Risk Control Guide

BUSINESS CONTINUITY MANAGEMENT – WHAT IS IT?

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 (BC) management 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. RSA can help answer all of them for you, and can offer assistance in various forms to its clients, so please do contact us for more information.

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; to continue operations to an agreed level regardless of the nature of the incident.

BC also improves the organisational resilience of a business by having:

- Risk management in place that helps to reduce the need to invoke a BC 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 staff, 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, security/safety issues etc. 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 BC framework, it is important that the business has senior management buy in; this way both staff 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 needs to be aligned to their overall business objectives and strategies.

BC Policy

A formal BC 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 (IR) team
- A BC team - one team, or a 'tiered' number of BC teams.
- A BC Coordinator/manager/lead
- Department BC 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?

You will firstly need to work with the SMT to agree:

- What the key products/services are for your business
- What the impact of their loss over time would be – productivity, revenue, reputation, nock on effects upstream/downstream in the business, client confidence, staff etc
- Who the key clients, partners and other stakeholders are
- How clients and competitors will react to disruption
- The key times of year that the business operates and when demand/production is higher
- A timeline for recovery – when should 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 needs to start with this SMT strategic view.

How do you do it?

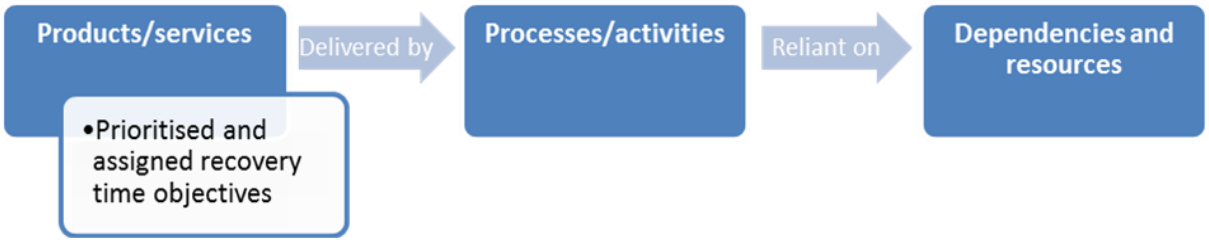
Armed with this SMT view of recovery priorities, you need to gain a thorough understanding of how the business works and what the various interdependencies are. Then go out to those in the business who understand how all this is delivered and determine from them:

- What activities and processes are involved in delivering products/services
- What resources and dependencies are required to enable these activities/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 any risk mitigation fails or is absent

What do you need to do it?

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

- Premises
- Facilities/utilities
- Equipment, machinery
- Specialist tools, moulds etc
- IT, data
- Telephony
- Suppliers/partners
- Stock, consumables
- Transport
- Teams/staff
- Partner businesses
- Hard copy documents



What might 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

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

Identify generic threats to any business

Extreme weather, pandemic, fire, flood, crime, cyber attacks, supply chain failure, terrorism etc.
Poor training, poor management, accidental damage, equipment failure, H&S etc.

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

Supply chain may fail due to weather disruption, IT network disruption may impact critical IT used to operate machinery etc. Single piece of specialist equipment may fail due to poor training or maintenance, fire may destroy stock due to presence of flammable goods etc.

Mitigation required to reduce risks occurring

For example - sprinklers, spare components, stand by power, split site operations, formal training/operating procedures, timely fix/replace of key equipment, cross trained staff, robust cyber security/IT management etc.

Recovery measures required in case mitigation fails/not in place

For example - dedicated recovery sites, alternative supply chain options, stand by machinery, stand by IT systems/data back ups, off site spare stock/supplies etc.

Typical measures to reduce risk events occurring include:

- Early warning detection – IT, fire, flood etc.
- Multiple site operations, dual suppliers etc
- Stand by electrical power, AC units etc
- Dual cable entry points
- Mirrored or Cloud based IT systems
- Physical and cyber security measures
- H & S compliance
- Sprinklers and fire suppression

What if you lose your premises, IT, supplier etc?

