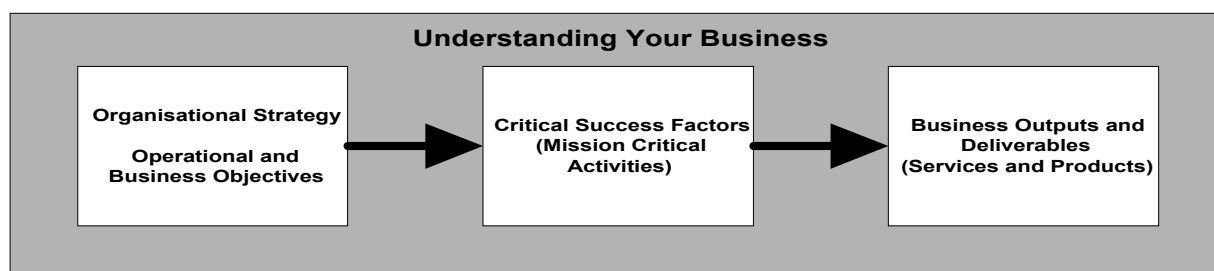


Stage 1: Understanding Your Business.



Introduction.

Understanding your business is about the analysis of the operational aspects of an organisation; both public and private sector, and provides the foundation upon which all Business Continuity Management (BCM) is based.

It is not only about understanding the organisation and its business but establishing what is critical for its continuance. Consequently, a mission statement and key supporting aims that indicate the raison d'être of the organisation is essential. Within this context there are five basic questions to be asked:

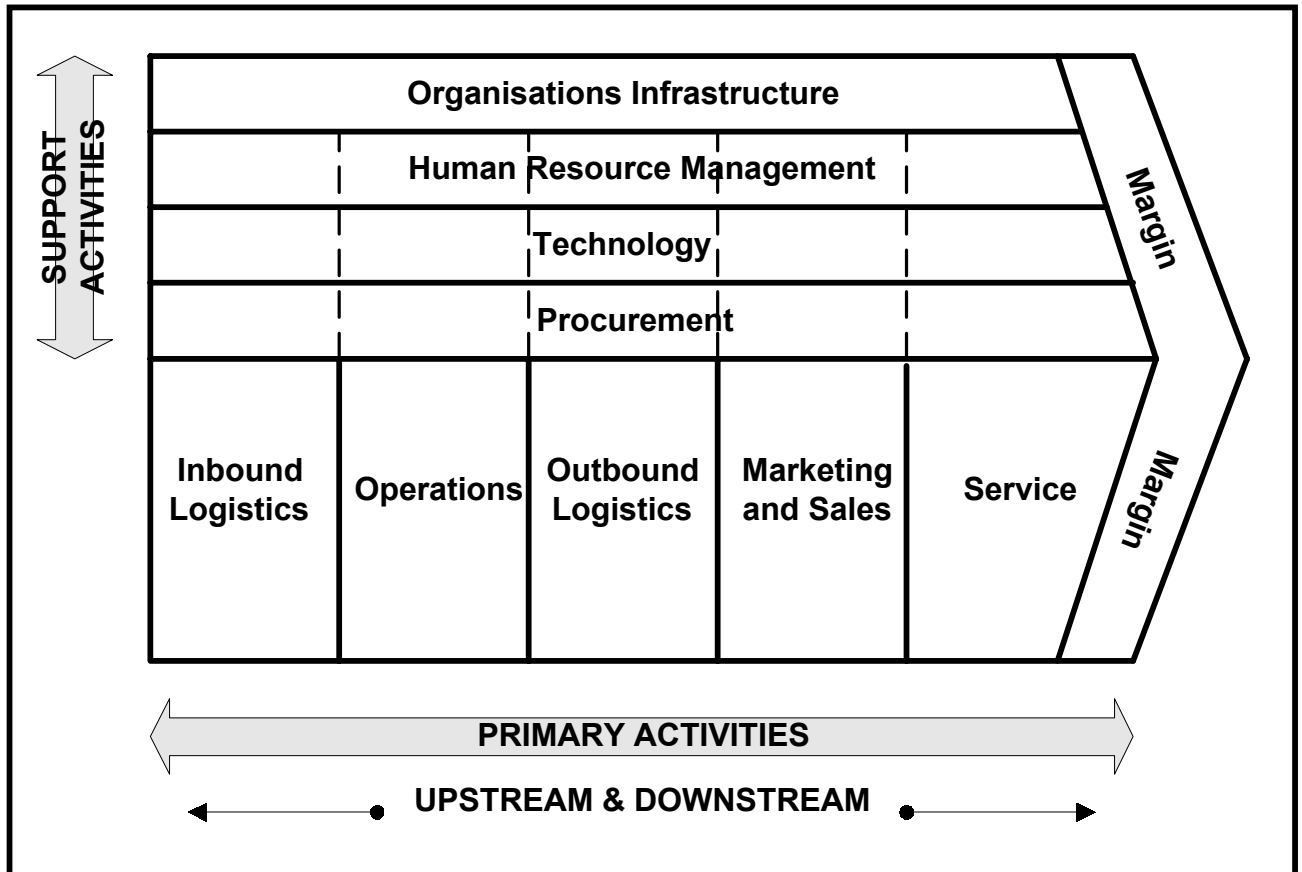
- What are the key business objectives of the organisation?
- What are the outputs/deliverables i.e. products/services of the business objectives?
- When are the business objectives to be achieved?
- Who is involved (both internally and externally) in the achievement of the business objectives?
- How are the business objectives to be achieved?

It is the Mission Critical Activities (MCA) and their dependencies that enable the achievement of the business objectives i.e. services and products. It is upon these activities that BCM must be focused. An organisation has many dependencies both internally and externally that may either support or provide the Mission Critical Activities. A further key factor is the single point of failure to a Mission Critical Activity i.e. there is no alternative. The elements of Mission Critical Activities include:

- Human Resources.
- Stakeholders.
- Suppliers (intra-organisation and/or outsourced providers).
- Customers/Clients
- Facilities.
- Functions.
- Processes.
- Materials.
- Technology.
- Telecommunications.
- Data (all formats and media).

Porter’s Value Chain Analysis (M.E. Porter 1985 ‘Competitive Advantage: Creating and sustaining superior performance’ Free Press, New York) process model of an organisation provides a very useful method of understanding how an organisation functions. Its application enables an examination of all the organisation’s activities to assist in identifying its Mission Critical Activities their dependencies and single points of failure.

