

B U S I N E S S

C O N T I N U I T Y

**ENISA FORTH SUMMER SCHOOL
Network and Information Security**

Business Continuity

19 September 2008

Glen Abbot Ltd

Background

- Janet Beattie, Director of Glen Abbot
- MBCI
- Based in Perth, Scotland
- 10 full-time employees, 6 associates
- 10 years old this year!
- Oil, gas, banking, insurance, investment, health, manufacturing, IT, media, tourism, local government, transport

Outline of Presentation

- Explain the work we carried out for ENISA and why it was so important
- Using ENISA's Overview introduce the audience to Business Continuity and its lifecycle
- Describe the various worldwide methods which support BC planning
- Describe the various tools which support BC planning
- Summary
- Q & A



ENISA's Risk Objectives

Enhance the capability of the Community, EU Member States and the business community to prevent, address and respond to network and information security problems, by:

- ✓ Promoting risk assessment and risk management methods
- ➔ Promoting business continuity management for the IT continuity risks faced by critical business units



Objectives of the Report

- Provide solutions to:
 - Missing overview on methods, tools and good practices
 - Absence of a common language
 - Lack of surveys on existing methods, tools and good practices



Why is Business Continuity so Important?

- No system is foolproof
- Even though
 - You have identified your IT and IS risks (e.g. loss of data, system failure, virus attack)
 - You have determined your risk acceptance level
 - You have mitigated the risks which could be treated
 - You have implemented controls (e.g. encryption, intrusion prevention mechanisms, network monitoring)
- And you proactively manage your risks
- You may still end up with an incident....



Business Continuity Management

- The long term effects of an incident will not be so severe if:
 - You already know which parts of the business are critical
 - You already know which components are critical (systems, network, servers etc)
 - You know how to put things back together
 - You have identified who will do what
 - You know when to do everything
 - You have an incident management team who oversee all the recovery work
 - You can manage the media



[Supporting research - Knight and Pretty 1997]



This advance planning is your

Business Continuity Plan!



Glen Abbot Ltd

What Did we Do?

- Wrote a report introducing a methodology for Business Continuity aimed at ICT
- Referred to world wide BCM methods
- Showed the relationship between risk, IT and IS
- Analysed worldwide BCM tools



Audience for the Report

- In particular:
 - Information Technology professionals
 - Information Security professionals
- Overview for:
 - Anyone involved in BCM





A Small Glossary

BCM Business Continuity Management

RM Risk Management

ITSC Information Technology Service Continuity

DR Disaster Recovery

IS Information Security

RPO Recovery Point Objective (data and information)

RTO Recovery Time Objective (processes and components)

EM Emergency Management

CG Corporate Governance

Definitions

- Business Continuity Management (BCM)
 - Availability of processes and resources to ensure continued achievement of critical objectives (HB 293)
- Emergency Planning and Management (EP/EM)
 - Process resulting in a set of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency which impacts the organisation (BS 25999-1)
- Information Technology Service Continuity (ITSC)
 - Supports BCM by ensuring that required IT components can be recovered with required and agreed business timescales (PAS 77)
- Disaster Recovery Planning (DRP)
 - Procedures to restore operability of the target system, application or computer facility (NIST 800-34)

