Business Continuity Management (BCM)

Socrates Coudounaris
Certified IRM Fellow
Contents

• Why have BCM
• Establishing a BCM Programme
• Understanding the organisation
• Business Impact Analysis (BIA)
• Risk Assessment (RA)
• Determining BCM strategies
• Developing and implementing a BCM response
• Exercising and Maintaining
• Conclusion
Effective business continuity understands how environmental factors affect an organisation’s profile and its breadth of operations.

Moreover, it assesses each external factor against the internal goals and objectives of the organisation.
The Benefits of BCM

• Provides a structured approach to Business Continuity activities
• Demonstrates to all stakeholders (both internal and external) capability to manage disruptive events
• Enhances competitive advantage
• Improves maintenance of existing contracts
• Protects organisation as a whole
Key Elements of BCM

- BCM is based on a ‘lifecycle’ – it is a continuous process
- Forms part of Enterprise Risk umbrella and organisational culture
- Based on impacts – not just the threats themselves
- It is as much about prevention as about recovery
- Must be proven by exercises and lessons learnt
- Must be maintained in a changing and challenging environment
- Work with an established framework and customise to your needs

There is no need to reinvent the wheel!
The BCM Continuous Lifecycle Approach to Improvement

ISO22301
ISO22301 Business Continuity Programme Elements

- Business Continuity Programme Management
- Embedding Competence and Awareness
- Understanding The Organization
- Selecting Business Continuity Options
- Developing and Implementing a Business Continuity Response
- Exercising and Testing

Embedding Competence and Awareness

- Understanding the Organization
- Exercising and Testing
- Selecting Business Continuity Options
- Developing and Implementing a Business Continuity Response
Stage 1
Establishing a Business Continuity Programme Management
Stage 1 – Establishing a BCM programme

The BCM Programme includes the development and management of policies and procedures in order to protect:

People,

Processes, and

Supporting technology.
Determine BCM Scope

Factors that influence BCM scope include:

- Size and complexity of organisation's operations
- Stakeholder needs
- Type of activities performed
- Environment and location of operations
- Organisation’s business objectives
An effective BCM programme should have the following in place:

- BCM Policy statement
- Ongoing support from the top of the organisation
- BCM structure – roles & responsibilities clearly defined
- Adequate resources in order to deliver BCM
- Effective management and control of documentation and records
- An overall assurance process
Embedding BCM

Train the appropriate staff
Raise awareness
Articulate why BCM is being introduced
Explain what is being done and by when
 Demonstrate benefits to everyone
Inform all stakeholders
Reinforce ongoing support from Executive team
Communicate, Communicate, Communicate ....
Stage 2
Understanding the Organisation
Firstly, identify all key products and services,

Secondly, define the time criticality of all activities that support the above.
Understanding the business

What are the key services and products?

Which are the critical activities?

What processes are being used in order to deliver those critical activities?
Understanding the business

Who and what is used in these processes?
Consider both internally & externally

What is the impact if key services & products are disrupted – for whatever reason:
Carry out a Business Impact Analysis and a Risk Assessment
Key Services and Products

Not all services and products are critical

Some services and products are seasonal

Criticality is determined by drivers and stakeholders

The impact on the organisation if the service is disrupted will influence the criticality

Group’s risk appetite will affect criticality

Criticality ratings must be ‘signed off’ by top management
Carrying out a Business Impact Analysis (BIA)
What is a Business Impact Analysis (BIA)

The BIA is that process of determining the **Financial Impact** and **Operational Impact** on critical organisational activities, in order to assign recovery objectives.

Identifies, quantifies and qualifies the business impact of a loss, interruption or disruption of business processes.

The BIA results provide data from which the appropriate continuity strategies will be determined.
How to conduct a BIA – Step 1

List key services which, if disrupted for whatever reason, will have the greatest impact on the organisation

For each service identified, consider the impact of a disruption in terms of ability to meet business aims and objectives, as well as impact on stakeholders

Document what the impact would be for example:

- The first 24 hours
- 24 – 72 hours
- Up to one week
- Up to two weeks
Maximum Acceptable Outage (MAO)

Identify the maximum length of time that you can manage a disruption to each of our key services without threatening viability, either financially or through a loss of reputation
How to conduct a BIA – Step 3

Recovery Time Objective (RTO)

Set that point in time at which each of the key services would need to be resumed in the event of a disruption.

