Business Continuity Management – what is it and why is it so important?

Risk Bulletin

September 2021

Introduction

While insurance cover can offset costs incurred as a result of disruptive incidents, it is not the only mitigation you should rely on. Incidents can also have an impact on areas that are not insured such as your reputation, share price, consumer and market confidence, the cost and distraction of managing the incident and of course there may be other unexpected uninsured costs associated with the incident.

Businesses should implement a robust business continuity management (BCM) framework that helps identify and mitigate risks before they become disruptive, and also enables a timely and effective recovery when they do.

Ask yourself the questions in this document, and consider how well prepared your business is to meet disruption, to recover from disruption and to become a more resilient organisation in the process.

What is Business Continuity Management?

Business continuity management (BCM) is a management activity that focuses on the prioritised needs of the business. It prepares solutions that will help detect, respond to, manage and recover in a timely manner should there be disruption and to continue operations to an agreed level regardless of the nature of the incident.

Business continuity improves the organisational resilience of a business by having:

- Risk management in place that helps reduce the need to invoke a business continuity plan
- A recovery and response structure in place to manage those risks that cannot be prevented or predicted, or where mitigation fails

What does this mean for you?

BCM means knowing what parts of your business are important to you, what would happen if you lost them, how you might lose them and when and how to get them back up and running again. Some of the benefits of BCM are:

- Less risk to your productivity, revenue, brand name and reputation
- Disrupted operations can be back online quicker
- Greater visibility of key processes, risks, supply chain and other vital dependencies
- Greater confidence for employees, clients and partners in your ability to deliver during and after incidents
- BCM can help reduce contractual and service level breaches, penalties and fines
- Competitive advantage - BCM is a good selling point, and can be a prerequisite for some new clients
- Possible reduction in insurance premiums
- Analysing the workflow and interdependencies of activities can help identify risks, inefficiencies and security and safety issues in all areas of the business

Who needs to be involved in BCM?

As well as having the required resources to build and maintain the business continuity framework, it is important that the business has senior management buy in. This way both employees and management will be fully engaged with BCM.

Management buy in

Ensure the Senior Management Team (SMT) and senior stakeholders are engaged with BCM as it must be aligned to their overall business objectives and strategies.

Business continuity policy

A formal business continuity policy should be produced that acknowledges SMT ownership of BCM and defines the objectives, scope and the roles and responsibilities of all involved with BCM.

Roles and responsibilities

A number of posts will need to be formed, with clear guidance and training for each:

- An Incident Response Team
- The Business Continuity and Recovery Team
- A Business Continuity Coordinator, Manager or Lead
- Department Business Continuity Reps

What is important to your business?

Before implementing recovery plans, it is critical to know what the key business lines are, and what the SMT priorities are.

In order to understand what is important to the business, you need to understand how the entire business operates.

What do you do?

Firstly, you will need to work with the SMT to agree:

- What the key products or services are for your business
- What the impact of their loss would be – productivity, revenue, reputation, client confidence, employees
- Who the key clients and partners are, and what other areas of the company rely on your business
- How clients and competitors will react to disruption
- The key times of year that the business operates and when demand or production is higher
- A timeline for recovery – when must each be recovered after disruption, in what order and to what degree

The term for this piece of work is a 'business impact analysis (BIA)' and must start with this SMT strategic view.

How do you do it?

Armed with the SMT view of recovery priorities, you will need to gain a thorough understanding of how the business works and what the various interdependencies are. You can then go out to those in the business who understand how it can be delivered and determine the following:

- What activities and processes are involved in delivering these products and services
- What resources and dependencies are required to enable these activities and processes
- How do various threats pose a risk to these dependencies and resources
- What can be done to minimise risk events occurring to them
- What can be done to enable a recovery in case risk mitigation fails or is absent

What dependencies do you need to do it?