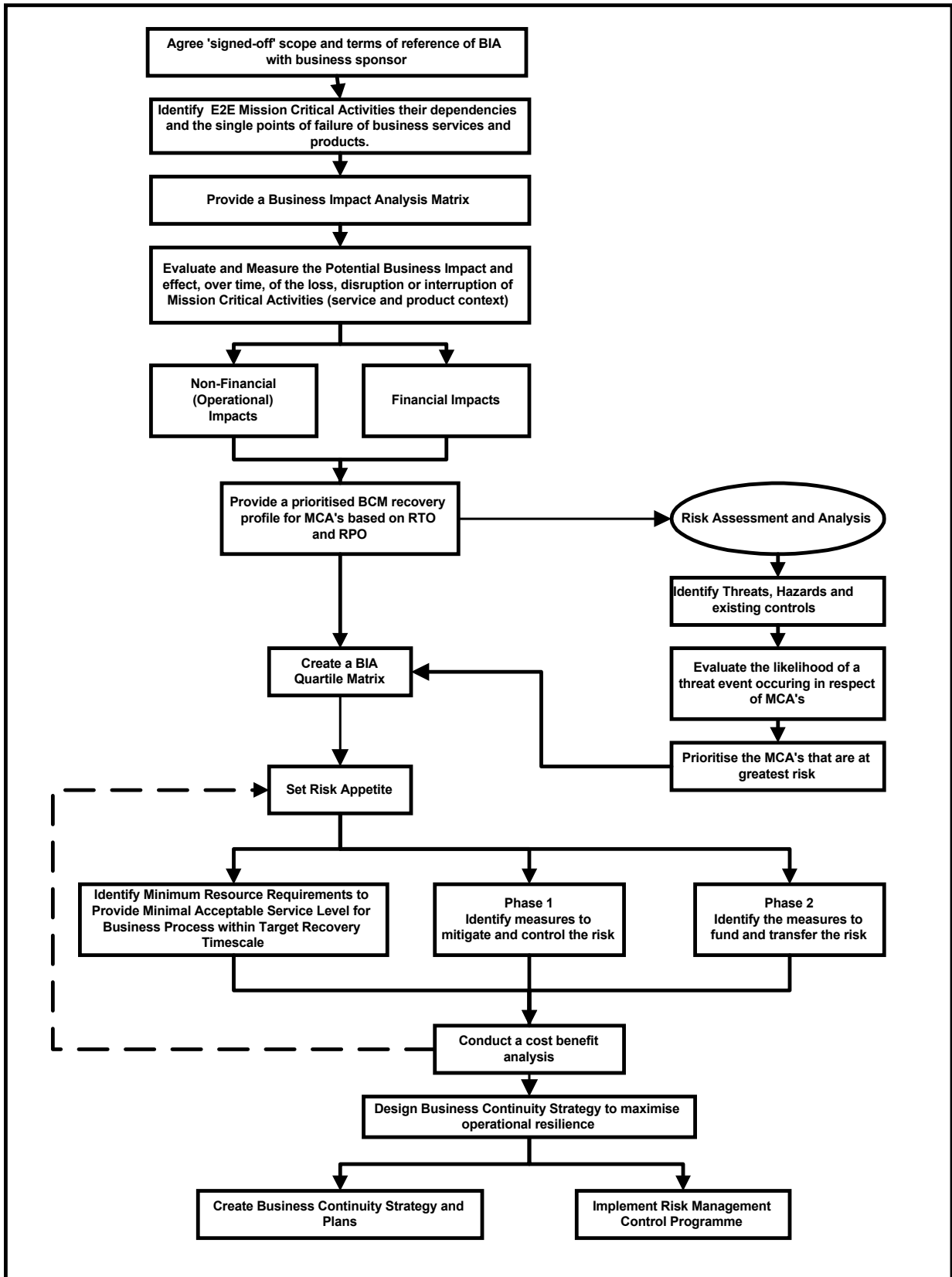
Porter’s Value Chain Analysis.



The top four sections (a) Firm Infrastructure, (b) HRM, (c) Technology Development, Procurement add support value of a product or service. The main value adding activities are identified as (a) Inbound Logistics, (b) Operations, (c) Outbound Logistics, (d) Marketing and Sales, (e) Service, are the primary value adding variables.

Understanding your business and identifying its Mission Critical Activities their dependencies and single points of failure consists of two distinct but complementary processes. The first is a Business Impact Analysis (BIA) and the second a Risk Assessment and Analysis (RA). The Business Impact Analysis process also contains a Business Impact Resource Recovery Analysis (BIRRA).

A Business Impact Analysis and Risk Assessment Process.



BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

It is important to identify the organisation’s Mission Critical Activities at any early stage. The involvement of representatives from these Mission Critical Activities and their dependencies is essential and will add value to the process. A further key point (Meredith 1998) is that it is easier to teach someone to carry out a Business Impact Analysis than it is to teach someone your business.

An organisation also has many external influences that can affect its Mission Critical Activities. These can include:

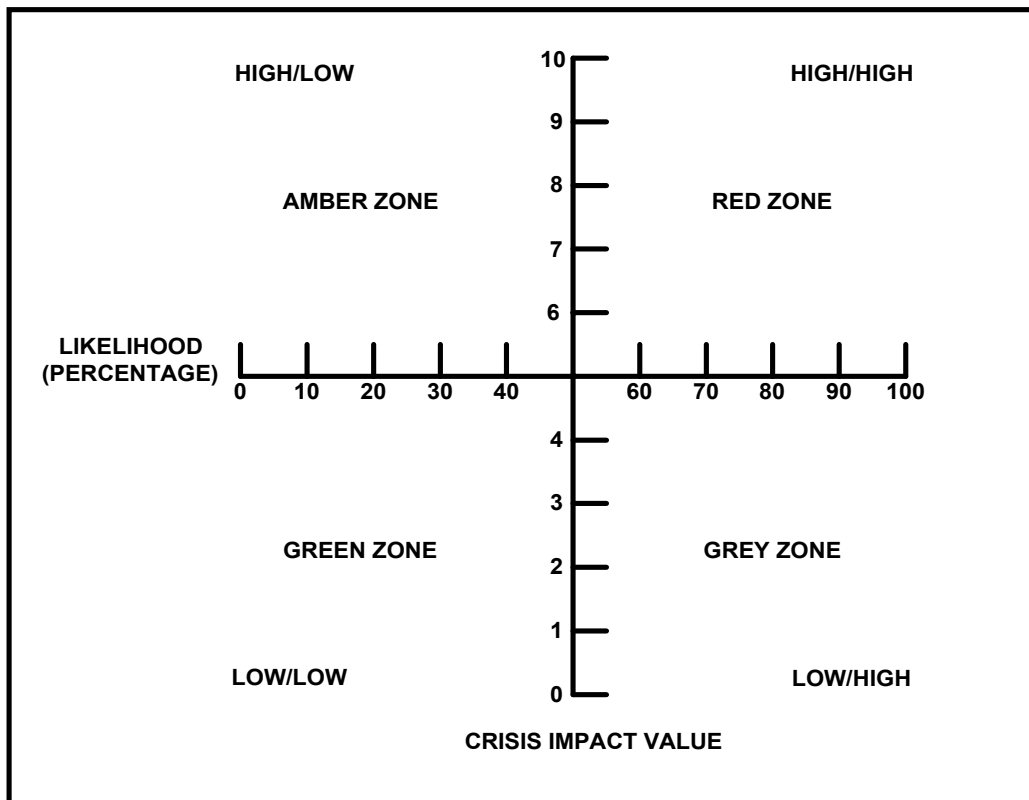
- Government Departments.
- Regulators.
- Competitors.
- Trade/Industry Bodies.
- Professional Associations.
- Trade Unions.
- Pressure groups.
- Clients/Customers.

It is equally important to identify these key influential stakeholders at an early stage and to take their view(s) and requirements into account.

As a result the key to understanding a business is founded upon identifying:

- Mission Critical Activities.
- Internal and external Mission Critical Activity dependencies
- Single points of failure to Mission Critical Activities.
- External influences that may impact upon Mission Critical Activities.

BUSINESS IMPACT ANALYSIS and Risk Quartile Matrix.



BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

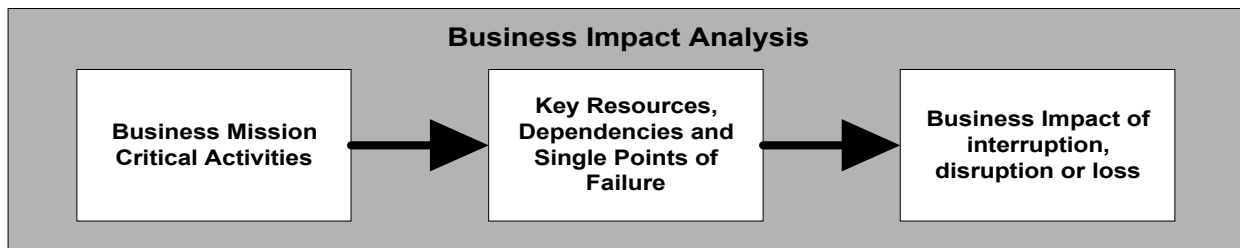
Having identified the organisation's Mission Critical Activities, their dependencies and single points of failure it is important to determine the impact upon the organisation if any of them were disrupted, interrupted or lost. The level of impact also provides a challenge and review process whereby activities and their dependencies can be assessed as to their mission criticality and rating in any business continuity prioritisation process.

Once the Business Impact Analysis has identified the organisation's Mission Critical Activities it will take into account the time sensitivity of each to disruption, interruption or loss and this will determine the BCM Recovery Time Objective(s) (RTO), Recovery Point Objective(s) (RPO) and Level of Business Continuity (LBC). The outcome of the Business Impact Analysis enables the organisation to focus its risk assessment (RA) on the Mission Critical Activities of the organisation rather than conducting a traditional all risks analysis.

After completing both the Business Impact Analysis and Risk Assessment it is important to combine their findings to produce a ranking system based on a Business Impact Analysis and Risk Assessment Quartile Matrix. This informs and enables the identification of those areas where the organisation's BCM efforts and investment should be concentrated based on its risk appetite.

This approach should ensure the setting of a risk appetite prior to the organisation agreeing its BCM strategy and solutions. The strength of this process lies in its focus upon business impact and risk rather than an immediate focus on a cost benefit analysis of BCM solutions that will probably unduly Business Impact Analysis and prematurely affect the outcome.

Business Impact Analysis (BIA).



Introduction.

The Business Impact Analysis underpins the whole BCM process. It is a linear process and consists of techniques and methodologies that can be used to identify, quantify and qualify the business impacts and their effects on an organisation of a loss, interruption or disruption of a Mission Critical Activity(ies) and/or their dependencies including their intra-organisation and outsourced provision. It further identifies the minimum level of resources via a Business Impact Resource Recovery Analysis (BIRRA) required to enable an organisation to achieve its Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for Mission Critical Activities.

The key to a Business Impact Analysis is the recognition that it needs to be conducted and analysed in an End-to-end (E2E) business service/product context and not as individual 'stove pipe' components, processes or functions.

An organisation's risk appetite should not be considered and set before undertaking a Business Impact Analysis. It is the Business Impact Analysis and any subsequent risk assessment that informs the setting of a risk appetite.

Purpose.

The purpose of a Business Impact Analysis is to:

- Identify an organisation's Mission Critical Activities their dependencies and single points of failure.
- Identify the impact and effect of the loss, interruption or disruption of an organisation's Mission Critical Activities.
- Inform and enable the setting of an organisation's risk appetite.
- Inform and enable the options for developing the resilience of the organisation's business operations
- Inform and enable the setting of an organisation's business value based BCM strategy and solutions.
- Inform and enable an organisation to prioritise its recovery profile for Mission Critical Activities and their dependencies (minimum required level at which Mission Critical Activities can viably operate by setting clear Recovery Time Objectives (RTO) and

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Recovery Point Objectives (RPO) for the business continuity of each Mission Critical Activity and dependency.

- Provide a BCM recovery resource profile that identifies the minimum level resources necessary for an organisation to achieve the prioritised recovery profile of its Mission Critical Activities and their dependencies.

Outcome(s).

The outcomes from a Business Impact Analysis include the identification and documentation of:

- Organisational aims, objectives and outputs (services and products).
- End-to-End (E2E) Mission Critical Activities (service and product context), their dependencies and single points of failure (including seasonal trends and/or critical timing issues).
- Financial and non-financial impacts and effects (consequences) resulting from the disruption, interruption or loss of one or a number of Mission Critical Activities over various time periods.
- The BCM objectives for each of the organisation's Mission Critical Activities and their dependencies.
- A prioritised minimum acceptable resource recovery configuration, overtime, that is required to enable a predefined minimum level of business continuity (LBC) of Mission Critical Activities and their dependencies.
- Vital Records/Data (all media).
- Key Customers, Clients and Stakeholders.
- Suppliers (intra-organisation and/or outsourced providers).
- Constraints (contractual and other).

Components

The key components of a Business Impact Analysis include:

- Porter's Value Chain analysis.
- Self assessment questionnaires - paper and automated.
- Checklists.
- A Business Impact Analysis Matrix (BIAM). The matrix includes the following components:

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- **Over time:** Time is usually expressed in days (or parts of a day) but in some situations may be considered as minutes and hours. Its purpose is to determine the maximum period of time that a Mission Critical Activity can be degraded or lost before the impact becomes unacceptable.
- **Types and Effect:** The types of business impact are usually described as financial and non-financial. The non-financial impacts are usually divided into specific types of impact that relate directly to brand, staff, legal, regulatory, customer service, and customer confidence issues.

The effects of financial loss include: loss of revenue, bad debts, loss of shareholder value, additional operating costs, penalties and lost opportunity cost.

The effects of non-financial and operational impact include: loss of market share, loss of reputation, brand tarnish, loss of processing capability, dilution of quality and extended processing times must also be recognised.

A Business Impact Analysis Matrix.

TYPE OF IMPACT AND ITS EFFECTS	IMPACT DESCRIPTORS AND EVENT CATEGORISATION			
	Catastrophic	High	Medium	Low
FINANCIAL				
Loss of Revenue	<£100m *	>£100m *	>£10m *	>£1m *
Loss of Shareholder value				
Penalties				
Bad debts				
Additional operating cost(s)				
NON-FINANCIAL				
Reputational Loss	* Adverse and sustained national media campaign and/or loss of confidence/ trust by market, public and/or damage to brand image and trust.	*Adverse comment in national media and/or loss of confidence in a range of service and/or products or several parts of the organisation.	*Adverse comment in national media and/or loss of confidence in specific service and/or product or part of organisation.	*Adverse comment in local media only and/or confined to a limited number of localised customers.
Loss of Operational Capacity				
Customer Service				
Regulatory/Legal				
Loss of Market Share				
Loss of Quality				
Brand Tarnish				
Environmental				
Contractual				
Staff Moral				
Political				

* EXAMPLES ONLY

- **Description:** The level of business impact and its effects are evaluated by reference to a set or range of predefined impact criteria descriptors e.g. the level and type of adverse media comment (national or local level); the number and type of customers/clients affected; the number and type of services/products affected; the impact on the organisation (as a whole, several parts or one department).
- **Categorisation:** The categorisation of an event/incident is directly linked to the predefined impact descriptors and is usually based on the four categories of Catastrophic, High, Medium and Low. It is this categorisation that informs and enables the prioritisation of Mission Critical Activities and their Recovery Time Objective(s) (RTO), Recovery Point Objective(s) (RPO) and minimum acceptable Level of Business Continuity (LBC).
- **Business Impact Recovery Resource Analysis (BIRRA):** This analysis identifies the minimum level of resource(s) necessary to achieve the prioritised recovery profile of Mission Critical Activities.

