oak CONSULT

A to Z of Business Continuity Management

Introduction

- Business continuity is a far reaching topic that many business owners and managers do not think about until it is too late. ‘It will never happen to me’ until it does and then the majority of businesses cease to exist within 2 years of a serious incident.
- Yes, business continuity can take a few months to implement properly. Yes, it takes some effort, resource and money to implement and maintain and Yes, it takes some focus away from all the urgent things on your to do list for a short time. BUT an implemented, tested and accredited Business Continuity Management System can win you new business, help you retain existing business and ultimately, should the worst happen, keep you in business!
- In this A to Z I’ll be talking about some of the main terminology that Business Continuity Practitioners will bamboozle you with. I should know, I am one!

oak CONSULT

Activity

- Key activities that a business undertakes to provide products and services to customers and maintain operations whilst an incident is taking place.
  - What are your organisation's key products and services?
  - What are the critical activities and resources required to deliver these?
  - What are the risks to these critical activities?
  - How will you maintain these critical activities in the event of an incident (loss of access to premises, loss of utilities etc)?

oak CONSULT

Business Impact Analysis (BIA)

- A BIA identifies and documents your key products and services; the critical activities required to deliver these; the impact that a disruption of these activities would have on your organisation; and the resources required to resume the activities.
- 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 major incidents on your 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 / delayed sales and income
  - Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
  - Regulatory fines / Contractual penalties or loss of contractual bonuses
  - Customer dissatisfaction or defection
  - Delay of new business plans
  - Timing and Duration of Disruption
- The point in time when a business function or process is disrupted can have a significant bearing on the loss sustained. A store damaged in the weeks prior to the Christmas shopping season may lose a substantial amount of its yearly sales. A power outage lasting a few minutes would be a minor inconvenience for most businesses but one lasting for hours could result in significant business losses. A short duration disruption of production may be overcome by shipping finished goods from a warehouse but disruption of a product in high demand could have a significant impact.

oak CONSULT

Command, Control and Co-ordination

- This is a well-established Crisis Management process used within the emergency services and implemented in many large multi-level organisations.
- **Command** - the authority for an organisation or part of an organisation to direct the actions of its own resources (both personnel and equipment).
- **Control** - the authority to direct strategic, tactical and operational operations in order to complete an assigned key activity. This includes the ability to direct the activities of others engaged in the completion of that function, i.e. the crisis as a whole or a function within the crisis management process. The control of an assigned function also carries with it the responsibility for the health and safety of those involved.
- **Coordination -** the integration of the expertise of all the agencies/roles involved with the objective of effectively and efficiently bringing the crisis to a successful conclusion.

oak CONSULT

Disaster Recovery

- Disaster Recovery or DR is the ability of an organisation to provide critical Information Technology (IT) and telecommunications capabilities and services after it is disrupted by an incident, emergency or disaster.
- DR recovers the disrupted IT and telecommunications capabilities to ensure key activities can continue within a minimum period of time, pre-determined by the organisation, to planned levels of operations.

oak CONSULT

Exercising and Testing

- Exercising is a process that an organisation uses to assess, practice, or improve performance within their Business Continuity Plans.
- Exercises can be used to train personnel, to practice improvisation, to enhance communication and coordination, to identify resource gaps and performance improvement opportunities, and to validate policies, plans, procedures, and agreements.
- Whilst exercising is key element of accreditation to Business Continuity standards it really does help the organisation keep fit should the worst happen.

oak CONSULT

Full Rehearsal

- Linked with exercising, a Full Rehearsal is the ultimate exercise.
- The best equipped organisations carry these out.
- If it's carried out in similar conditions to a real incident, it will show you how the different elements of the plan fit together.
- This may be expensive, especially if it involves changing sites, but planning will reduce costs and the efforts might pay off in the future.

oak CONSULT

Gold, Silver and Bronze Teams

It can be useful to use the Gold, Silver and Bronze (GSB) structure to help define who should do what during an incident.

Gold

- This usually refers to the CEO or other senior managers who make strategic decisions about the business, and who will also take strategic responsibility for responding to an incident, for example speaking to the media about the incident. 'Gold' people will communicate strategic business decisions following a terrorist attack or other major incident directly to 'Silver' people.

Silver

- Usually a senior management team of experts within your business. Already involved in both your overall BCM approach and specific planning. They are responsible for co-ordinating and directing the resources of the business to ensure that the plans are being properly implemented. 'Silver' people will link directly to the 'Gold', keeping them updated on the developing situation.