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:

Premises and utilities/facilities

Premises include the main operating areas, but also storage areas, parking areas etc. – anything key to the business. They may be put out of use because of fire or flood, but also because of activities at neighbouring sites or an incident that prevents access to site, even though it is operational.

Typical solutions involve maximising multi-site operations, relocating staff to alternative sites, handing off work to other sites/business, using the marketplace/other businesses to assist, resilient electrical/other facilities, and of course good housekeeping and maintenance regimes.

Staff

Staff are key in the event of the loss of any dependencies, but consider the non availability of large numbers of staff themselves (pandemic, poor weather, transport issues etc.) as well as the loss of key members of staff.

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

IT and Comms

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 understanding and management of IT, IT component failure, physical damage caused by fire, floods etc. or cables being cut (or stolen) and so on.

Typical solutions include the use of 'cloud' systems, off site stand-by IT systems that are at various stages of stand-by, 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 business needs.

Equipment/machinery

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

Solutions may be a combination of using spare capacity on and off site, handing off work to other businesses/ sites, good maintenance and repair response procedures, the ability to secure timely replacement of failed machinery/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 (fork lifts for example). Disruption may be to the transport itself, fuel shortages, the infrastructure (roads, access, rail, freight issues etc.) or the drivers/handlers.
Typical measures include having a fleet of different types of vehicles, cross training drivers/handlers, dual haulage suppliers, garaging vehicles a good distance apart etc.

Consumables/stock

Consumables and stock will include incoming items required as part of the production process, supplies to enable machinery to operate (oil etc.) as well as finished products that are ready to dispatch from site. Loss of either may be due to poor storage and handling, pest infestation, fire, flood etc. or a supply chain issue.

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

Supply chain/stakeholders

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. Suppliers may fail your business for many reasons including the failure of their own suppliers, lack of raw materials, labour shortages, physical damage to their premises, cyber-attack etc.

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 to in good time, the retention of supplies on/off site to cover downtime of suppliers etc.

Paper records/files

Some businesses rely on hard copy documents and paper records – as a service for others (e.g. scanning, storage of files) or 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, scanning records onto resilient IT systems etc. thus reducing the risk significantly.

How will you respond to a disruptive incident?

The importance of timely and appropriate communications cannot be stressed enough – escalation and timely 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 BC 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 happen. The right people will need to know immediately if there has been an incident – in or outside of working hours.

Some of these are obvious such as fire/smoke detection, leak detection, a building management system and so on, but consider break-ins, failure of key machinery, loss of IT/electrical power outside of working hours – how will this be communicated?

Response teams

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

Local incident response (IR) teams – manage the incident

Responsible for the immediate response to disruptive incidents such as fires, spills, IT outages and so on. They will often be responsible for the conduct of evacuations, immediate response and comms, alerting the BC Team while managing and fixing the incident itself, rather than the recovery.

BC teams/recovery teams – manage the recovery

Depending on the size and structure of your business, you may prefer a tiered BC team approach - Bronze, Silver and Gold Teams for example. Often, the IR Team will be able to manage an incident without any BC plan activation but if the incident is getting worse and likely to be prolonged, the IR Team informs the BC Team who will then invoke the BC Plan and manage the onward communications and recovery measures in place.

Crisis management (CM) team – manage the crisis

There should be a CM Team of senior members that would convene if events had got to a point where the entire business was at risk, and events could not be contained by BC arrangements alone - a crisis.

Staff and teams involved with recovery, but not part of the IR/BC teams

There will be staff who are not in response teams who are responsible for setting up alternative premises, switching IT systems etc. such as facilities teams, security staff, IT teams etc. Ensure all this is coordinated!

Command centres

While conference call facilities are a good way to set up a BC Team meeting, there may come a time when the BC Team needs somewhere secure to meet up, both on and off site (at a suitable distance from site).

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 (internal and external).