Methods Used

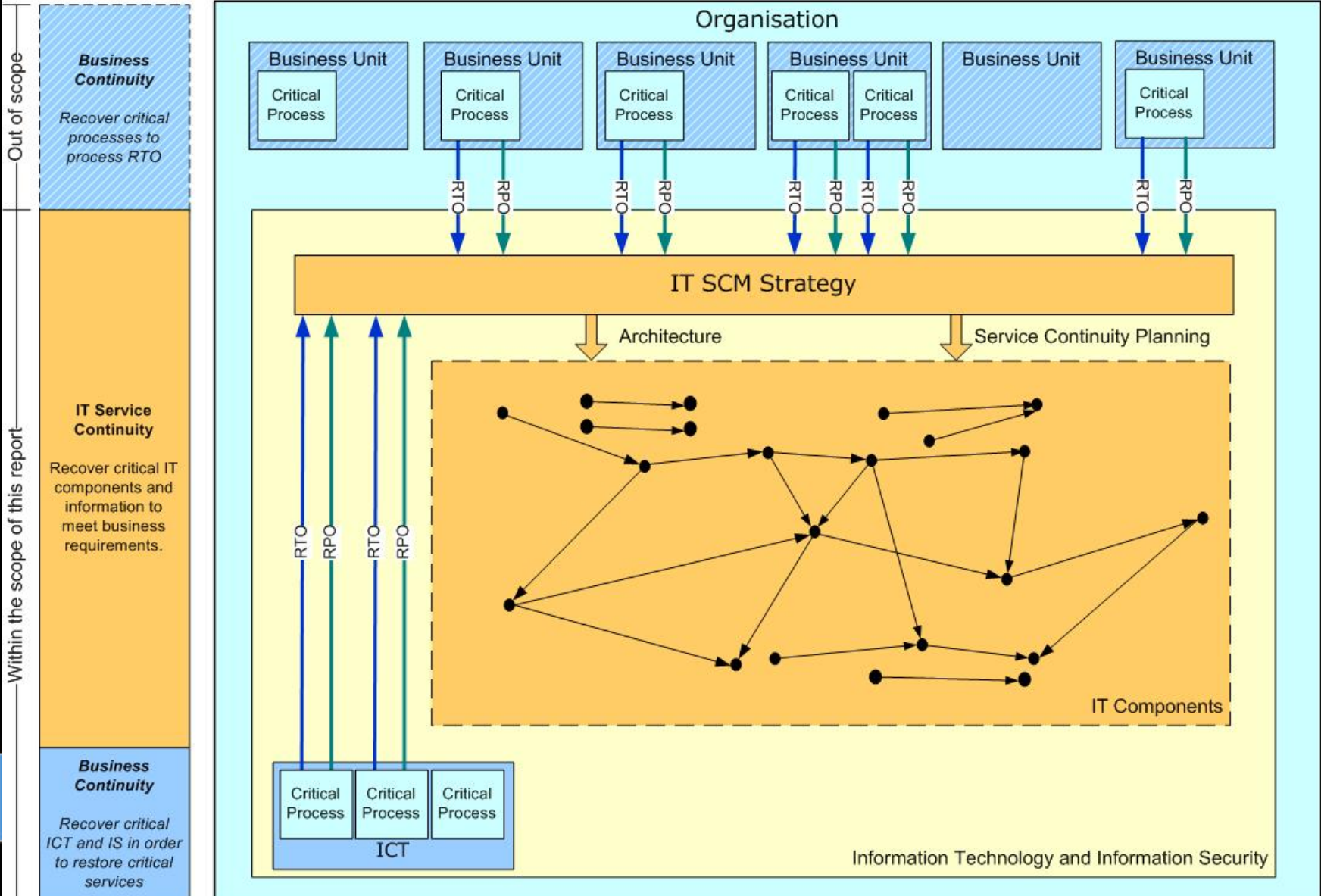
- PAS77/BS 25777 (ITSC - UK)
- NIST 800-34 (ITSC - USA)
- ISO 17799 (IS - International)
- BSI 100-2 (IS - Germany)
- COBIT 4 (IT - USA)
- ITIL 2 & 3 (IT – UK)
- BS ISO IEC 24762 (DR – International)
- BS 25999 (BCM - UK)
- BCI GPG (BCM – UK)
- HB 221 (BCM – Aus & NZ)
- HB 292 (BCM – Aus & NZ)
- HB 293 (BCM – Aus & NZ)
- APS 232 (BCM – Aus & NZ)
- TR 19 (BCM – Singapore)
- NFPA 1600 (EM – USA)
- FEMA 141 (EM – USA)
- ISO PAS 22399 (EM/BCM – International)

