

# MARSH



MARSH MERCER KROLL  
GUY CARPENTER OLIVER WYMAN

16 January, 2008

## **Business Continuity Management AIRM Presentation**

David Hamilton, Senior Consultant

# Presentation Overview

- Terms used for BCP
- Where BCM fits in a business plan
- Business Interruption challenges that face Underwriter in 2008 and beyond
- Critical Process Identification
- Summary of three phase plan
- Example of a BCP project
- Questions followed by Break

# Presentation Overview

- What is Risk
- Risk Variables
- Business Impact Analysis
- Testing and Training
- Information Technology

## ■ Terms Used (Reference BS 25999 – 1 – 2006)

- **Business Continuity:** Strategic and tactical capacity of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.
- **Business Continuity Plan:** A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.
- **Business Impact Analysis:** A process of analysing business functions and the effect that a business disruption might have upon them.

## ■ Terms Used (Reference BS 25999 – 1 – 2006)

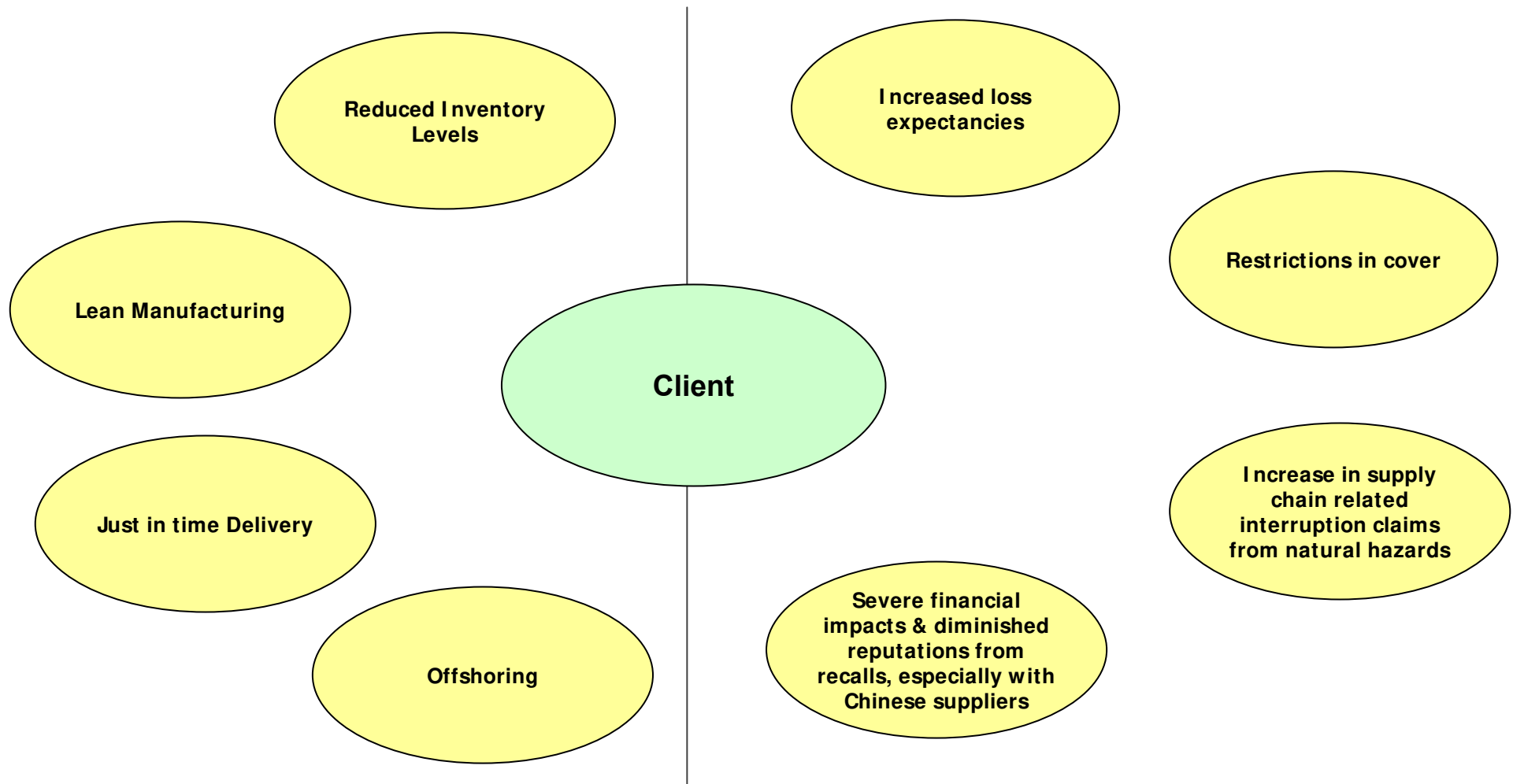
- **Critical activities:** Those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives
- **Disruption:** An event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organisation's objectives