All businesses will have dependencies that are relied upon in order to maintain production and service. The identification and assessment of these will be key to the success of your business continuity arrangements. These may include:

- Premises
- Facilities and utilities
- Equipment and machinery
- Specialist tools and moulds
- IT, data and paper records
- Telephony
- Suppliers and partners
- Other areas of the business reliant on your area of the business
- Stock and consumables
- Transport
- Teams and employees
- Partner businesses

What could go wrong?

Even the smallest and sometimes most unexpected things can escalate and lead to significant disruption. These are often the things that could not feasibly have been predicted, which provide all the more reason to have a recovery plan in place.

Using your existing risk management processes, identify and register any risks that might:

- Cause disruption to business
- Prevent recovery from disruption

Typical measures to reduce risk events occurring include:

- Early warning detection – IT, fire and flood
- Multiple site operations, such as suppliers
- Standby electrical power, such as air conditioning units
- Dual cable entry points
- Verified off-site data backups
- Physical and cyber security measures
- Health and safety (H&S) compliance
- Sprinklers and fire suppression

Once you know what needs protecting, a typical process to identify risks is as follows:

1 Identify generic threats to any business

Extreme weather, pandemic, fire, flood, crime, cyber attacks, supply chain failure or terrorism.

Poor training, poor management, accidental damage or electrical failure.

2 Risks to your business as a result of these threats and local hazards

Supply chain may fail due to weather disruption or IT network disruption which may impact poorly secured critical IT which is used to operate machinery.

Single piece of specialist equipment fails due to poor training or maintenance or fire in stock room due to presence of flammable goods.

3 Mitigation required to reduce risks occurring

E.g. Sprinklers, spare components, standby power, split site operations, formal training or operating procedures, timely fix and replacement of key equipment, cross trained employees, robust cyber security and IT management.

4 Recovery measures required in case mitigation fails or is not in place

E.g. Dedicated recovery sites, alternative supply chain options, standby machinery, standby IT systems and data backups, off-site spare stock and supplies.

What if you lose your premises, IT or supplier?

Regardless of the measures that have been put in place to reduce risk events occurring, there will always be events that can be neither predicted nor prevented. With this in mind it is important that the required recovery measures are in place.

In order to enhance your recovery capabilities, you will need to consider two key areas:

- Build recovery arrangements – implement measures to recover in a timely manner
- Design a formal response structure to manage the use of those arrangements

Rather than having a recovery solution for the loss of a particular product or service, it is often better to focus on the dependency. Typically, you will need proven arrangements in place to manage the recovery after the loss of the following areas.

Premises and utilities or facilities

Premises include the main operating areas, as well as storage areas and parking, anything that is key to the business, particularly specialised areas. They may be put out of use due to incidents such as fire or flood, but also because of activities at neighbouring sites or an incident that prevents access to site, even though it is still operational.

Typical solutions involve maximising multi-site operations, relocating employees to alternative sites, handing off work to other sites or businesses that have the capacity to ramp up and meet the loss, using the marketplace or other businesses to assist, resilient on-site electrical or other facilities, and of course good housekeeping and maintenance regimes.

Employees

Employees are key in the event of the loss of any dependencies, but you also need to consider events where you will experience a loss of employees or when large numbers of employees aren't available, this could be due to a pandemic, poor weather, transport issues and more.

Solutions include the conduct of key activities across multiple sites, drafting in skilled employees at short notice, cross training employees, handing off work to others and employees working from home or remotely.

IT and communications

Most businesses are reliant on IT and data. IT can be complex, usually critical and often out of your hands to fix if it goes wrong. IT and data may be used across the whole business, or locally to run a piece of equipment. While cyber-attacks are a much discussed threat to IT, there are still many failures that are down to poor management of IT, such as IT component failure, physical damage caused by nature e.g. fire and flood or cables being cut or stolen, just to name a few examples.

Typical solutions include the use of 'cloud' systems, off-site standby IT systems that are at various stages of standby, manual workarounds and good all round IT and IT security management. IT and data may be hosted within the business or by a third party, but you should still ensure recovery measures meet your business needs.