Methodologies/Techniques.

The methods, tools and techniques to carry out a Business Impact Analysis include:

- Templates.
- Checklists.
- Workshops (facilitated by a professional BCM practitioner).
- Questionnaire(s) - paper and automated software.
- Interviews (structured and unstructured).
- Business Impact Analysis Matrix.

Whilst a variety of proprietary software products are available to conduct a Business Impact Analysis they are not essential to enable a successful completion of a Business Impact Analysis.

A key principle in conducting a Business Impact Analysis is to keep the process (it) simple and straightforward (KISS). This approach is frequently based on the organisational design and use of self-assessment Business Impact Analysis formats.

Business Impact Analysis results should be presented in a graphic (table, pie or bar chart) or matrix format. This enables the different categories of effect in relation to the different types of impacts to each Mission Critical Activity to be compared.

However, care must be taken to fully understand the operation of an organisation as a whole before giving focus to any specific area.

Process.

The following key issues should be fully considered in conducting a Business Impact Analysis:

- A Business Impact Analysis should be conducted and analysed in an End-to-End (E2E) business service/product context;
- The Business Impact Analysis (BIA) part of the process should be carried out by the business managers as they are better placed to correctly assess any impact effect whilst having a specific role in the setting of the organisation risk appetite.
- The Business Impact Resource Recovery Profile (BIRRA) should be carried out by operational staff as they are best placed to identify the resources that are required to achieve the Recovery Time Objectives and Recovery Point Objectives of each Mission Critical Activity.

The key constructs of a Business Impact Analysis include:

- The scope and terms of reference of the Business Impact Analysis agreed and 'signed-off' by the organisation sponsor.
- Identify and notify the knowledgeable and credible business managers, operational supervisors and staff.
- Develop a self assessment Business Impact Analysis survey questionnaire.
- The survey questionnaire should contain, as a minimum, the following elements:
 - Clear instructions on how to complete the questionnaire.
 - Clear guidance concerning the following issues:
 - A help line.
 - The component parts of an organisation retain their individual business risk and are responsible for their BCM competence and capability.
 - BCM is not just about Information Technology Disaster Recovery (ITDR) and off-site (third party) restoration of services and facilities.
 - Points that encourage forward planning.
 - Global or multi-site organisations may provide a BCM capability in consequence of their geographic and site structure.
 - **Business Impact Analysis:** Good practice indicates this section should be completed and 'signed-off' by the business owner of the product, service or a component part.
 - The identification of Mission Critical Activities their dependencies and single points of failure including seasonal trends and time critical issues.
 - The identification and categorisation of business impacts based on the loss, disruption or interruption of Mission Critical Activities.
 - Establishing Recovery Time Objectives and Recovery Point Objectives.

- **Business Impact Recovery Resource Analysis:** Good practice indicates this section should be completed and 'signed-off' by operational staff and supervisors. The analysis should identify the minimum level of resource required, over time, to achieve the Recovery Time Objectives and Recovery Point Objectives of the Mission Critical Activities recovery profile. The types of resources typically include:
 - Staff and Managers;
 - Technology;
 - Software applications;
 - Telecommunications;
 - Connectivity Links;
 - Supporting Systems;
 - Data (all formats and media);
 - Facilities (workstations);
 - Office Equipment;
 - Specialist Equipment;
 - Relocation site special requirements;
 - Constraints (contractual or otherwise).

- Distribute the survey questionnaire and collect responses by agreed date.
- Analyse and review completed survey questionnaires.
- Conduct follow-up interview(s) with questionnaire respondents as necessary.
- Analyse and review survey data.
- Prepare draft report of survey findings and consult (verify/validate results) with respondents.
- Prepare final draft report of findings for the business sponsor.
- Report agreed and 'signed-off' by business sponsor. This is absolutely key: first to ensure the business sponsor understand the results and secondly to justify where resourcing may be required to implement a BCM programme.

Frequency and Triggers.

The frequency that a Business Impact Analysis should be carried out or reviewed is dependent upon the nature, scale and complexity of the organisation based on its business risk profile, appetite and the environment in which it operates. Good practice indicates a Business Impact Analysis should be carried out at least every 12 months unless:

- It is an initial Business Impact Analysis.
- The pace of business change is particularly aggressive.
- The initial outsourcing or intra-organisation sourcing of a Mission Critical Activity or dependency.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- A significant change in the key technology and/or telecommunications including systems and/or networks.
- There is a major business change that may include:
 - Business strategy or objectives.
 - BCM strategy and/or scope.
 - BCM solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation and/or outsourced providers)
 - Post BCM event.
 - Process re-design.
 - New business line or product or service.
 - Merger.
 - Acquisition.
 - Significant change in the regulatory environment.

Participants.

The following roles or functions (not restrictive or exhaustive) are identified as being either Responsible or Accountable or should be either Consulted or Informed (RACI) in the Business Impact Analysis. The matrix process provides a process that can be used to indicate/identify the specific roles, functions and/or area of the organisation within each of the RACI categories.

Role or Function	R	A	C	I
	Responsible	Accountable	Consulted	Informed
Executive Senior Business Management (Business Impact and Risk Appetite)				
Supervisors and Operational staff (Business Impact Resource Recovery Analysis Profiling)				
Change Management				
Professional BCM practitioner				
Subject Experts (where appropriate)				
Suppliers (intra-organisation and/or outsourced providers)				

Deliverable(s)

The deliverables of a Business Impact Analysis include:

- A clearly defined, documented, up-to-date and fit-for-purpose Business Impact Analysis 'signed-off' by the sponsor.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- A clearly defined, documented and prioritised timeline of activities for the recovery of the organisation's Mission Critical Activities and/or their dependencies.
- A clearly defined and documented risk (business impact) appetite including residual risk 'signed-off' by the sponsor.
- A clearly defined and documented schedule of priorities for BCM and Business Continuity investment subject to the organisation's risk appetite.
- A clearly defined and documented BCM resource recovery profile identifying the minimum level of resources, overtime, necessary to achieve the prioritised recovery profile of Mission Critical Activities and/or their dependencies.
- A clearly defined and documented multi-level Business (financial and non-financial) Impact Analysis Matrix.

Good Practice Evaluation Criteria.