# BI Challenges for Underwriters

# Developing Loss Estimates for BI

## Positive Operational trends within Industry (financial benefits)

## Current & Future Challenges to Underwriters of BI Coverages

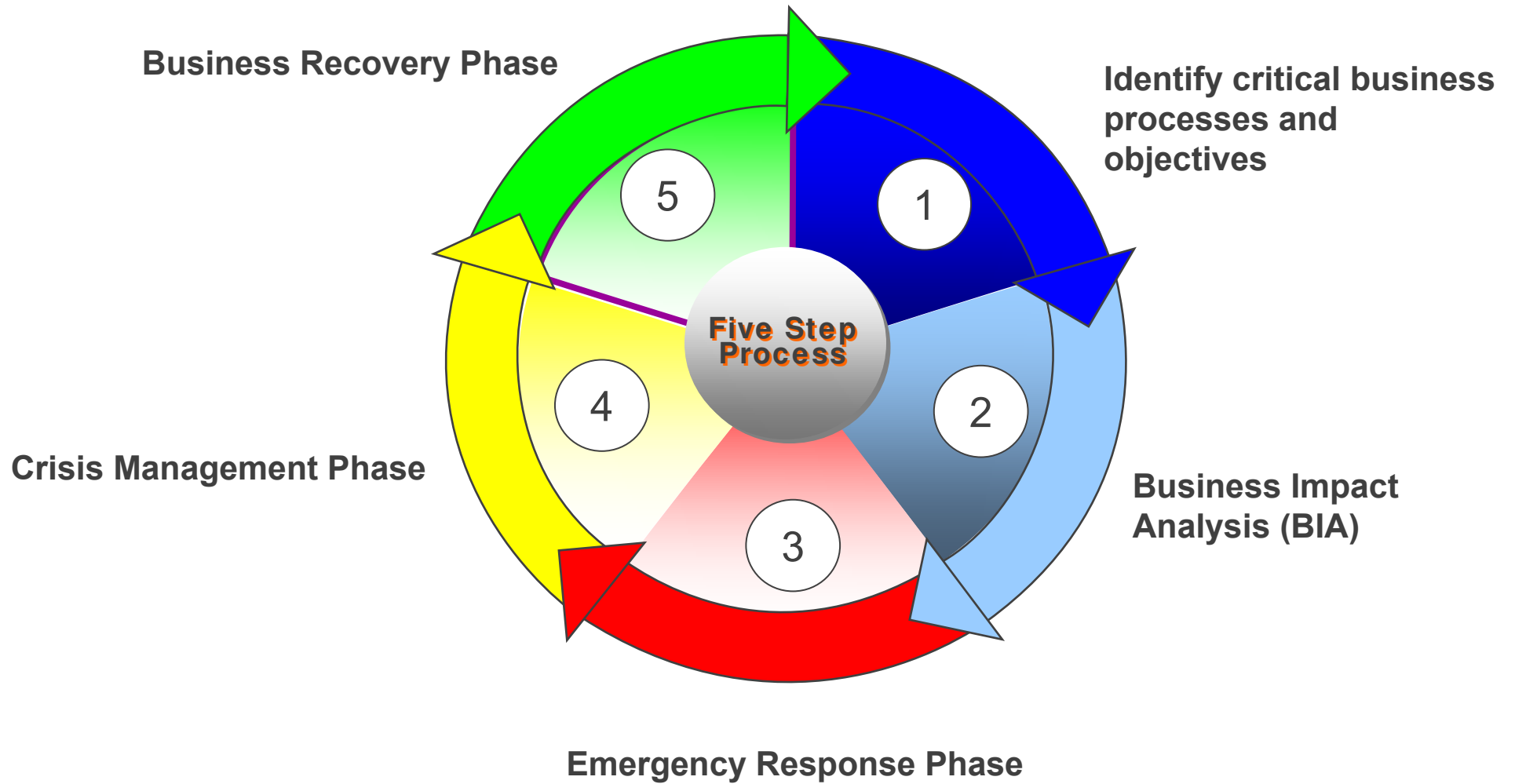


## Further Challenges facing BI Insurers

- Industry is very positive to supply chain optimisation by producing significant benefits to US companies by freeing up cash
- These changes have been credited with the record levels of mergers and acquisitions in recent years
- According to recent studies, companies that have not whittled down their inventories have left \$877 billion tied up in their balance sheets
- Loss estimates too high = higher premiums for them to underwrite the risk based upon the data available to them