Other Methods

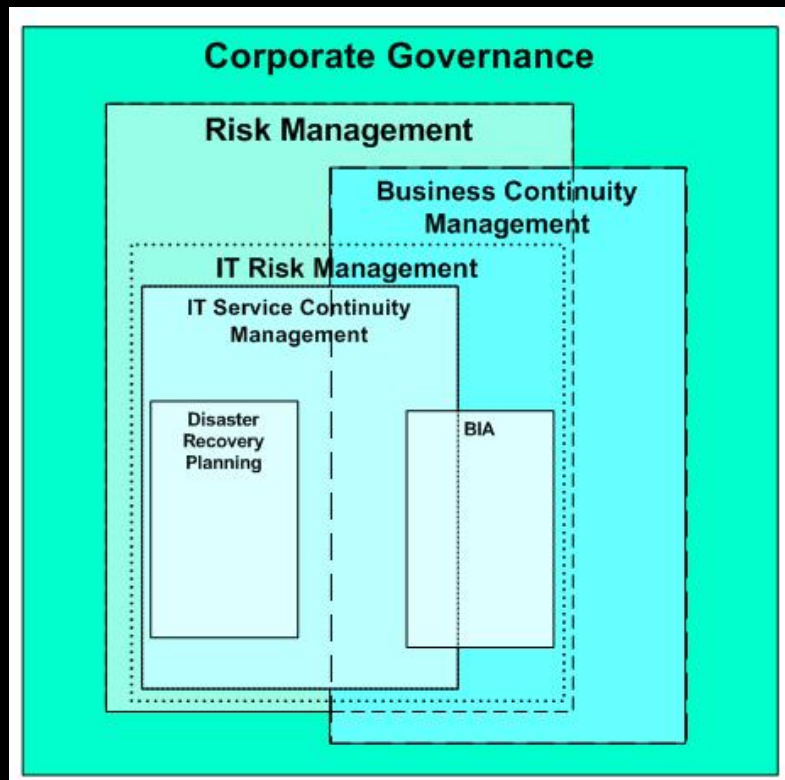
- Use our Glen Abbot Knowledge
 - Experience of writing BC, IT and IS Plans for many years
 - Know how to do it – what works, what doesn't
 - Personal involvement in crises
- Use our contacts
 - BCI
 - ICM, BT
 - Fellow professionals



Scope of the Report



Relationship to Risk Management



- Define frameworks together
- Risk treatments
 - Avoid, share, retain, modify
 - Modify
 - Reactive treatment
 - Lessen impact
 - implement a plan for continuity
 - Proactive treatment
 - BCM Programme highlights further risks
 - Feed back into Risk Assessment
- Impact Analysis
 - Risk and BCM together
 - Prioritise activities
- Resource Requirements
 - Results feed into ITSCM