The Good Practice evaluation criteria for a Business Impact Analysis (BIA) includes:

- Does the organisation have clearly defined and documented Business Impact Analysis Policy.
- Are the main business units within the organisation involved in preparing and conducting their BIA?
- Has the organisation adopted a clearly defined and documented standard BIA methodology?
- Has the organisation adopted a clearly defined and documented standard multi-level financial and non-financial Business Impact Analysis Matrix?
- Does the BIA conform to the Business Continuity Institute (BCI) Good Practice Guidelines?
- Have the organisations business staff and managers been fully trained in the use and application of the BIA criteria, methodology and tools?
- Does the BIA process clearly identify the need for external expertise where appropriate?
- Does the BIA use a Mission Critical Activity and/or their dependencies failure impact to measure criticality in contrast to an event-driven (list of risks) process.
- Does the BIA Matrix consider the potential of the following types of impact?
 - Human Resources (non availability of key personnel i.e. specific skills, experience, knowledge, decision makers, concentration of key skills at a single location and management hierarchy)
 - Operational
 - Financial.
 - Loss of Stakeholder value

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Reputation.
 - Brand.
 - Legal.
 - Regulatory.
 - Customer Service.
 - Supplier (internal and/or outsourced providers).
- Has the current BIA been completed within the last 12 months?
 - Has the date of the next BIA and organisational role to complete it been identified and clearly documented?
 - Is there a process to challenge and review the BIA as a part of a periodic updating of the BIA?
 - Has the current BIA been conducted in End-to-End (E2E) business service/product context?
 - Have the effect(s) of the potential loss, interruption or disruption of Mission Critical Activities or their dependencies e.g. the inability of a bank to clear payments, been fully assessed and documented?
 - Has the owner of the business service/product or its component part 'signed-off' of the current BIA as up-to-date and fit-for-purpose?
 - Has the organisation clearly identified, defined and documented its Mission Critical Activities?
 - Has the organisation clearly identified, defined and documented its Mission Critical Activities dependencies?
 - Has the organisation clearly identified, defined and documented its Mission Critical Activities single points of failure?
 - Has the organisation clearly identified, defined and documented its outsourced (third-party) supplier(s) of its Mission Critical Activities and their dependencies?
 - Have the providers of sourced (internal and/or outsourced) Mission Critical Activities and their dependencies been informed of their criticality?
 - Has the organisation clearly defined and documented the Recovery Time Objective (RTO) for its Mission Critical Activities (products and services) their dependencies and single points of failure?
 - Has the organisation clearly defined and documented the Recovery Point Objective (RPO) for its Mission Critical Activities (products and services) their dependencies and single points of failure?
 - Has the organisation clearly defined and documented the Level of Business Continuity (LBC) for its Mission Critical Activities (products and services) their dependencies and single points of failure?

- Has the owner and/or manager of each Business Critical Activity and its dependencies agreed and 'signed-off' the RTO, RPO, LBC and BIRRA in respect of their Mission Critical Activity and its dependencies.
- Has the organisation identified critical business projects and included them in the process of interdependency mapping in relation to Mission Critical Activities their dependencies and single points of failure?
- Have the dependencies and interdependencies for Mission Critical Activities on the following been identified, defined and documented as a part of the BIA?
 - Human Resources (key personnel);
 - Technology;
 - Software (including bespoke applications, spreadsheets and databases);
 - Telecommunications;
 - Connectivity Links;
 - Data (all formats and media together with their location);
 - Facilities;
 - Outsourced and/or internally sourced of Services;
 - Equipment/Machinery;
 - Key and/or unique records/documents;
 - Site special requirements.
- Have critical Human Resources (key personnel, skills, knowledge, expertise) been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical telecommunications been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical IT systems been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical connectivity links been identified, documented and their RTO clearly defined as a part of the BIA?
- Has critical software (including bespoke applications, spreadsheets and databases) been identified, documented and their RTO clearly defined as a part of the BIA?
- Has critical data (all formats and media together with their location) been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical facilities e.g. sites, been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical equipment/machinery been identified, documented and their RTO clearly defined as a part of the BIA?
- Have critical key and/or unique records/documents been identified, documented and their RTO clearly defined as a part of the BIA?

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Has the organisation identified, clearly defined and documented the minimum requirements, over time, of the following resources, as a part of an up-to-date Business Impact Recovery Resource Analysis (BIRRA), to realistically achieve the Recovery Time Objectives, Recovery Point Objectives and Level of Service Continuity of its Mission Critical Activities their dependencies and single points of failure?
 - Human Resources (staff dependencies - key personnel - numbers and skill sets);
 - Technology;
 - Software (including bespoke applications, spreadsheets and databases);
 - Telecommunications;
 - Connectivity links;
 - Data (all formats and media together with their location);
 - Facilities (work stations);
 - Outsourced and/or internally sourced services;
 - Equipment/Machinery;
 - Key and/or unique records/documents;
 - Relocation site special requirements;
 - Specialist services.

- Does the organisation have a process to ensure that a BIA is carried out as a part of all project and change management including new developments of (and major changes to) IT systems, services and their sourcing?

- Are the results of the BIA used to identify risk concentrations within the organisation?

- Are the results of the BIA presented in graphic or matrix format to enable effects and impacts to each Mission Critical Activity and its dependencies to be compared?

- Does the organisation use the BCI BCM Good Practice Guidelines as a part of its BCM BIA assurance process?

- Does the BIA process achieve the BIA outcomes set out in the Business Continuity Institute BCM Good Practice Guidelines?

- Does the BIA process provide the BIA deliverables set out in the Business Continuity Institute BCM Good Practice Guidelines?

Further Reading.

Birch, D. (2002) 'Business Continuity Management for telecommunications', Continuity, Vol.6, No.1, pp.10-13.

Business Continuity Institute, (1999) 'Benchmarking Business Continuity Management' Business Continuity Institute, Worcester.

Business Continuity Institute, (2000) 'The ten competencies of Business Continuity Management' Business Continuity Institute, Worcester.

Business Continuity Institute, (2001) 'Getting Started' Business Continuity Institute, Worcester.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Central Computer and Telecommunications Agency, (1995) 'An introduction to Business Continuity Management', HMSO, London. ISBN 0-11-330669-5.

Chadwick, T. (2001) 'Setting the scene: e-Business Continuity Management issues', *Continuity*, Vol.5, No.4, pp.7-9.

Charters. I. (2000) 'The reality of worst case scenarios', *Continuity*, Vol.4, Issue.4, pp.7-8.

Chase, R. (1999) 'Brands and intellectual property', *Continuity*, Vol.3, Issue.4, pp.12-14.

Elliott, D., Swartz, E., Herbane, B. (1999) 'Business Continuity Management: Preparing for the worst', Income Data Services, London. ISBN 0-905525-56-6.

Elliott, D. (2000) 'Three steps to better continuity', *International Journal of Business Continuity Management*, Vol.1, Issue 2, pp.8-10.

Federal Reserve Bank. (2002) 'Summary of lessons learned and implications for Business Continuity Management', Federal Reserve Bank, New York, pp.1-10.

Federal Reserve Bank. (2002) 'Implications of 9/11 for the financial services sector', *Bank of International Settlement Review*, pp.1-5.

Fenn, D. (2002) 'Supplier Continuity: Managing risks across the supply chain', *Continuity*, Vol.6, No.1, pp.4-6.

Financial Services Authority. (2001) 'A risk focused review of outsourcing in the UK retail banking sector', Financial Services Authority, London, pp.1-19.

Financial Services Authority. (2002) 'A Business Continuity Management risk matrix', Financial Services Authority, London, pp.1-20.

Financial Services Authority. (2002) 'FSA working paper on Business Continuity Management', Financial Services Authority, London, pp.1-19.

Fink, S. (1986) 'Crisis Management: Planning for the inevitable', Amacom, New York. ISBN 0-8144-5859-9.