The first person to be aware of an incident may be any member of staff. Ensure they know what to do and how to contact the IR Team/line manager, even out 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 that may have been affected.

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.

Welfare of staff

The impact on staff 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 then, to consider and monitor the impact of incidents on the physical and mental welfare of your staff. Pay attention to staff communications as they are often overlooked.

Response plans - general

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:

- IR Plans. The contents of an IR Plan will differ for each organisation and be specific to scenarios such as loss of IT, fire evacuation, bomb threats, chemical spills etc. The focus will be on managing the incident itself
- BC Plans. The aim of the BC Plan should be to provide the BC Team (or Teams if you have a tiered BC Team 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. Teams that have been identified for recovery/relocation may need their own 'one pager' to give them the details they require for their part of the recovery
- ITDR Plans. The technical plan detailing how to recover IT. This may be owned by the IT team but should be compiled and aligned to the BC Plans
- CM Plans. This may also be part of the BC Plan, detailing the SMT response to events that are beyond the scope of BCM (data breach, adverse publicity, loss of client/funds, multi-site loss etc.).
- Other contingency and technical plans. As well as immediate incident response plans, there may also be a need for specific contingency plans/procedures that deal with incidents that are common or demand a very particular type of response, such as equipment failure, data back-up restore, product recall etc.

BC Plan contents

The focus of a BC Plan will depend on whether it is a single site level BC Plan, or whether it is an overarching/ Silver/Gold level BC Plan. Higher level plans will have less of the operational detail in them, with more detail on the wider strategic response and support to the lower level operational BC Plans.

Contents should include all of the actions, contact details and reference information that the BC Team would need to aid management of the recovery. Look at the RSA BC Plan template for more details on the content.

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 BIA.

How will you prove 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 BC Plan in place, you now need to prove that they are fit for purpose by testing and rehearsing them.

Testing and exercising

Some benefits of testing/exercises include:

- Improves familiarity of BC Teams with plans and recovery measures
- Allows challenge/confirmation of recovery measures and plans
- Identifies gaps and actions required to improve resilience and recovery capabilities
- Confirms availability of staff, key contacts, documentation/plans, resources, stand by sites etc.
- Raises awareness among staff, not just the response teams and stakeholders
- Raises confidence of response teams, staff, clients (existing and prospective) and insurers

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

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

How will you keep the BC framework current?

Ensure that the effort and good work that goes into establishing a BC framework, does not go to waste – keep it current.

As well as regular testing and exercising, BC plans, recovery measures and response teams should be subject to regular review and update to meet the changing shape and needs of the business.

Review

All elements of the BC framework should be formally reviewed with the SMT and key stakeholders to make sure they are still fit for purpose and up to date. This would include a review of the BC Policy, BIA, BC Plans, recovery arrangements, test reports etc. Not just annually, but after any significant change.

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

Governance/Oversight

While the BC Coordinator/Manager may be responsible for executing much of the above work, the SMT is responsible for making sure it happens. As detailed earlier, they should formally be involved with the review of the plans and should also schedule an audit/oversight programme to make sure that the BC Policy is effective.

Change management

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

Awareness of staff

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

Embedding BC and continuous improvement

As BC management 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 BC will stay in shape as the business evolves through constant and sometimes unexpected changes.

How else we can help?

RSA has a number of templates and guidance documents available to assist, which have been referred to in this guidance. These include:

- Fuller more detailed guidance
- BIA template
- BC Plan template
- Test template and guidance

RSA can also do reviews of your BC arrangements for you, to help uncover gaps, refine BC Plans, initiate or improve your BCM etc. We are also able to assist with testing and exercising, particularly with desktop exercises for management teams/key teams.

Other resources, websites and publications include:

- The Business Continuity Institute (BCI) is the UK's BC 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/ (then click on Business Continuity)
- 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 and BS publications dedicated to continuity of services, IT etc. – available at https://www.bsigroup.com
- Automated third party online tools that can be used to produce a BC plan and supporting framework