BCM Overview Modules

Define BCM
Framework

Conduct Business
Impact Analysis

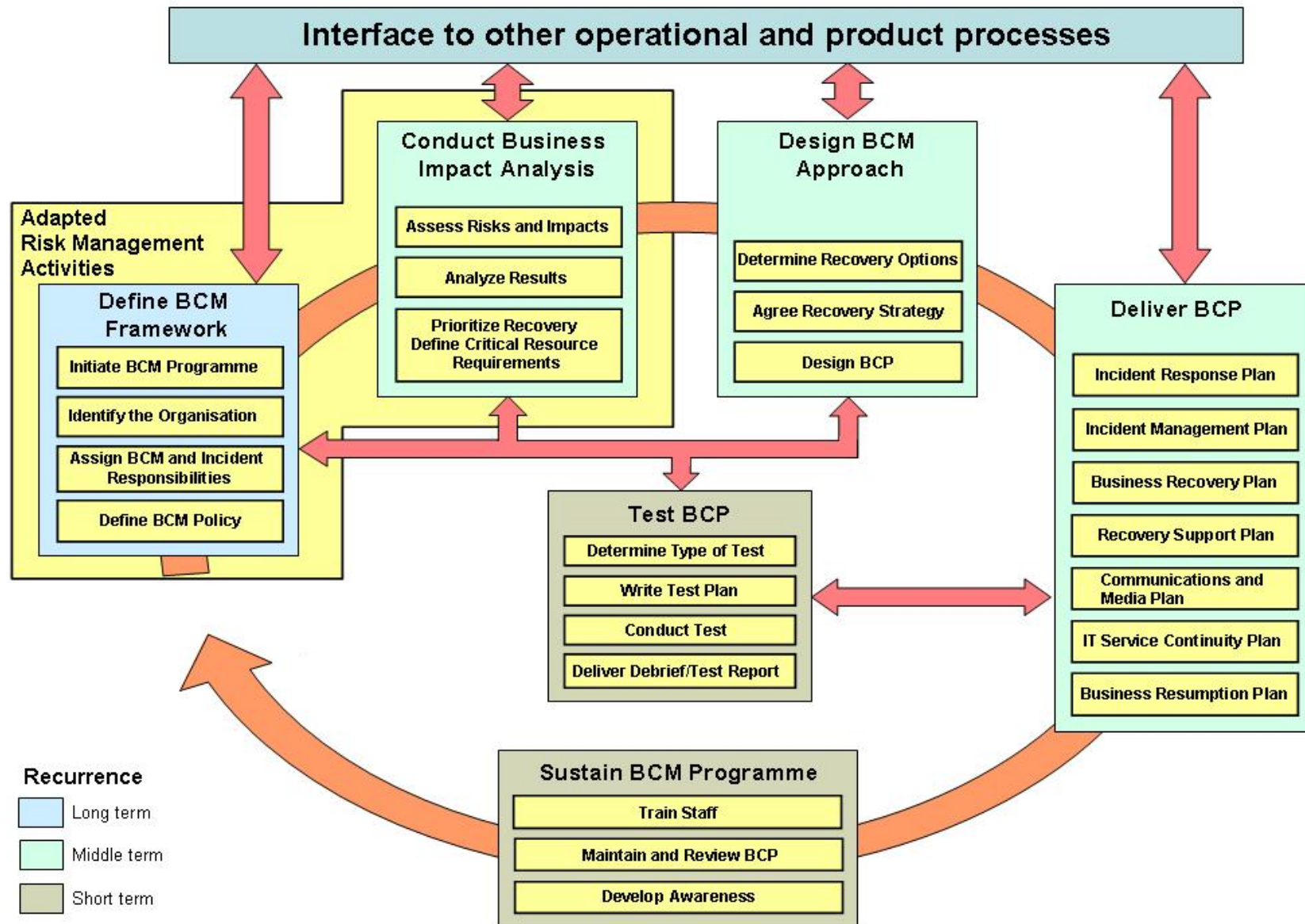
Design BCM
Approach

Deliver BCP

Test BCP

Sustain BCM
Programme

BCM Overview



Define BCM Framework

Define BCM Framework

Initiate BCM Programme

Identify the Organisation

Assign BCM and Incident Responsibilities

Define BCM Policy

- Ongoing management process
- Treat BCM implementation as a project
- Forms basis for rest of programme
- Obtains senior management buy in
- Determines important areas of activity

Conduct Business Impact Analysis

Conduct Business Impact Analysis

Assess Risks and Impacts

Analyze Results

Prioritize Recovery
Define Critical Resource
Requirements

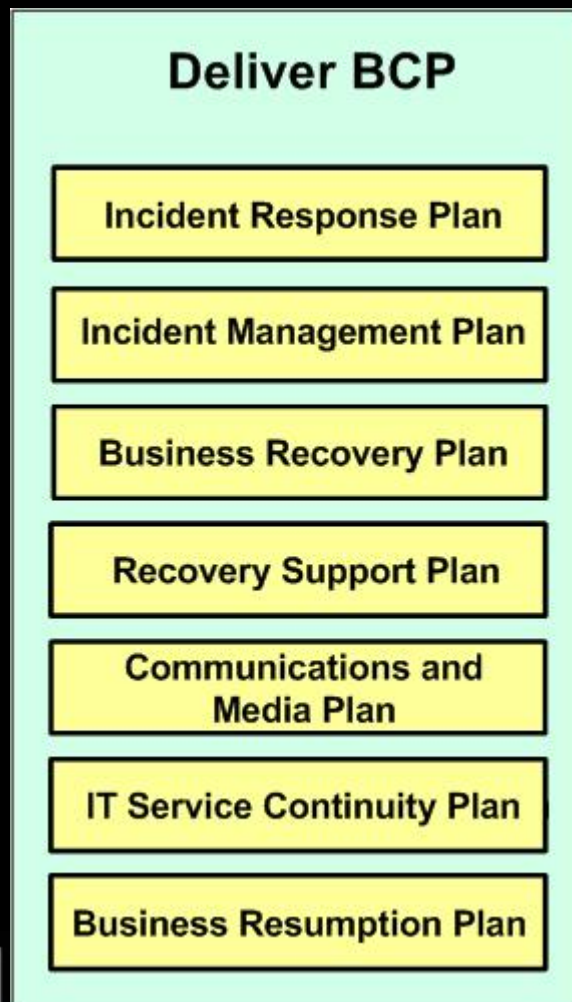
- Foundations for BCP
- Find out what is critical – from the Business Unit
- Prioritise requirements
- Compare with capability
- Forms basis of IT Service Continuity Plan
- Defines the Disaster Recovery Plan