Bronze

- Identified in your business continuity plan as responsible for recovering/restarting crucial business functions. They are responsible for ensuring that their specific business continuity plans are implemented. They take direction from 'Silver' people and keep them updated.

oak CONSULT

Hot, Warm, Cold and Dark Backup Sites

- A backup site or work area recovery site is a location where an organisation can easily relocate following a disaster or other disruptive event. This is an integral part of the DR plan and wider business continuity planning of an organisation.
- A backup site can be another location operated by the organisation, or contracted via a specialist company. In some cases, one organisation will have an agreement with a second organisation to operate a joint backup site.
- There are three types of backup sites, including cold sites, warm sites, and hot sites. The differences between the types are determined by the costs and effort required to implement each.

Hot Sites

- A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real time synchronisation between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialised software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before employees have relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to operate.

Warm Sites

- A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

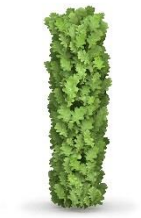
Cold Sites

- A cold site is the least expensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the incident.

Dark Sites

- A dark site has no facilities for staff and is built purely to host technology in the event of a major incident.

oak CONSULT



Invocation of Business Continuity Plans

- An invocation is an official declaration that an organisation's business continuity arrangements need to be formally activated or put into effect.
- An official invocation is necessary whenever a disruptive incident interferes with your organisation's ability to deliver key products and services.