Equipment and machinery

This can include machinery and equipment used in a manufacturing or production facility, a warehousing operation, a conference venue, or any business with equipment needs as part of its operation. Consider also any specialised racking or tools required to work alongside the equipment or production line. Disruption may be caused by poor training, operations or maintenance as well as reliance on single points of failure or fire.

Solutions may be a combination of using extra capacity on and off-site, handing off work to other businesses or sites, good maintenance and repair response procedures, as well as the ability to secure timely replacement of failed machinery and components by suppliers where lead times don't breach business recovery needs.

Transport

Transport requirements may be owned by the business or a third party. They may include freight and movement between locations or within the site e.g. fork lifts. Disruption may be to the transport itself, fuel shortages, infrastructural such as access, rail or road issues or even the drivers or handlers.

Typical measures may include having a fleet of different types of vehicles, cross training drivers or handlers, enlisting dual haulage suppliers and garaging vehicles a good distance apart.

Consumables and stock

Consumables and stock will typically include items required as part of the production process, e.g. to enable machinery to run you may need oil. It may also include finished products that are ready to dispatch from site. Either could be due to any of the following examples; poor storage and handling, pest infestation, fire, flood, a supply chain issue and more.

Measures include having an 'in use' reserve of products or finished items that can be used when there is any interruption to production (on and off-site), safe storage and securing multiple supply chains.

Supply chain

Many businesses are reliant on a supply chain of some sort. Supply chains are a dependency that you have little control over, so it is important to understand where the vulnerabilities in the supply chain are as suppliers may fail your business. This could be for many reasons, including the failure of their own suppliers, lack of raw materials, labour shortages, physical damage to their premises or experiencing a cyber-attack. In addition, consider those areas of the business upstream to yours that you rely on in some way, such as internal suppliers.

Solutions include maintaining oversight and good relations with all elements of the supply chain, the use of parallel providers, ensuring alternative suppliers can be switched over in good time and the retention of supplies on and off-site to cover downtime of failed suppliers.

Paper records and files

Some businesses rely on hard copy documents and paper records as a service to others, e.g. scanning and/or storage of files. They may also need them to refer to as part of the business operation.

Recovery measures include the maintenance of safe, 'fire and flood free' storage solutions, off-site duplication and scanning records onto resilient IT systems. Taking these steps will reduce the risk significantly.

How will your business respond to a disruptive incident?

The importance of timely and appropriate communications cannot be stressed enough – escalation and prompt notification of events can be the key to speeding up the recovery of business.

Now you know what the recovery solutions are, how will you manage them? How will you respond and invoke them – and who will do this? A system and plan to manage the initial response and the recovery should include:

- Incident detection systems and escalation protocols, with the ability to communicate at any time
- Formal, competent and trained Response Teams
- Measures to support the use of your recovery arrangements
- A business continuity plan (and any supporting documents) that will formally detail all response actions

Incident detection

For an effective response, you need to be able to identify incidents as they occur. The right people will need to know immediately if there has been an incident, whether this is inside or outside of working hours.

Identifying an incident such as fire or smoke, a leak, or interruption with a building management system will be obvious but you also need to consider incidents such as break-ins, loss of IT or electrical power - how will these be identified and communicated, especially outside of working hours?