Design BCM Approach



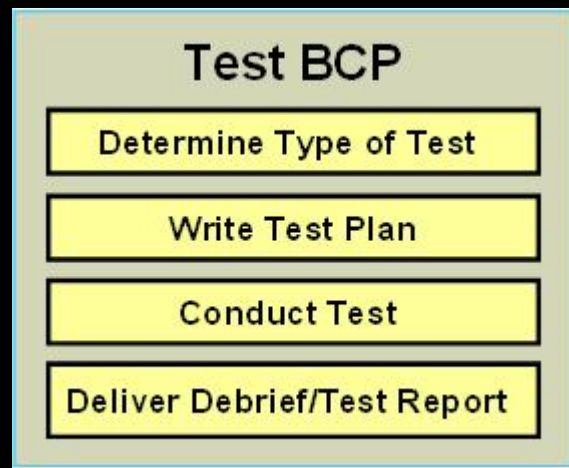
- Options for recovery are developed from the results of the BIA
- Options need to meet BC Objectives (in BCM Policy)
- Strategy developed from appropriate options
- BCP is a suite of documents – decide which are appropriate

Deliver BCP



- Information gathered from previous stages is used to write plans
- Plans written to format agreed in Design BCM Approach
- Each plan serves a different purpose
- Each plan has an owner

Test BCP



- An Organisation's Business Continuity and Incident Management arrangements cannot be considered reliable until tested
- Testing essential to develop teamwork, competence, confidence and knowledge
- Tests should ensure that all members of the recovery teams and other relevant staff are aware of the plans and their roles and responsibilities

Sustain BCM Programme



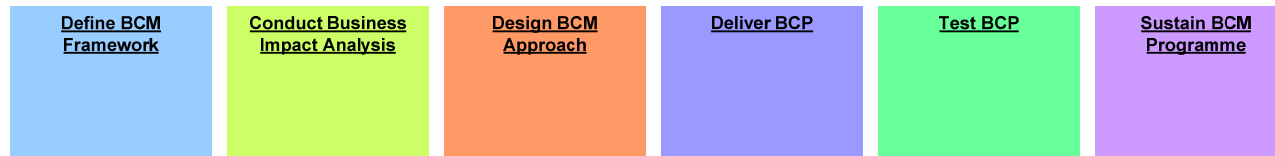
- Training should become part of organisation's training portfolio
- Everyone knows their role instinctively
- Out of date plans are no use
- Cycle of awareness events

The Glossary

- Glossaries on main methods not comprehensive
- Different terminology
 - One term different meanings
 - Many terms same meaning
- Many sources (incl ourselves!)
- Many entries
- Jargon free



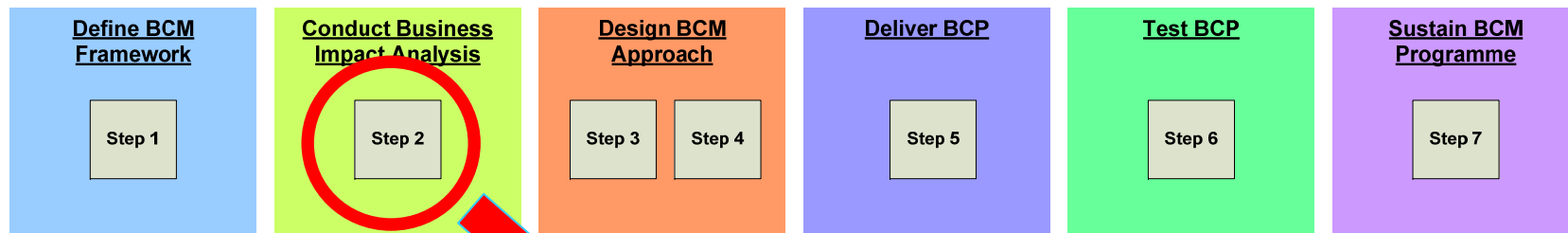
Method Overviews



- Block diagram for each method, relating back to BC Overview
- Description of main elements of the method
- Highlight responsibilities and accountabilities
- Allows user to understand main points of each method without reading whole thing

Method Overview Example

NIST SP 800-34



Step 2 - Conduct the Business Impact Analysis (BIA)



Method Overview Example

NIST 800-34

Description

- **Step 2 - Conduct the Business Impact Analysis (BIA)**
 - Identify critical IT resources.
 - Identify outage impacts and allowable outage times.
 - Develop recovery priorities.