In determining the RTO:

- take into account the confidence you have in the MAO and whether on reflection it was too optimistic;
- ensure that you have built in a margin for unforeseen difficulties with recovery.
How to conduct a BIA – Step 4

Document the critical activities that are required to deliver the key services for each department

Quantify the resources required over time to maintain the critical activities at an acceptable level and to meet the RTO already identified

These may include:

- people
- premises
- technology, information
- supplies and partners
Maximum Acceptable Outage (MAO)

MAO is the maximum amount of time that the organisation’s key products or services can be unavailable or undeliverable before its stakeholders realise unacceptable consequences (i.e. the point beyond repair)

Recovery Time Objective (RTO)

RTO is the point in time following a disruption when operations must resume (at a minimum level) in order to meet downtime tolerances.
Setting the RTO

RTO > month (Leave any decisions until after that event)

RTO > 1/2 days (Allows time for staff to be relocated to another site)

RTO < 1 day (Requires tactics that enable the activity to be taken on by staff at other locations – this implies the immediate availability of the resources required by that activity at other site including current information)

Once the RTO parameter has been satisfied, cost and availability will guide the choice of tactics.
Risk Assessment (RA)

Following the BIA, performing a Risk Assessment will identify single points of failure:

- People
- Information technology
- Premises
- Plant & machinery
- Suppliers
Not just a one-time project because of constant business changes, revise your Business Continuity Plans

Identify critical business activities that need to be recovered in order to ensure organisational survival

Identify the timescales these activities need to be resumed within
Identify basic business resources required in order to maintain the minimum acceptable level of operation for the business.

Identify dependence of the business on IT systems and applications.

Identify key internal and external dependencies.

Identify potential threats to the business and options to deal with those threats.
Stage 3
Selecting BCM Options
Determining BCM Strategy

The aim is to:

Ensure and protect the ability of the organisation to keep on delivering its services

What can the organisation do if some of its key services are disrupted?
BCM Strategy Options

Approach to determining a BCM Strategy include the following:

Implement appropriate measures to reduce likelihood of incidents occurring and/or reduce their impact if they do e.g. Health & Safety

Provide continuity for key services and supporting activities during and following an incident

Take account of those services and their supporting activities that have not been identified as critical
BCM Strategy

Take the following into account:

- People
- Premises
- Technology
- Information
- Supplies
- Stakeholders
BCM Strategy

Consider 4 high level scenarios and what alternative working arrangements could be made if:

- Cannot gain access to office
- A high percentage of the staff are unavailable
- Systems are unavailable
- A key supplier/partner is disrupted
BCM Strategy must:

Recognise **critical functions**,

Recognise **dependencies**

Recognise **single points of failure**

Enable the organisation to perform critical activities

Allow decisions to be taken by responsible managers

Signed off by senior management
Stage 4
Developing & Implementing a BCM Response
Plan Invocation

Establish procedures for how the Business Continuity Plans will be invoked

• Identify the person(s) who determines whether a disruption has occurred
• Specify the procedure to be used
• Specify who should be consulted
• Specify who should be informed
Invocation Teams

LEVEL 1
STRATEGIC
(GOLD)

LEVEL 2
TACTICAL
(SILVER)

LEVEL 3
OPERATIONAL
(BRONZE)

THINK

PLAN

DO
Communications Management

- Regularly update senior management
- Keep customers informed
- Mechanisms to inform employees
- Keep other stakeholders informed
- Ensure media are briefed
Incident Response Structure

The incident response structure must enable personnel to:

- be capable of confirming the nature and extent of the incident, and
- manage the incident

- be responsible for triggering an appropriate business continuity response
Incident Response Structure

The incident response structure must enable personnel to:

- have access to plans, processes and procedures to manage an incident;

- have plans for the activation, operation, coordination and communication of the incident response;

- have resources available to support the plans, processes and procedures to manage the incident.
Business Continuity Management

- Managing Risk
- Emergency Management
- IT Disaster Recovery
- Facilities Management
- Supply Chain Management
- Operations
- Environmental Management
- Health & Safety
- Knowledge Management
- Human Resources
- Security
- Crisis Communications & PR
Developing Business Continuity Plans

- Keep them simple
- Ensure that you can use them during a disruption
- Identify what resources are needed
- Make plans owned by operational units
- Exercised, audited and reviewed
- Version and distribution controlled
- Accessible
Stage 5
Exercising - Maintaining - Reviewing Plans
Exercising the plans

Consider the following:

- Risk, impacts and capabilities
- Types of exercise to be used
- Involvement of senior management
- Process of delivering exercises
- Relationship between exercising emergency plans and Business Continuity Plans
- Planning exercises which minimise the risk of disruption and the risk of an incident occurring as a direct result of the exercise is minimised
The Exercise Process Requires:

- Senior management commitment
- Planning team
- Risk assessment
- Documentation
- Briefing
- Exercise
- De-brief
- Review of lessons learnt
- Funding
Exercising BCP – the learning cycle

- **Business Continuity Plan**
- **Exercise**
- **Debrief**
- **Post-Exercise Report**
- **‘Lessons Learned’ Report**
- **Review Plan**
- **Implement Changes**
- **Post-Exercise Report**
- **Audit BCP**

- This can be a test of part or the whole of the plan.
- This should be a debrief after each exercise in order to capture the experience of all the participants.
- This post-exercise report should collate the output of all debriefs with the post-exercise analysis of the exercise outcomes.
- Having made changes to the BCP, it is important to review the plan in its entirety before disseminating the ‘current version’.
- Approval and acceptance of recommendations by BCM strategic lead.
- This report closes the exercise programme and outlines the full outcome of the programme. It makes recommendations for changes to the BCP.
- The BCP should be audited regularly and necessary changes identified.
Carrying out an Exercise

Consider the following high level scenarios:
Denial of access or loss of facilities
Loss of key staff/skills
Loss of critical systems, including ICT
Loss of key resources, including suppliers/partners

Capabilities
Mobilisation
Co-ordination
Communications

Warning!
Don’t let the exercise create a disruptive incident
Maintaining a Business Continuity Plan

Regularly review in order to ensure that details are current,

Check facts are correct and if changes are required to instigate amendments,

Re-issue and re-train as appropriate.
Maintain and Review

Nothing stays the same, there is always change

- Organisations
- Regulations and laws
- Customers
- Suppliers
- People
- Contacts
- Technology
- Processes
- Locations

All plans should be reviewed annually and signed off by plan owners and management.
BCM Conclusions

- Clearly Define the Scope
- Establish an effective management system
- Identify critical activities and resources, including critical suppliers and partners
- Risk assessment (effects, not causes; prevention, not just cure)
- Create appropriate incident and continuity plans
- Exercise plans and record results
- Audit BCM and BCMS
- Management of documentation & records
- *Establish a culture of BCM*
Upcoming IRM Courses (London):

MANAGING RISK, LEADING PEOPLE (Half Day):  
HOW TO CONDUCT A HIGH QUALITY RISK ASSESSMENT (Half Day):
CRISIS COMMUNICATION STRATEGY (Half Day):
STRATEGIC AND OPERATIONAL DECISION MAKING (1 Day):
RUNNING EFFECTIVE RISK WORKSHOPS (1 Day):
RISK IN THE BOARDROOM (Half Day):
MANAGING REPUTATIONAL RISK (Half Day):

Email: training@theirm.org  
Web: www.theirm.org  
Tel: 020 7709 4114/4117
Thank you

Socrates Coudounaris BEng (Hons) MSc FCII CIP CFIRM
Risk Management Director, RGA International Reinsurance Company

Email: scoudounaris@rgare.com