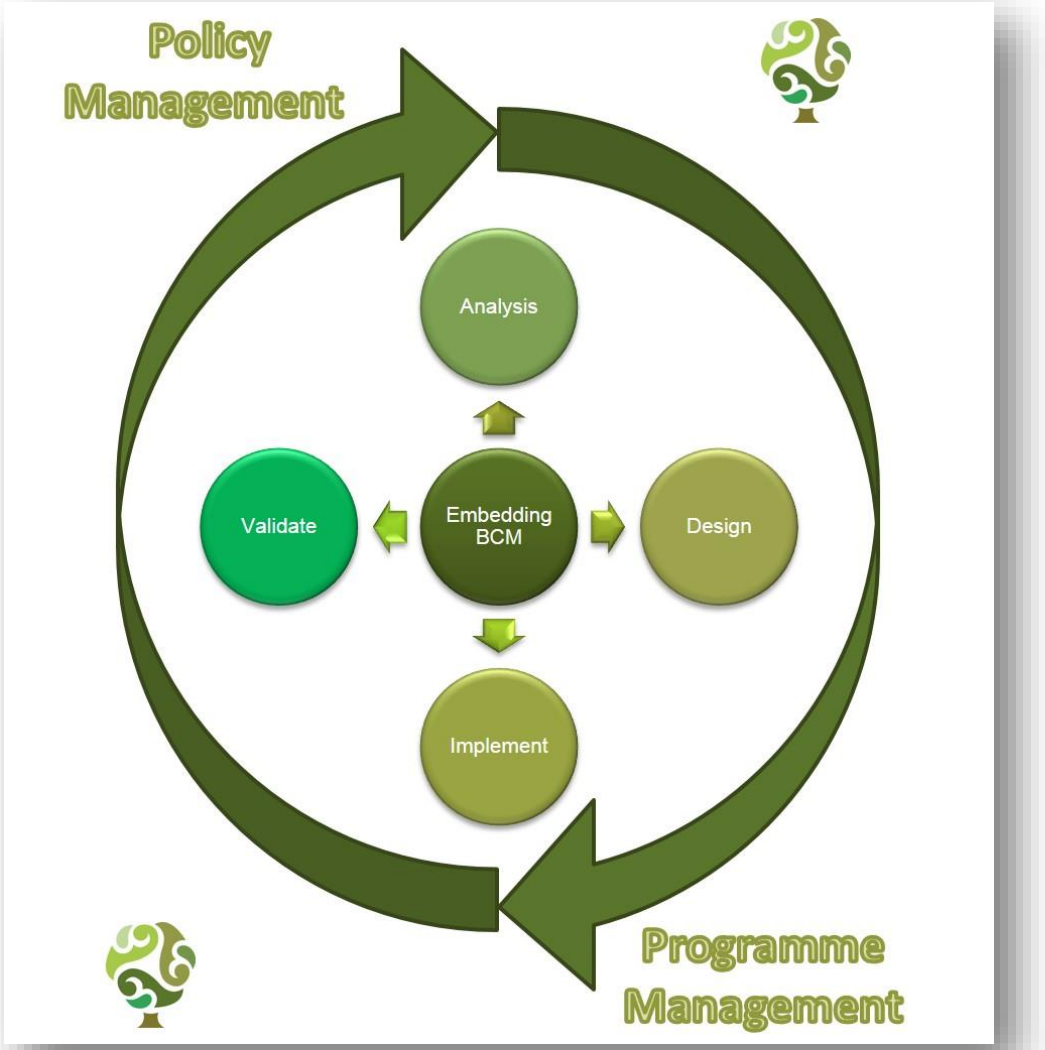
oak CONSULT

Justification for a Business Continuity Management System

- When I ask business owners about their position on business continuity planning, they often say that is that it's not something they are focused on, or that it is something they have thought about but not implemented. If you are the owner or senior manager of a business, then here are five good reasons why you should take Business Continuity seriously:
- **Regulatory** – In some areas of business, regulatory demands are high and business continuity planning is a requirement. Examples are financial services, insurance, utilities and public transport.
- **Customer Demand** – In an increasing number of cases, evidence of business continuity planning is demanded by customers. Companies are increasingly dependent on their suppliers and with the continued emergence of 'Just in Time' processes, suppliers can be a significant risk to their own business continuity. Thus, tenders and contracts often demand that potential suppliers prove their resilience.
- **Investor Requirement** – Organisations that fund or support start-ups and businesses undergoing expansion are risking their capital. Having in place a business continuity plan is a means of reducing some of the risks to which that investment is exposed.
- **Governance** – For many small businesses, it is a maturity thing. Once the owners recognise that they are in it for the long term, then they automatically start thinking about how to protect their long term investment in the business. The longer a business is operating, the more likely it will be exposed to a disruptive event, so it makes sense to plan how to survive the disruption.
- **Past Experience** – Lastly, the impetus to start planning often comes after the company has experienced an adverse event, or has seen the effect an adverse event has had on others.

oak CONSULT

Key elements of a Business Continuity Management System



oak CONSULT

Likelihood and Impact

- In the context of BCM, a risk assessment looks at the likelihood and impact of a variety of risks that could cause a business interruption. By assessing these, you will be able to prioritise your risk reduction activities.
- You should focus your risk assessment on the critical activities and supporting resources identified in the BIA stage. For this reason a risk assessment can only take place once a BIA has been completed.
- Risks could include:
  - Loss of staff
  - Loss of systems (IT and telecommunications)
  - Loss of utilities eg water, gas or electricity
  - Loss of, or access to, premises
  - Loss of key suppliers
  - Disruption to transport

Risk Impact					
	5	10	15	20	25 (High Risk)
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1 (Low Risk)	2	3	4	5
	Risk Likelihood				

oak CONSULT

Maximum Acceptable Outage (MAO)

- Maximum Acceptable Outage or MAO is the time frame during which a recovery must become effective before an outage compromises the ability of an organisation to achieve its business objectives and/or survival.

oak CONSULT

Notification Call Cascade

- Understanding the audiences that a business needs to reach during a major incident is one of the first steps in the development of a communications plan.
- There are many potential audiences that will want information during and following an incident and each has its own needs for information.
- The challenge is to identify potential audiences, determine their need for information and then identify who within the business is best able to communicate with that audience.
- Identifying the audiences and assigning ownership as to who is going to communicate with whom, when and with what information is a crucial part of your Business Continuity Management System.
- The following is a list of potential audiences:
  - Customers
  - Survivors impacted by the incident and their families
  - Employees and their families
  - News media
  - Communityóespecially neighbours living near your impacted offices
  - Company management, directors and investors
  - Government officials, regulators and other authorities
  - Suppliers

oak CONSULT

Objectives of Business Continuity

- At the very outset of a Business Continuity engagement I always like to clearly document the objectives of the project and gain agreement from the business owner / senior management team.
- This give a clear statement of intent and ensures that we can always ensure that we are delivering against the Business Objectives.
- Some examples might be:
  - To develop, implement, maintain, monitor, review and continually improve our Business Continuity Management System.
  - Determine the minimum level of services that are acceptable to the company to achieve stakeholder satisfaction during an unforeseeable incident.
  - Appoint a Business Continuity Team and hold regular meetings to discuss monitor and review business continuity progress.
  - Appoint an Incident Management Team to be responsible in the event of an incident.
  - Embark on an internal training programme to generate a better understanding amongst our staff of the importance of preventative measures to safeguard our business in the event of a crisis.
  - Ensure that the company has full confidence in providing business continuity in the event of a crisis through regular exercising of plans.
  - Develop an emergency number and website that staff can access for information and guidance should an incident occur.
  - Enhance corporate credentials when tendering for business and open up access to new markets.
  - To obtain formal certification to ISO 22301

