night of the blaze.

Fourteen residents were not in the building at the time, leaving at least 80 people dead or missing, the Metropolitan Police said thirty-two people have been [formally identified by the coroner](https://www.bbc.co.uk/news/uk-40457212), but not all names have been released.

Metropolitan Police Commander Stuart Cundy has said there is "a risk that sadly we may not be able to identify everybody". He announced on 5 July that the last of the visible human remains had been forensically recovered from the building.

The Metropolitan Police says it will consider manslaughter, health and safety and fire safety charges.

[The fire started in a Hotpoint fridge freezer](https://www.bbc.co.uk/news/uk-40380584), but police said it was not started deliberately. Footage has shown the fire spreading up one side of the building externally, before engulfing the entire block. Downing Street ordered immediate testing of the fridge freezer that was involved.

The cladding - installed on Grenfell Tower in a recent renovation - has come under scrutiny, with experts saying a more fire-resistant type could have been used. Both the cladding and insulation on the outside of the building failed all preliminary tests by the police. The insulation samples burned more quickly than the cladding tiles.

Documents obtained by the BBC suggest the cladding fitted during its refurbishment was [changed to a cheaper version](https://www.bbc.co.uk/news/uk-40453054). They show the zinc cladding originally proposed was replaced with an aluminium type, which was less fire resistant, saving nearly £300,000. Cladding can create cavities which in some cases can cause a chimney effect, drawing flames up the cavity if there are no fire barriers.

The Department for Communities and Local Government (DCLG) said composite aluminium panels with a polyethylene core should not be used as cladding on buildings over 18m high.

Engineering and manufacturing company Arconic later said one of its products, Reynobond PE (polyethylene) - an aluminium composite material - was "used as one component in the overall cladding system" of Grenfell Tower.

Disaster Recovery (DR) is the process an organisation uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans. While Disaster Recovery plans, or DRPs, often focus on bridging the gap where data, software, or hardware have been damaged or lost, one cannot forget the vital element of manpower that composes much of any organisation. A building fire might predominantly affect vital data storage; whereas an epidemic illness is more likely to have an effect on staffing. Both types of disaster need to be considered when creating a DR Plan. Thus, organisations should include in their DRPs contingencies for how they will cope with the sudden and/or unexpected loss of key personnel as well as how to recover their data.

Disaster Recovery Plans are generally part of a larger, more extensive practice known as Business Continuity Planning (previously covered). DR plans should be well practised so that the key players are familiar with the specific actions they will need to take should a disaster occur. DR plans must also be adaptable and routinely updated, e.g. if new people, a new branch office, or new hardware or software are added to an organisation they should promptly be incorporated into the organisation's disaster recovery plan. Companies must consider all these facets of their organisation as well as update and practice their plan if they want to maximise their recovery after a disaster.

**The Disaster Recovery Plan**

From severe storms and forest fires to infrastructure issues and cyber-attacks, businesses of all sizes and types are subject to disasters and disruptions. While large businesses typically plan for such events, small businesses usually do not have a formal disaster-recovery plan, causing between 40 to 60 percent of them to close their doors after disaster strikes.

**"Without a plan, even those who do reopen typically take much longer to recover at a much greater cost than those who are prepared."**

**Without a plan, even those who do reopen typically take much longer to recover at a much greater cost than those who are prepared."**

**-Stan Brubaker, risk consultant with Liberty Mutual Insurance.**

**-Stan Brubaker, risk consultant with Liberty Mutual Insurance.**

However, there are many things that small businesses can do to make sure that when disaster strikes, they have a roadmap to help guide their business and increase the likelihood that their business will return to top form.

To craft a comprehensive disaster-recovery plan, include these eight steps.

**Select each of the 8 steps below and click on the individual cards**

**Asses yopur risk**

While its impossible to prepare against every risk you can identify with those most likely to affect business based on industry technology geography and other factors. design your plan to include all action for all conceived disruptions.

**Identify egress and evacuation points**

**A screenshot of a cell phone

Description automatically generated**

**Appoint an Employee recovery team**

**A screenshot of a cell phone

Description automatically generated**

**Provide business operations**

****

**Communicate internally and externally**

**A screenshot of a cell phone

Description automatically generated**

**Manage customer and supply chain interaction**

**A screenshot of a cell phone

Description automatically generated**

**Establish emergency accounting and payroll**

**A screenshot of a cell phone

Description automatically generated**

**Cyber secure**

**A screenshot of a social media post

Description automatically generated**

**Liaison with Emergency Services**

Effective communication with emergency services is vital, in the wake of a crisis or disaster

**The emergency services and armed response**

For the purposes of this course, the emergency services are described as:

* Police
* Fire
* Ambulance
* Coastguard

It is recommended that all Security Managers - at some stage -  familiarise themselves with the services provided by emergency teams in their area of operations. In a crisis or disaster situation, it will be to the advantage of the Security Manager to establish good communications with those functions recognised as blue light response.

When the emergency services have been notified, they will take over the situation and cordon the area. For the emergency services, preservation of life comes first; then preservation of evidence. In some instance, arrests may be required and there may be a need for an armed response. The senior office is always in command however, the established CMT must effectively communicate any information to the senior commander, in order to offer assistance with the current situation and in the event that any further investigation must take place, thereafter.