- Loss estimates too low = risk being underinsured

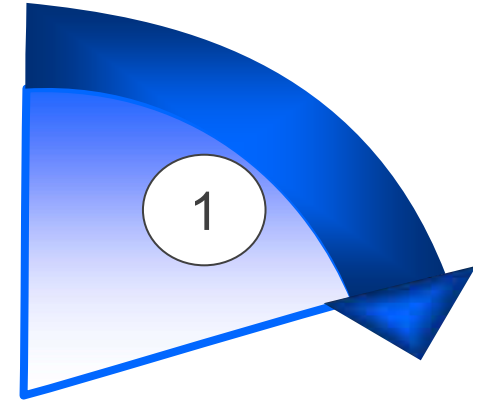


# BCP helps identify this



# Critical business process identification

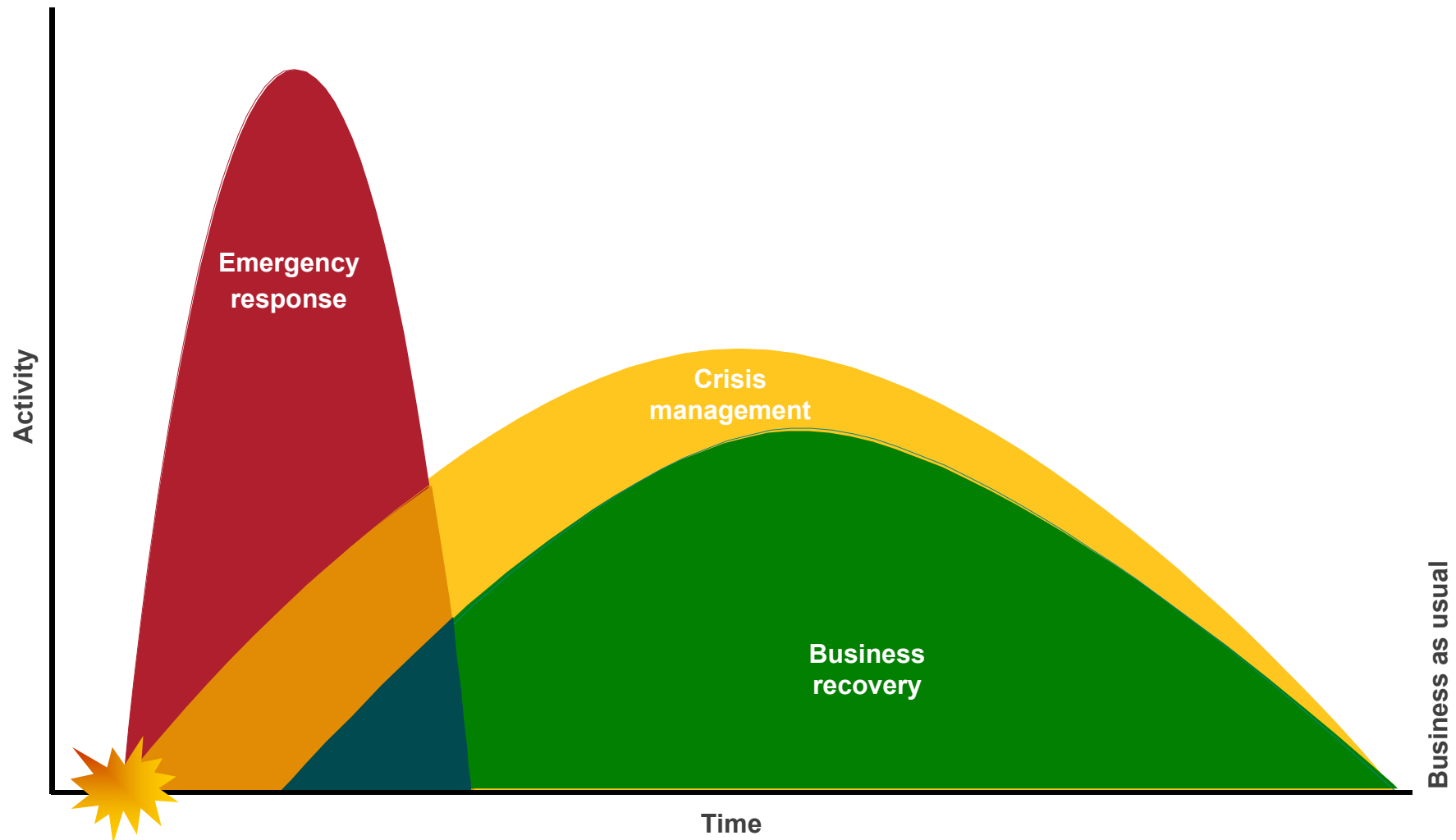
- **The aim of the Business Continuity Plan needs to be linked to the:**
  - Key objectives of your business
  - Key performance indicators
- **Key planning assumptions are:**
  - Strategic aim to recover the critical business operations within say 3 working days to maintain acceptable service to customers.
  - The plan usually assumes that there will be a maximum period of one day downtime. The business will have sufficiently recovered to allow for the plan to be closed at the latest 28 days after the incident.