oak CONSULT

Plans and Policy

- Below I've outlined some of the key documentation that would be expected for a typical Business Continuity Management System (BCMS), especially if you wished to gain ISO22301 accreditation:
  - Business continuity objectives
  - Scope of the BCMS and explanation of exclusions
  - Business Continuity Policy
  - Business Impact Analysis
  - Risk Assessment
  - Business Continuity Plans
  - Incident Management Plan
  - Communications Plan
  - Exercising Plan
  - Other documentation would be used for ongoing management of your BCMS such as exercising and training logs, audit reports and corrective actions

oak CONSULT

Qualitative and Quantitative Assessments

Qualitative Assessment

- The process for evaluating a business function based on observations and does not involve measures or numbers.
- Instead, it uses descriptive categories such as customer service, regulatory requirements, etc to allow for refinement of the quantitative assessment.
- This is normally done during the BIA phase of planning.

Quantitative Assessment

- The process for placing value on a business function for risk purposes.
- It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritisation.
- This is normally done during the BIA phase of planning.

oak CONSULT

Recovery Time Objectives and Recovery Point Objectives

Recovery Time Objectives

- The term recovery time objective refers to a time period.
- It is the maximum amount of time allowed to resume a critical activity, recover resources, or provide products and services after a disruptive incident occurs.
- This target time period must be short enough to ensure that adverse impacts do not become unacceptable.

Recovery Point Objectives

- The term recovery point objective refers to a data recovery objective.
- It is the point to which information or data used by an activity must be restored after a disruptive incident occurs.
- It is an information or data recovery objective that must be achieved in order to allow a critical activity to resume after a disruptive incident has occurred.

oak CONSULT

Supply Chain Management

- In a supply chain context, Business Continuity Management (BCM) is a highly useful risk mitigation technique for procurement professionals. By ensuring that key supply chains have business continuity plans (BCPs) in place, aligned with your own requirements, the impact of any disruption to these chains is likely to be reduced and faster recovery assured.
- It is good practice, of course, to have a BCP for your organisation as a means to identify key suppliers and your requirements on them.
- A supplier's BCP is always going to be aligned with the supplier organisation's objectives, not your own. So you are looking for reassurance that the plans they have in place to deal with disruption to their operations will also minimise disruption to your organisation.
- Therefore you should:
  - ask the right questions and interpret the answers;
  - get the right people involved, and in a timely manner;
  - build understanding and confidence among those asking business continuity questions.
- Research shows that the impact of supply chain failure through business continuity disruption is very common and commercial organisations are losing revenue and customer confidence as a result.
- Applying BCM through the supply chain can help ensure a common language and skill set when working with suppliers and partners supporting a faster response and quicker recovery.

oak CONSULT

Threats

- The Business Continuity Institute (BCI), in association with the British Standards Institution (BSI) produce an annual Horizon Scan based upon talking to businesses all over the UK.
- 77% of business leaders said they fear the possibility of an unplanned IT and telecoms outage, whilst 73% worry about the possibility of a cyber-attack or data breach.
- The report has also identified long-term trends, with 73% seeing the use of the internet for malicious attacks as a major threat that needs to be closely monitored, and 63% feeling the same way about the influence of social media.
- This year's top 10 threats to business continuity:
  1. Unplanned IT and telecom outages
  2. Cyber attack
  3. Data breach
  4. Adverse weather
  5. Interruption to utility supply
  6. Fire
  7. Security incident
  8. Health & Safety incident
  9. Act of terrorism
  10. New laws or regulations

oak CONSULT

Understanding and Training of Business Continuity

- Considerable resources are invested in business continuity readiness. However, training and awareness program development and execution is often very limited in my experience.
- A select group of executives, plan owners and response/recovery team members are often the only people aware that the programme exists.
- This lack of awareness drives an increased availability risk, and directly impacts the efficiency and effectiveness of the recovery effort.
- Take the time to measure awareness across your entire organisation.
- Take inventory of the methods used and the frequency of instruction.
- If you are one of the majority of organisations that could improve your training and awareness effort, take the time to formally organise and develop a training and awareness curriculum that makes all stakeholders aware of their roles and responsibilities during a crisis.