Kirvan, P.F. (2000) 'Business Continuity Strategies for call centres', *Continuity*, Vol.4, No.2, pp.9-10.

Knight, R.F. AND Pretty, D.J. (2000) 'The impact of catastrophes on shareholder value', *Oxford Executive Research Briefings*, Templeton, College.

Meredith, B. (1998) 'Business Impact Analysis', *Continuity*, Vol.2, Issue.1, pp.4-77.

Newton, J. and Pattison, R. (1998) 'The business implications of wide spread disasters', *Continuity*, Vol.2, No.2, pp.5-8.

Mitroff, I.I. and Pearson, C.M. (1993) 'Crisis Management: A diagnostic guide for improving your organisations crisis preparedness', Jossey-Bass, San Francisco. ISBN 1-55542-563-1.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Porter, M.E. (1985) 'Competitive Advantage: Creating and sustaining superior performance', Free Press, New York.

Power, P. (1999) 'Business Continuity Management: Preventing chaos in a disaster', Department of Trade and Industry, London.

Rassam, C. (1999) 'A matter of control', Survive, February Issue, pp.58-59.

Videos.

Business Continuity Institute (2001) 'Back to Business: Planning ahead for the unexpected', Merlin Communications Ltd, Cirencester, Gloucestershire.

Case Studies.

Ckonjevic, M. (2001) 'The Californian power crisis', Continuity, Vol.5, Issue. 2, pp.8-9.

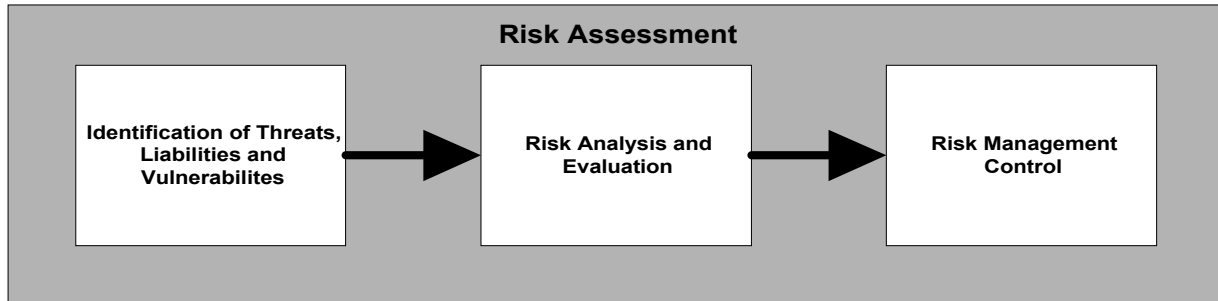
Dombrick, J. (2001) 'British Airways: A business continuity plan in practice', Risk Management, Vol.6, Issue.1, pp.5-8.

Federal Reserve Bank (2002) 'Summary of lessons learned and implications for business continuity', pp.1-10.

Federal Reserve Bank (2002) 'Financial industry summit on business continuity Federal Reserve Bank of New York on 26th February - Meeting Summary', pp.1-7.

Knight, R. F. and Pretty, D. J. (2000) 'The impact of catastrophes on shareholder value', Oxford Executive Research Briefings, Templeton College, Oxford.

Risk Assessment (RA).



Introduction.

A major part of Business Continuity Management is to ensure that the likelihood (frequency and probability) of Mission Critical Business Activities their dependencies and single points of failure being affected by the occurrence of a threat 'event' is adequately and properly managed.

A Business Impact Analysis identifies the organisation Mission Critical Activities their dependencies and single points of failure and the impact (consequences) of their disruption, interruption or loss. It also identifies a minimum level of resources necessary to achieve the organisation's prioritised recovery, overtime, of its Mission Critical Activities their dependencies and single points of failure.

In particular, together with the Business Impact Analysis, a Risk Assessment provides information to enable the business to determine its risk appetite.

Within the United Kingdom a key aspect of risk assessment and its control is clearly defined in 'The Combined Code for Directors' published by the Institute of Chartered Accountants of England and Wales.

Purpose.

The Purpose of a risk assessment is to identify:

- The internal and external threats, liabilities and exposure, including risk concentrations, that could cause the disruption, interruption or loss to an organisation's Mission Critical Activities.
- The likelihood (probability or frequency) of a threat occurring.
- How vulnerable an organisation is to the various types of threat and enables their prioritisation and control management.
- A basis to establish a risk appetite and risk management control programme and action plan.

Outcomes.

The outcomes from a Risk Assessment include the identification and documentation of:

- The vulnerability and exposure (likelihood of occurrence) of the organisation to specific types of threat.
- Risk concentration(s) e.g. where a number of Mission Critical Activities are located within the same building or on the same site.
- A risk assessment and analysis (combined with a Business Impact Analysis) to inform and enable the setting of a risk appetite.
- A risk control management strategy and action plan.
- The prioritised focus of BCM and risk controls

Components.

The components of a risk assessment and analysis include:

- **Identify risks:**
 - When the Business Impact Analysis has been completed it is important to identify the various threats and sources of threats to Mission Critical Activities and includes dependencies and single points of failure.
- **Analyse/Evaluate risks:**
 - To ascertain the significance of each threat it is important to establish the relationship between the likelihood (frequency or probability) and the business impact (consequence and level/size) of a threat occurring. This enables each type of threat to be plotted on an impact/likelihood Mission Critical Activity quartile matrix to identify its priority.
 - The business impact is determined during the Business Impact Analysis.
 - The likelihood (score rating) of each threat occurring is assessed on a probability or frequency scale. The rating indicates the likelihood of the threat occurring.
 - The assessed 'likelihood' ratings are entered for each threat against each Mission Critical Activity.
 - Historical information of past events may provide useful in assessing the potential likelihood of a threat occurring.

- **Control and management of risks:**
 - The decision how to control/manage the threat is made by considering the likelihood of its occurrence, the impact and the cost of controls/management.
 - The options to control and manage the risk include:
 - Avoid the risk
 - Accept the risk (where it cannot otherwise be cost-effectively managed)
 - Reduce (control) the risk
 - Transfer the risk (except reputation, market share and shareholder value)

Methodologies/Techniques.

The methods, tools and techniques to provide a Risk Assessment include:

- Probabilistic Risk Assessment:
 - Event Tree Analysis
 - Fault Tree Analysis
- Current state assessment 'Gap' analysis:
 - Questionnaire(s)
 - Scorecards
 - Interviews (structured or unstructured).
- Quantified Risk Assessment.
- Risk Analysis/Evaluation.
- Risk Prioritisation Quartile Matrix.
- Scenario Planning.
- Controls
 - Preventative (prevent or reduce likelihood of threat occurring)
 - Corrective (management of the impact once a threat has occurred).
- Cost Benefit Analysis.

Process.