Method Overview Example

Detail

- **Step 2 - Conduct the Business Impact Analysis (BIA)**
 - Responsible:
 - Accountable:
 - Consulted: Contingency Planning Coordinator
 - Inputs:
 - Output: Identification of Critical IT resources; Identification of Impacts and allowable Outage times; Recovery Priorities; BIAs

List of Controls

Corporate Governance

- Need a management system in place for the BCM programme which:
 - Shows progress against deliverables
 - Demonstrates conformance to relevant compliance standards
 - Identifies continuous improvement actions
- Developed a list of controls which if achieved shows that BCM programme has been followed in accordance with Overview process



The Inventories

- Developed a questionnaire type document
 - 16 method inventories already completed and 8 tools inventories
 - Further completion will be possible
- Identified the information which a user would want to know about:
 - The extent to which the Overview modules are covered (rated -, •, ••, •••)
 - What does it cover
 - Use of the method or tool
 - References to Controls
 - Availability of Training/free downloads
 - Costs

Methods Inventory

- **A - Identity Card**

- 1. General information
- 2. Level of reference of the method
- 3. Identification
- 4. Continuity Controls
- 5. Lifecycle
- 6. Useful links
- 7. Languages
- 8. Price

- **B - Scope**

- 1. Target organisations
- 2. Geographical spread
- 3. Level of detail
- 4. License & certification scheme

Methods Inventory

- **C – Users Viewpoint**
 - 1. Skills needed
 - 2. Consultancy support
 - 3. Regulatory compliance
 - 4. Compliance to IT standards
 - 5. Trial before purchase
 - 6. Maturity level
 - 7. Tools supporting method
 - 8. Technical integration of tools
 - 9. Process integration
 - 10. Flexible knowledge database



Methods Inventory

APPLICATION FORM FOR METHODS

A: Product Identity Card

1. General information

Method or tool name	Vendor / Publisher name	Country of origin
BCI Good Practice Guidelines 2008	BCI	UK

2. Level of reference of the product

National Standardisation body	International Standardisation body	Private sector organisation /association	Public / government organisation	White Paper/ Recommendation	Handbook	Guidelines
		✓				✓

3. Identification

Define BCM Framework	Business Impact Analysis	Design BCM Approach	Deliver BCP	Test BCP	Sustain BCM Programme
✓	✓	✓	✓	✓	✓

Coverage of BCM Framework

BCM Framework activities	Included? (-, ●, ●●, ●●●)	Comments
Initiate BCM Programme	●●●	Implementing BC in the Organisation, Project Management, Ongoing BC Management and Documentation cover this area in detail.
Identify the Organisation	●●●	This is well covered in the GPG, under Reflecting Organisational Context and is an area not often covered in other standards. It looks at areas such as aligning BC to the organisational strategy, understanding the business plan, areas of the organisation in scope, new products, process or technology.
Assign BCM and Incident responsibilities	●●	This is described under Assigning Responsibilities (1b.1) and highlights that a member of the Executive should be given overall accountability for the effectiveness of the BCM capability. Detailed responsibilities of each person/team are not described.
Define BCM Policy	●●●	This is comprehensively covered by the sections on BCM Policy Content (1a.2) and BCM Programme Scope and Determining Choices (1a.3). These

Coverage of Sustain BCM Programme

Sustain BCM Programme processes	Included? (-, ●, ●●●)	Comments
Train Staff	●●●	Training and awareness are discussed together under Section 6 (Embedding BCM in the organisation's culture) and the need for staff to have an awareness of BC before being trained in particular aspects is discussed. How to identify the Training Gap is presented and how this will drive the awareness campaign. Suggested training resources are presented. A Skills Matrix is given in the Appendix.
Maintain and Review BCP	●●●	The importance of maintaining the BCP is stressed and the need for any changes to go through change control. The need for a maintenance schedule is introduced and the need to get the Maintenance Report and Maintenance Report Action Plan signed off by a senior manager.
Develop Awareness	●●●	Awareness is discussed together with training and based on the results from the Training Gap analysis, the various ways in which awareness can be raised is introduced. A section on monitoring cultural change is presented where the way in which the effectiveness of awareness campaigns and training courses are measured.