Response Teams

Response Teams should be staffed by people with the right knowledge, skills and authority. These teams should be aligned with existing management structures across the business. For many businesses, the following is common:

- **Managing the incident - Local Incident Response Teams**
  Responsible for the immediate response to disruptive incidents such as fires, spills and IT outages. They will often be responsible for the conduct of evacuations, immediate response and communications and alerting the Business Continuity team while managing and fixing the incident itself, rather than the recovery.
- **Managing the recovery - Incident Response Team**
  Often, the Incident Response Team will be able to manage an incident without any business continuity plan activation but if the incident is getting worse and likely to be prolonged, the Incident Response Team will inform the Business Continuity Team who will invoke the business continuity plan and manage onward communications and put recovery measures in place.
- **Managing the crisis - Crisis Management Team**
  There should be a Crisis Team of senior members that will convene if events reach a point where the entire business is at risk and events cannot be contained by business continuity arrangements alone - also known as a crisis.
- **Employees and Teams involved with recovery, but not part of the Incident Recovery or Business Continuity team(s)**
  There will be employees who are not in Response Teams but are responsible for setting up alternative premises or switching IT systems for example. These may include facility staff and IT teams. Ensure this is all co-ordinated accordingly.
- **Command centres**
  While conference call facilities are a good way to set up a Business Continuity Team meeting, there may come a time when the Business Continuity Team needs somewhere secure to meet up, both on and off-site. We recommend this being a significant distance from the site itself.

Escalation and communications

All Response Teams will need to have clear escalation paths in place with each member having immediate access to the relevant contact details (listed on their phone is often best) for all key contacts, both internally and externally.

The first person to be aware of an incident could be any employee. Ensure they know what to do and how to contact the Incident Recovery Team or their line manager, even if this is outside of working hours.

Ensure that you have considered all forms of communication and are able to use at least one of them effectively without reliance on the site or IT, as they could have been affected in the incident.

Media

Consider how the media will be handled and how media coverage of the incident will be monitored. Identify who in the business will manage media queries in and messaging out. Consider your social media presence – what is being posted about your business, and by your business? How can you use social media to assist when incidents occur?

Welfare of employees

The impact on employees welfare and wellbeing during and after a disruptive incident can have as great a bearing on the business as the financial impact. It is important to consider and monitor the impact of incidents on the physical and mental welfare of your employees. Pay attention to employee communications as they are often overlooked.

General response plans

With all of the recovery arrangements agreed and a structure that allows timely responses and communications, you now need to formalise and gather the actions and reference details into response plans. This may include:

- Incident report plan - The contents of an incident report plan will differ for each organisation and be specific to scenarios such as loss of IT, fire evacuation, bomb threats and chemical spills The focus will be on managing the incident itself
- Business continuity plan - The aim of the business continuity plan should be to provide the Business Continuity Team(s) (if you have a tiered structure) with an easy to use document that contains all of the actions and reference information required in the event of prolonged business disruption
- Individual team response plans - The teams that have been identified for recovery and relocation may need their own ‘one pager’ document, which outlines all the details they require for their part of the recovery process
- IT disaster recovery plans - The technical plan detailing how to recover IT. This may be owned by the IT Team but must be managed alongside business continuity plans
- Crisis management plans - This may also be part of the business continuity plan which outlines the SMT response to events that are beyond the scope of the BC Plan (such as data breach, adverse publicity, loss of clients, funds or multi-site)
- Other contingency and technical plans - As well as immediate incident response plans, there may also be a need for specific contingency plans and procedures that deal with common incidents or demand a very particular type of response, such as equipment failure, data back-up restore or product recall

Business continuity plan contents

The focus of a business continuity plan will depend on whether it is a single site level business continuity plan or whether it is an overarching, silver or gold level plan. Higher level plans will have less of the operational detail in them and more detail on the wider strategic response and support to the lower level operational business continuity plans.

Contents should include all of the actions, contact details and reference information that the Business Continuity team would need to aid management of the recovery.

Plans should be formal (signed off by the SMT), easy to use, available at all times to those that need them, flexible to manage all manner of incidents and be based on a thorough business impact analysis.

How will you prove that recovery measures work?

Your recovery solutions should never be assumed – proven and tested plans will confirm your readiness and give confidence that the solution is fit for purpose.

Now that you have recovery and response arrangements agreed, and a business continuity plan in place, you need to prove that they are fit for purpose by testing and rehearsing them.