Minimal service level requirements?  
Recovery Time Objective?  
What is the risk tolerance level?

# Business Continuity Plan in focus

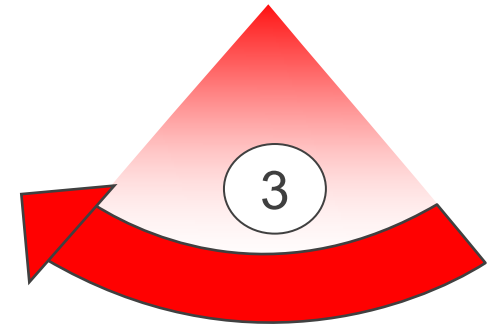
## Phases of recovery



# Emergency Response Team

- Key involvement – HR, Facilities, IT
- Deals with:
  - Emergency evacuation
  - Employee issues
  - Recovery site (IT & HR)

# Emergency response Examples

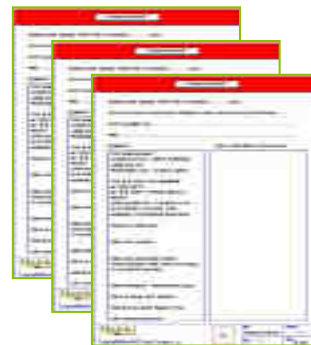
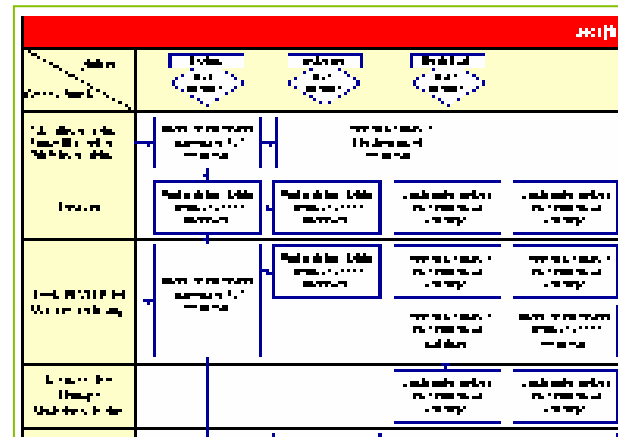


## Emergency Response Plan

**Strategic :** Notification and activation criteria covering 0 to 2 hours

**Operational:** Leader interfacing with:

- Evacuation procedures
- Security procedures
- First Aid
- Medical assistance
- IT