oak CONSULT

Vital Records

- In this digital age many organisations have set up comprehensive systems to ensure that electronic records are safely stored and backed up, with a plan in place should an unexpected crisis occur. These days most employees rely on electronic systems to do their job and lost or damaged files can spell disaster. However, while IT systems are often carefully considered and any perceived emergencies planned for, paper records can frequently be neglected.
- Many organisations are under a legal obligation to keep certain records for a specified period of time. For example, financial institutions are now required to keep mortgage loan files for up to ten years after the loan has been repaid. Some medical records must be stored throughout the life of the patient and government institutions are now required to keep certain records for up to 50 years.
- The first rule of thumb for any organisation should be to assess their records according to the following criteria: business value, legal value, administrative value, historical value. The records can then be classed as vital, important, useful or non-essential. For those records deemed vital, the next step is to ensure that the storage of those records is an integral part of your business continuity plan and this means considering how and where they are stored. In exactly the same way as you would safeguard your IT systems and electronic records, consideration should be given to the possible disaster scenarios and how you can guard against loss or damage of those records.

oak CONSULT

Workarounds

- A workaround is an alternative process used to replace the normal ëbusiness-as-usualí process or IT system which may be unavailable during business disruption. When determining the Maximum Acceptable Outage (MAO) for a business function, whether or not there are manual, paper-based workarounds is a factor that can help work out how long you can afford to be offline from your IT systems and possibly allow you to implement a lower cost ëwarmí or ëcoldí solutioní instead of a ëhotí one.
- These workaround procedures define the interim tasks to keep the process going whilst the IT systems or other resources are being recovered.
- When considering how long a process can operate manually one area to beware of is the backlog effect. At time of incident, if the volume of work remains constant but the rate of processing is slower because it is manual, an increase in workload builds up which will result in backlog. This backlog may increase exponentially for as long as you are not processing at full capacity. For each process there comes a time when no matter how much overtime you throw at it, it is very costly or impossible to catch up.
- It is important to consider what this threshold may be for your process and what the absolute maximum period of time is that the process can operate manually and still feasibly recover. It is wise to allow some contingency between the RTO you select and your absolute maximum time operating manually to ensure that you have some breathing space in case something goes wrong with the recovery efforts.
- As a result, how long will your area will be able to function using manual workaround procedures should be revisited during your areaís BIA updates and tested as part of your business continuity exercise program.

oak CONSULT

Xerox and other document management solutions

- The safe storage of business documents is a vital part of an organisation's business continuity plan. Having a document management and archiving solution in place is key to this strategy.
- Document management technology, which can be tightly integrated into organisations' accounting and other systems, enables their inbound and outbound paper documents to be scanned and logged. Once in the electronic archive, all documents are securely stored and can be retrieved by drilling down through the various systems or stored in the cloud for better protection.
- There are a plethora of tools available on the market that can integrate with your business and reduce the risk of loss of vital paper records.

oak CONSULT

Yearly Checks

- As a minimum all Business Continuity Plans and other documentation should be reviewed and tested every year. To make this task less onerous, I would advise spreading the load across the year and across your plan owners so that some activity is happening each month and can be reported back into your quality management reviews.

oak CONSULT

Zero Downtime

- Less than a decade ago, most IT departments pursued a business continuity strategy that was based on duplicate servers, redundant resources, dedicated networks, and backup sites. These strategies were inherently expensive and characterised by overcapacity and manual processes.
- Virtualisation and cloud computing have significantly improved both the quality and the economics of business continuity solutions in many ways: reducing hardware costs by replacing siloed applications with mobile virtual machines, facilitating clustering, and allowing organisations to perform data migration to their backup sites, achieving 99 percent intact data so that all data can be accessed.
- In addition, with the development of virtualised desktop solutions in which all user applications reside on servers, IT departments can restore business operations to normal more quickly because they can quickly provide employees with access to their data and applications from anywhere.
- Whilst Zero downtime is still not an option for many business, technology has certainly made this much more achievable.
- I hope you enjoyed reading this A to Z. On the face of it, setting up a Business Continuity Management System is an arduous and complex process. It isn't. If set up correctly in the first place and with senior management support and a good exercising / embedding plans you can start to sleep a little more soundly at night!
- If you would like further information about how Oak Consult can help you, please call us today or click here.

oak CONSULT

Transform, Grow & Protect Your Business with

oak CONSULT