Testing and exercising

Some benefits of testing and carrying out exercises include:

- Improves familiarity of Business Continuity Teams with plans and recovery measures
- Allows challenge and confirmation of recovery measures and plans
- Identifies gaps and actions required to improve resilience and recovery capabilities
- Confirms availability of employees, key contacts, documentation, plans, resources and standby sites
- Raises awareness among staff, not just the Response Teams and stakeholders
- Raises confidence of Response Teams, employees, clients (both existing and prospect) and insurers

A programme of tests and exercises should be established throughout the year. This might include:

- Desktop exercises
- Live rehearsals
- Live test of recovery arrangements
- Communications tests

How will you keep the business continuity framework current?

Ensure that the effort and good work that goes into establishing a business continuity framework does not go to waste by keeping it up to date and current.

As well as regular testing and exercising of business continuity plans, recovery measures and Response Teams should be subject to regular review and updated to meet the changing shape and needs of the business.

Review

All elements of the business continuity framework should be formally reviewed with the SMT and key stakeholders to ensure they are still fit for purpose and up to date. This would include a review of the business continuity policy, business impact analysis, business continuity plans, recovery arrangements and test reports. Not just annually, but after any significant change.

Arrangements should be in place to ensure that key dependencies are maintained and repaired on time, subject to appropriate maintenance and adequate security measures. The same applies to recovery arrangements (standby sites or spare machinery) – ensure they remain ready for use. It is important that key suppliers are subject to periodic checks to ensure they retain a level of resilience that you are comfortable with.

Governance and oversight

While the Business Continuity Co-ordinator or Manager may be responsible for much of the work mentioned above, the SMT is responsible making sure it is carried out. As detailed earlier, the SMT should formally be involved with the review of the plans and should also schedule an audit and oversight programme to ensure that the business continuity policy is effective.

Change management

Good change management procedures mean that changes can be risk and impact assessed prior to implementation, with less risk of impacting changes to the operation or to recovery arrangements.

Employee awareness

Engaging with staff and raising their awareness of the business continuity plan and their responsibilities is key to making business continuity part of the everyday operation and maintaining an alert and capable workforce in times of disruption.

Embedding business continuity

As BCM is implemented across the business, the SMT can embed it into all areas of the business by making sure that it aligns with strategic objectives and corporate values. If this is done effectively, then business continuity will stay in shape as the business evolves through constant and sometimes unexpected changes.

How else can we help?

For more help and guidance please contact your broker.
Other resources, websites and publications include:

The Business Continuity Institute (BCI) is the UK's Business Continuity best practice body - **www.bci.org.uk**

To assist you further, RSA works in partnership with the RISCAuthority who have developed a BCM planning tool called Robust©. This is available via the RISCAuthority - **https://robust.riscauthority.co.uk/**

The RISCAuthority also has other resources to use - **https://www.riscauthority.co.uk/free-document-library/**

Continuity Central is a great resource for guidance, tips and news **www.continuitycentral.com**

The National Risk Register, with the UK Government's assessment of various threats and hazards that may impact the UK - National Risk Register of Civil Emergencies – 2017 Edition

The Business Continuity Good Practice Guidelines (GPG) 2018 Edition - available from the BCI link above. There is also a free lighter version, available on their website.

ISO 22301:2019 – Security and Resilience. BCM systems – **https://www.bsigroup.com/iso-22301-business-continuity**

Various ISO/BS publications about continuity of services, IT – available at **https://www.bsigroup.com**

Automated third party online tools that can be used to produce a BC plan and supporting framework.

RSA Risk Consulting remains here to help you evaluate and manage your risks during this period of uncertainty. For any further technical and risk management based questions please contact the following, or your normal risk management advisor.

For any information relating to the specific details about your policy please speak with your normal insurance advisor.

Lachie Brown
(UK)

lachie.brown@uk.rsagroup.com

Andrew Friend
(UK)

andrew.friend@uk.rsagroup.com