The key constructs and stages of a Risk Assessment include:

- Determine the Threats to Mission Critical Activities.
- Determine the likelihood (probability or frequency) of the threat(s) occurring.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Identify the vulnerability of the organisation via a scoring mechanism.
- Prioritise (ranking) of types of risk in a quartile matrix.
- Produce a combined Business Impact Analysis and Risk Assessment report for the assessment sponsor to identify the key focus for BCM and risk management control(s).
- Obtain organisation sponsor’s approval and sign-off of risk priorities (rankings) and risk appetite (ideally the risk appetite should be agreed before impact and risk controls are costed).
- Review (‘Gap’ analysis) existing risk management control strategies (where the assessed risk level remains unacceptable, notwithstanding existing (or planned) controls, it is incumbent on management to design new controls or to consider other options.
- The acronym ‘TARA’ can be used as a guide to consider appropriate strategies arising from the results of the Risk Assessment:
 - Transfer the risk e.g. through insurance
 - Accept the risk e.g. where low impact/ probability
 - Reduce the risk e.g. through the introduction of further controls.
 - Avoid the risk e.g. by removing the cause or source of the threat.
- Provide a costed (cost benefit analysis) impact and risk control report for business sponsor based on the defined risk appetite.
- Obtain organisation sponsor’s approval and sign-off of BCM and risk management control(s).

A Threat Vulnerability Matrix.

TYPE OF THREAT	LIKELIHOOD OF OCCURRENCE (PROBABILITY OR FREQUENCY)		
	High Weekly or < than	Medium Monthly	Low Annually or > than
Fire			
Power outage			
Flood			
Bomb			
Lost Data			
Telecom’s outage			
IT failure			
Terrorist Attack			
Industrial Action			

Frequency and Triggers.

The frequency that a Risk Assessment should be carried out or reviewed is dependent upon the nature, scale and complexity of the organisation based on its business risk profile,

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

appetite and the environment in which it operates. Good practice indicates a Risk Assessment should be carried out at least every 12 months unless:

- It is an initial Risk Assessment.
- The pace of business change is particularly aggressive.
- The initial outsourcing or intra-organisation sourcing of a Mission Critical Activity or dependency.
- A significant change in the key technology and/or telecommunications including systems and/or networks.
- There is a major business change that may include:
 - Business strategy or objectives.
 - BCM strategy and/or scope.
 - BCM solutions.
 - Location.
 - Large scale change in staff numbers, locations or office densities.
 - Key suppliers (intra-organisation and/or outsourced providers)
 - Post BCM event.
 - Process re-design.
 - New business line or product or service.
 - Merger.
 - Acquisition.
 - Significant change in the regulatory environment.

Participants.

The following roles or functions (not restrictive or exhaustive) are identified as being either Responsible or Accountable or should be either Consulted or Informed (RACI) as a part of the Risk Assessment. The matrix process provides a process that can be used to indicate/identify the specific roles, functions and/or area of the organisation within each of the RACI categories.

Role or Function	R	A	C	I
	Responsible	Accountable	Consulted	Informed
Executive Senior Business Management (Risk Appetite)				
Operational Supervisors and staff				
Change Management				
Professional BCM practitioner				
Project Managers				
Organisation operational risk management staff				
Subject Experts (where appropriate)				

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Suppliers (intra-organisation and/or outsourced providers)				
--	--	--	--	--

Deliverable(s)

The deliverables of a Risk Assessment include:

- A clearly defined and documented matrix of risk types.
- A combined Business Impact Analysis and Risk Assessment quadrant ranking matrix identifying the prioritised focus of BCM and risk controls.
- A clearly defined and documented Risk Assessment and analysis report identifying the risk priorities (rankings) that is approved and 'signed-off' by the organisation sponsor.
- A clearly defined and documented risk management control strategy and action plan approved and 'signed-off' by the organisation sponsor.
- A clearly defined and documented organisation risk appetite including residual risk acceptance that is approved and 'signed-off' by the organisation sponsor.

Good Practice Evaluation Criteria.

The Good Practice evaluation criteria of a Risk Assessment includes:

- Does the organisation have clearly defined and documented Risk Assessment Policy?
- Is the organisation's business risk appetite set and 'signed-off' by the organisation's senior business management?
- Does the organisation set and 'sign-off' its business risk appetite before it considers its BCM Strategy and solutions?
- Does the organisation have a clearly defined and documented standard methodology to carry out a risk assessment?
- Does the organisation have a clearly defined and documented standard assessment impact/criticality criteria to carry out a risk assessment?
- Have the organisation's risk assessment methodology, tools, techniques and criteria been fully evaluated and 'signed-off' as fit-for-purpose?
- Does the organisation have a clearly defined and documented process to ensure the approved risk methodology, tools, techniques and criteria are consistently applied?
- Are the organisation's staff fully trained in the use and application of the risk assessment methodology, tools, techniques and criteria?

- Does the organisation have a clearly defined and documented matrix of risk types?
- Does the organisation have combined Business Impact Analysis and Risk Assessment quadrant ranking matrix identifying the prioritised focus of BCM and risk controls?
- Does the organisation have a clearly defined and documented Risk Assessment and analysis report identifying the risk priorities (rankings) that is approved and 'signed-off' by the organisation sponsor?
- Does the organisation have a clearly defined and documented risk management control strategy and action plan approved and 'signed-off' by the organisation sponsor?
- Does the organisation have a clearly defined and documented organisation risk appetite including residual risk acceptance that is approved and 'signed-off' by the organisation sponsor?
- Has a risk assessment been completed within the last 12 months in respect of the organisation's Mission Critical Activities and their dependencies?
- Has the completed risk assessment (completed within the last 12 months) been agreed and 'signed-off' by the business manager/owner of the Mission Critical Activity or dependency(ies) as up-to-date and fit-for-purpose?
- Have the risks (threats, liabilities, vulnerabilities and exposures) identified by the risk assessment) completed within the last 12 months) in respect of the organisation's Mission Critical Activities and their dependencies been identified, documented and classified within a risk portfolio in terms of their relevance to the organisation?
- Are all business impacts and types of risks associated with any business service, product, system or process formally accepted and 'signed-off' by the business owner i.e. risk always stays within the business?
- Has a security (physical, people, sourcing and IT) audit been carried out, within the last 12 months, to specifically address security related risk and issues e.g. kidnapping, hacking, fraud, virus attack?
- Has the completed security (physical, people, sourcing and IT) risk assessment (completed within the last 12 months) been documented, agreed and 'signed-off' by the business manager as up-to-date and fit-for-purpose?
- Have the counter-measures to the possible security threats, vulnerabilities and exposures been identified, documented and implemented?
- Does the organisation have a process to challenge and review the risk assessment as a part of a periodic updating of risk?
- Has the organisation identified its plausible threats, vulnerabilities, liabilities and/or exposures from both internal and external sources?

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

- Has the organisation carried out a risk assessment and analysis of plausible threats, vulnerabilities, liabilities and/or exposures from both internal and external sources?
- Has the organisation identified its systemic risks?
- Has the organisation identified high risk concentrations e.g. one building/site with several Mission Critical Activities?
- Does the organisation use external expertise, in carrying out a risk assessment, where appropriate and necessary?
- Does the organisation have a clearly defined and documented process in place to track the type and frequency of BCM events and experience (lessons learned) internally and externally?
- Does the organisation have an integrated, clearly defined and documented process of credible information gathering and sources concerning issues of risk?
- Has the organisation introduced risk management controls (an action plan) to eliminate, mitigate, reduce, transfer against the effects of identified key threats, vulnerabilities, exposures and/or liabilities to Mission Critical Activities and their dependencies?
- Is there clear evidence that risk transfer strategies have been considered, evaluated and reference made to insurance policies and coverage?
- Has a cost benefit analysis been undertaken in respect of the risk controls in relation to identified threats, vulnerabilities, liabilities and/or exposures?
- Where risk and/or residual risk is to be 'accepted' is that decision clearly agreed, documented and 'signed-off' by the senior business management of the organisation?
- Does the organisation's overall risk 'picture' indicate a lack of BCM understanding?
- Does the organisation use the BCI BCM Good Practice Guidelines as a part of its BCM Risk Assessment assurance process?
- Does the Risk Assessment (RA) process achieve the RA outcomes set out in the Business Continuity Institute BCM Good Practice Guidelines?
- Does the Risk Assessment process provide the RA deliverables set out in the Business Continuity Institute BCM Good Practice Guidelines?