# Crisis Management Team

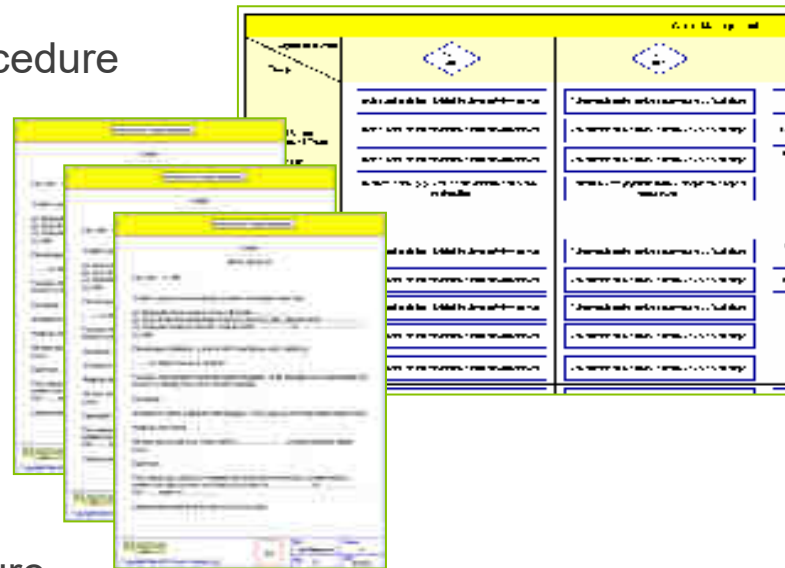
- Key involvement – Business Leaders (Senior Management Team)
- Deals with:
  - Overall responsibility for handling incident
  - Critical priorities
  - External organisations
  - Contact with Corporate

# Crisis management plan (Example)

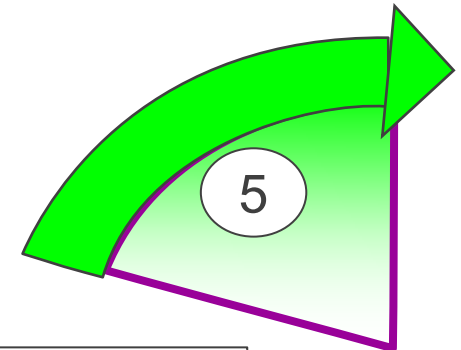
4

## CM plan delivery

- Notification and escalation procedure
- Layout of command centre
- First meeting agenda
- Crisis management actions
- Stakeholder mapping
- Media communication
- Procedure next of kin
- Trauma counselling
- Internal communication
- Logbook
- Debriefing / evaluation procedure

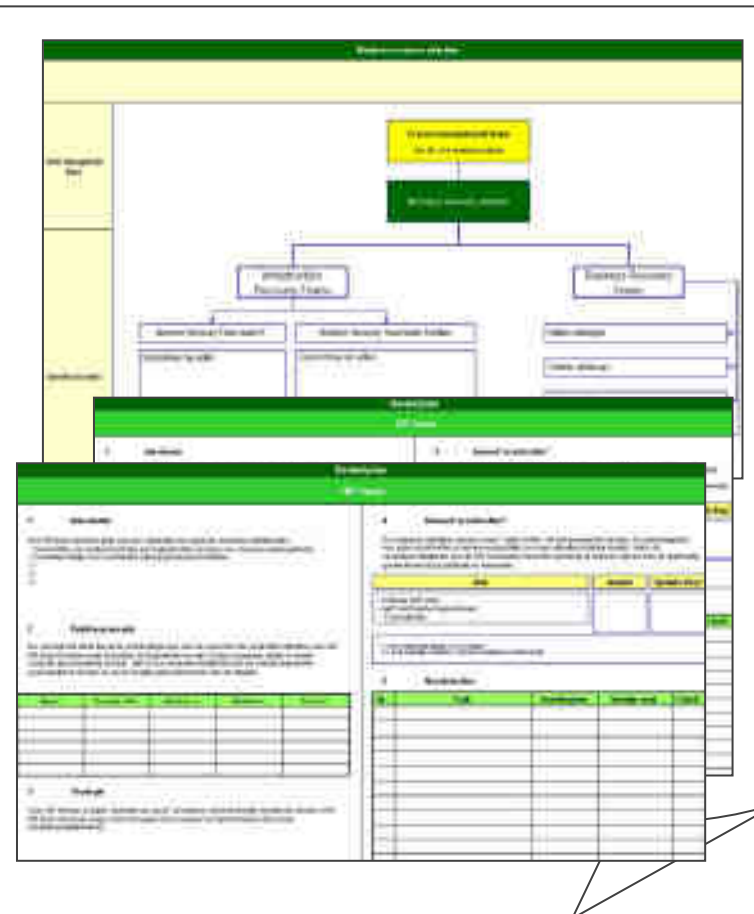


# Business recovery plan Example



## Business Recovery plan delivery

- Recovery organisational structure
- Per critical function:
  - Recovery strategy and assumptions
  - Recovery priority
  - Recovery specific actions (Who does what?)
  - Call trees
  - Contact details team members
  - Content of battle box