Brief description of the product:

The BCI Good Practice Guidelines 2008 are designed to complement BS 25999 (parts 1 and 2), although some sections do not go into as much detail as BS 25999-1 e.g. BCM Strategy. It provides reasons why planning activities should be carried out and ways in which they may be achieved. Each section is similarly presented with an Introduction, Precursors, Purpose, Concepts and Assumptions, Process, Methods and Techniques, Outcomes and Deliverables and Review. In some sections it lacks the detail of previous versions leaving more room for interpretation by the user

4. Continuity Controls

Controls implemented by using this method

Control Reference	Location of Reference to Control
BCMFI01	Section 1b.3
BCMFI02	Section 1b.3
BCMFI03	Section 1b.3
BCMFO01	Section 1a.3
BCMFO02	Section 1a.1
BCMFRR01	Section 1b.1, 1b.4
BCMFP01	Section 1a.2, 1a.3
BIA01	Section 1a.3, 2.3,
BIA03	Section 2.1

Methods Reviewed (Recap)

- PAS77/BS 25777 (ITSC - UK)
- NIST 800-34 (ITSC - USA)
- ISO 17799 (IS - International)
- BSI 100-2 (IS - Germany)
- COBIT 4 (IT - USA)
- ITIL 2 & 3 (IT – UK)
- BS ISO IEC 24762 (DR – International)
- BS 25999 (BCM - UK)
- BCI GPG (BCM – UK)
- HB 221 (BCM – Aus & NZ)
- HB 292 (BCM – Aus & NZ)
- HB 293 (BCM – Aus & NZ)
- APS 232 (BCM – Aus & NZ)
- TR 19 (BCM – Singapore)
- NFPA 1600 (EM – USA)
- FEMA 141 (EM – USA)
- ISO PAS 22399 (EM/BCM – International)

Summary of the Methods

- Each method has a slightly different focus
 - HB 292 - full BCM lifecycle & lots of templates
 - FEMA 141 - BCM with an emergency planning focus. Very detailed section on incident management
 - NIST 800-34 - IT Service Continuity focus. Good section on BIA. Describes strategies for maintenance of IT availability
- All use different terminology – quite confusing
- Need to read a good cross section to understand BCM and related disciplines
- Make up your own mind!

Tools Inventory

- **A - Identity Card**
 - 1. General information
 - 2. Level of reference of the tool
 - 3. Brief description of the product
 - 4. Supported functionality
 - 5. Lifecycle
 - 6. Useful links
 - 7. Languages
 - 8. Pricing and Licensing
 - 9. Trial before Purchase
 - 10. Tool Architecture



Inventory Example - Tools

- **B - Scope**

- 1. Target organisations
- 2. Spread
- 3. Level of detail
- 4. Compliance to IT Standards
- 5. Tool helps towards certification
- 6. Training

- **C – Users Viewpoint**

- 1. Skills needed
- 2. Tools support
- 3. Organisation Processes Integration
- 4. Interoperability with other Tools
- 5. Sector adapted knowledge databases supported
- 6. Flexibility of Tools database

Tools Inventory

APPLICATION FORM FOR TOOLS

A: Identity Card

1. General information

Tool name	Vendor name	Country of origin
Paragon	Sungard Availability Services	USA

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European Directive)	Local
Yes			
Has the development of the tool been sponsored by a professional or trade association?		No	

3. Brief description of the product

Paragon is a modular business continuity planning tool employing a central database of information which can be shared across all modules.