Further Reading.

AIRMIC (1999) 'A guide to integrated risk management', London.

Birch, D. (2002) 'Business Continuity Management for telecommunications', *Continuity*, Vol.6, No.1, pp.10-13.

Bland, M. (2001) 'Turnbull: Spot the omission', *Continuity*, Vol.5, No.2, pp.6-7.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Business Continuity Institute, (1999) 'Benchmarking Business Continuity Management' Business Continuity Institute, Worcester.

Business Continuity Institute, (2000) 'The ten competencies of Business Continuity Management' Business Continuity Institute, Worcester.

Business Continuity Institute, (2001) 'Getting Started' Business Continuity Institute, Worcester.

Central Computer and Telecommunications Agency, (1995) 'An introduction to Business Continuity Management', HMSO, London. ISBN 0-11-330669-5.

Chadwick, T. (2001) 'Setting the scene: e-Business Continuity Management issues', Continuity, Vol.5, No.4, pp.7-9.

Charters, I. (1998) 'Is risk management relevant to the Business Continuity Manager?', Continuity, Vol.2, No.4, p.15.

Charters, I. (2000) 'The reality of worst case scenarios', Continuity, Vol.4, Issue.4, pp.7-8.

Chase, R. (1999) 'Brands and intellectual property', Continuity, Vol.3, Issue.4, pp.12-14.

Crockford, N. (1986) 'An introduction to Risk Management', Woodhead-Faulkner, Cambridge. ISBN 0-85941-332-2.

Dykes, L. (2001) 'Business interruption insurance and Business Continuity Management', Continuity, Vol.5, No.3, pp.10-11.

Elliott, D., Swartz, E., Herbane, B. (1999) 'Business Continuity Management: Preparing for the worst', Income Data Services, London. ISBN 0-905525-56-6.

European Security Forum. (1997) 'SPRINT user guide: Risk analysis for information systems', European Security Forum, London.

European Security Forum. (1997) 'SPRINT directory of controls: Risk analysis for information systems', European Security Forum, London.

Federal Reserve Bank. (2002) 'Summary of lessons learned and implications for Business Continuity Management', Federal Reserve Bank, New York, pp.1-10.

Federal Reserve Bank. (2002) 'Implications of 9/11 for the financial services sector', Bank of International Settlement Review, pp.1-5.

Fenn, D. (2002) 'Supplier Continuity: Managing risks across the supply chain', Continuity, Vol.6, No.1, pp.4-6.

Financial Services Authority. (2001) 'A risk focused review of outsourcing in the UK retail banking sector', Financial Services Authority, London, pp.1-19.

Financial Services Authority. (2002) 'A Business Continuity Management risk matrix', Financial Services Authority, London, pp.1-20.

BUSINESS CONTINUITY MANAGEMENT - GOOD PRACTICE GUIDE

Financial Services Authority. (2002) 'FSA working paper on Business Continuity Management', Financial Services Authority, London, pp.1-19.

Fink, S. (1986) 'Crisis Management: Planning for the inevitable', Amacom, New York. ISBN 0-8144-5859-9.

Home Office. (1996) 'How resilient is your business to disaster', HMSO, London.

Home Office. (1999) 'Bombs: Protecting People and Property', (4th Edition), HMSO, London.

Home Office. (2001) 'Business as usual: Maximising business resilience to terrorist bombings', HMSO, London.

Institute of Chartered Accountants in England and Wales (1991) 'Internal Control: Guidance for directors on the Combined Code', Accountancy Books, London.

Kaye, D. (1999) 'Insurance and Business Continuity Management', Continuity, Vol.3, No.4, pp.14-15.

Kaye, D. The Chartered Institute of Insurance: Risk Management Study Course 655', Chartered Institute of Insurance, London. ISBN 1853692751.

Kirvan, P.F. (2000) 'Business Continuity Strategies for call centres', Continuity, Vol.4, No.2, pp.9-10.

Lack, K. (2000) 'Turnbull and e-commerce could put the board in turmoil', Insight on risk, Vol.3, No.1, pp.2-3.

Meredith, B. (1998) 'Business Impact Analysis', Continuity, Vol.2, Issue.1, pp.4-77.

Newton, J. and Pattison, R. (1998) 'The business implications of wide spread disasters', Continuity, Vol.2, No.2, pp.5-8.

Mitroff, I.I. and Pearson, C.M. (1993) 'Crisis Management: A diagnostic guide for improving your organisations crisis preparedness', Jossey-Bass, San Francisco. ISBN 1-55542-563-1.

Nussey, C., Carter, C.A. and Cassidy, K. (1995) 'The application of consequence models in risk assessment: A regulator's view', Health and Safety Executive, Merseyside, pp.1-24.

Power, P. (1999) 'Business Continuity Management: Preventing chaos in a disaster', Department of Trade and Industry, London.

Rassam, C. (1999) 'A matter of control', Survive, February Issue, pp.58-59.

Smallman, C. (1996) 'Risk and organisational behaviour', Disaster Prevention Management, Vol.5, No.2, pp.12-26.

Smith, D. (1990) 'Beyond contingency planning: Towards a model of crisis management', Industrial Crisis Quarterly, Vol.4, No.4, pp.263-275.

Tehrani, N. (1999) 'Dealing with disasters: The people issues', Continuity, Vol.3, No.3, pp.10-11.

Vogt, K. (1998) 'Business continuity and total risk management', *Continuity*, Vol.2, Issue.4, pp.11-14.

Westmacott, P. (2001) 'Contingency Planning: Contractual Issues', *Continuity*, Vol.5, No.1, pp.6-7.

Video.

British Broadcasting Corporation (2002) 'Disaster 1; Spiral To Disaster', BBC Worldwide Limited, London.

British Broadcasting Corporation (2002) 'Disaster 2: A Major Malfunction', BBC Worldwide Limited, London.

Business Continuity Institute (2001) 'Back to Business: Planning ahead for the unexpected', Merlin Communications Ltd, Cirencester, Gloucestershire.

Case Studies.

Ckonjevic, M. (2001) 'The Californian power crisis', *Continuity*, Vol.5, Issue. 2, pp.8-9.

Dombrick, J. (2001) 'British Airways: A business continuity plan in practice', *Risk Management*, Vol.6, Issue.1, pp.5-8.

Federal Reserve Bank (2002) 'Summary of lessons learned and implications for business continuity', pp.1-10.

Honour, D. (2001) 'Heeding the lessons of 9/11', *International Journal of Business Continuity Management*, Vol.2, Issue,1, pp.13-17.

Sipika, C. and Smith, D. (1993) 'From disaster to crisis: The failed turnaround of Pan American Airlines' *Journal of Contingencies and Crisis Management*, Vol.1, No.3, pp.138-151.