4. Solution Focus

What business continuity planning activities does the tool support? Does it provide support for a specific aspect of Business Continuity Planning or is it designed as a "full lifecycle" tool covering the following activities

Define BCM Framework	Tools which support the definition of scope, objectives and deliverables of the BCM project, identifying the key business areas and gathering key information of risks and tolerances to exposure.	Supported
Conduct Business Impact Analysis	Provide support for activities related to Risk analysis, dependency-modeling techniques, establishing recovery requirements and targets for both critical business enablers (such as information technology systems and infrastructure) and business activities	Supported
Design BCM Approach	Tools that assist with identification, costing and selection of recovery options.	Supported
Deliver BCP	Tools that assist with organizing, compiling or generating documents that form part of the overall business continuity plan. This may include (but is not limited to): -Incident Response Plans; -Business Recovery Plans; -IT Service Continuity and Recovery Plans; -Communications matrices; -Templates for incident management activities	Supported

Other functionality:

Name	Description
Paragon Impacts	Paragon allows organisations to conduct a business impact analysis of a potential disruption and provides the ability to create surveys, which now can feed results directly to any item in an availability plan. For instance, companies could assess and record how potential system disruptions may affect a business process such as Sarbanes-Oxley compliance procedures
Paragon Profiles (Dependency Modelling)	Ability to map many to many relationships, including (but not limited to) applications to infrastructure, technology to locations, business processes to locations and business processes to applications and infrastructure. The Profiles module provides a 'living whiteboard' to profile an organization's infrastructure, environment and interdependencies. The whiteboard can be printed and stored - in addition to being viewed. This capability enables companies to take a snapshot of an infrastructure area and examine the impact should a disruption occur. For example, an organization could look at how people, business functions and facilities would be affected if a specific server was disrupted.

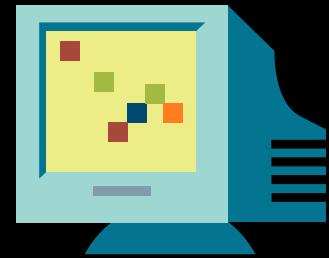
6. Continuity Controls

Controls implemented by using this method

Control Reference	Comment
BCMFI03	Progress reports can be produced
BCMFO01	Paragon Profiles helps an organisation understand the structure and to customise what is in scope
BCMFRR01	These can be defined via the contact database. Paragon Notifications will communicate with the required teams
BCMFP01	This can be attached at an appropriate place in the program
BIA03	Paragon Impacts allows flexible surveys to be built to collect data on resources, dependencies and impacts.
BIACRR01	The information gathered in the impact analysis is saved in a central database and can be analysed to determine resources and dependencies. The information is available for use in the plans.
BIACRR02	The information gathered in the impact analysis is saved in a central database and can be analysed to determine prioritised activities. The information is available for use in the plans.
BCMARS01	The results from the analysis can be used to develop the strategy which can be developed or a separate document can be attached at the appropriate place in the program.
BCPDCP01	Action Plans can be developed and templates are also available which can be customised
BCPDCP02	Action Plans can be developed and templates are also available which can be customised
BCPDCP03	Action Plans can be developed and templates are also available which can be customised
BCPDIM01	Action Plans can be developed and templates are also available which can be customised

Tools Reviewed

- Paragon (SunGard)
- LDRPS (Strohl Systems)
- Shadow-Planner (Office Shadow)
- myCOOP (COOP Systems)
- enVision (SDPL)
- BCP4me (CBD-e)
- ImpactAware (Texonet)
- Crisis Commander (Svensk Krisledning)



Summary of the Tools

- Different tools for different jobs
 - Paragon, LDRPS, Shadow Planner - full BCM lifecycle & plan templates
 - Crisis Commander – incident call out, notification and incident management
 - enVision – risk and corporate governance
- Most are browser based
- All use different terminology – quite confusing
- Need to identify what you need a tool for
- Review a few to find which one meets your requirements
- Make up your own mind!

Summary of the Report

- BCM Overview and detailed process
- Glossary
- List of BCM controls
- Method overview
- Method inventory
- Tools inventory

- Basis for understanding BCM and supporting resources



The Final Result

- The 'best bits'
- Readable
- Understandable
- Practical
- Clear and Concise
- Diagrams
- Examples



Findings


- We didn't manage to find any European BCM methods
- Countries without their own method/standard tend to use BS 25999
- Compliance is becoming sought after in the UK
- No one method is sufficient – you will find your own favourites
- Need integration of methods
- In today's large global organisations a tool is almost necessary to manage the BCM process
- Even with a tool, BCM knowledge is necessary – they don't fully guide you through the whole process



In Conclusion

- These studies helps to bring together the best parts of all the methods found
- Introduces users to available BCM tools
- Also uses authors' experience of BCM
- Delivers a comprehensive, easy to understand study of everything an organisation needs to know to implement a BCM programme





Thank You!
Any Questions?