# Questions?

# Business Impact Analysis

# What is *Risk*?

- Risk is the **possibility** of incurring misfortune or loss (Collins English Dictionary).
- Risk is the combination of the **probability** of an event and its **consequences** (IRM Risk Management Standard).
- Risk is any **unintended** or **unexpected** outcome of a decision or course of action (F. Wharton)
- Risk is a **threat** that an event, action or failure to act will **adversely** affect an organisation's ability to achieve its business objectives and execute its strategies effectively (The Association of Corporate Treasurers)
- **Risk** is the **chance** of something **happening** that will have an **impact** on **objectives** (Australian Standard AS/NZS 4360:1999).

# Risk – definition for A Company

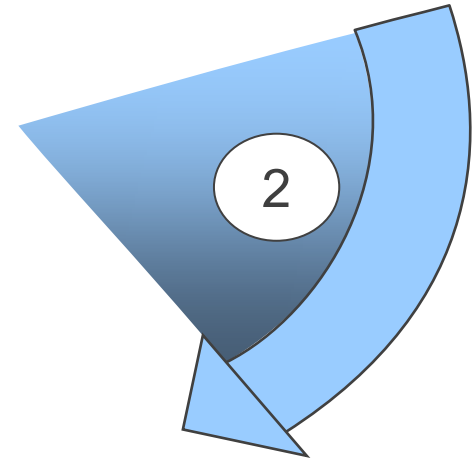
- The **possibility** or **likelihood** that an unplanned event will occur to adversely **affect** or **impact** the goals and objectives of A Company
- Risk = Impact X Likelihood

# Risk Assessment Variables

- **Impact** (severity)
  - How good/bad is it when it does happen?
  - Low to Catastrophic
  
- **Likelihood** (frequency / probability)
  - how likely is it (Unlikely, Likely, Very Likely)
  - How often does it happen?

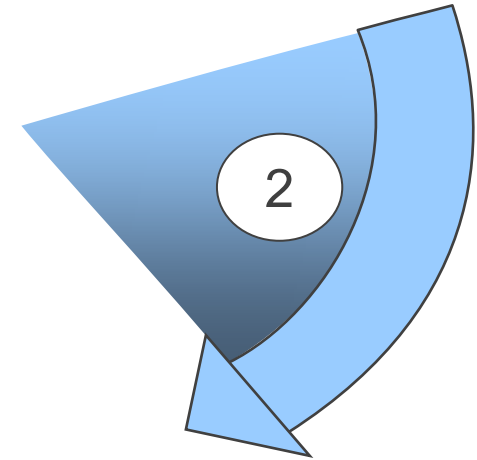
## Business Impact Analysis (BIA)

- Key starting point for a BCP project
  - Clear overview of the company and process
- Basis for formulating a recovery strategy
  - Focus on most critical processes
  - Identify most required resources



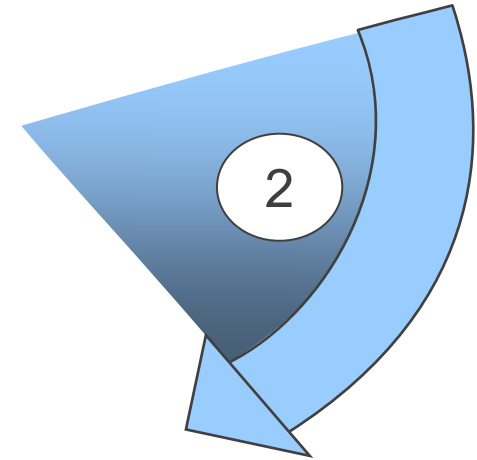
# Business Impact Analysis

- Review of processes and activities
  - Core and supporting processes
  - Objectives
  - Risk understanding and perception
  - Dependencies and (minimal) resources
  - Impact of interruption
  - Workarounds
- Defining most critical processes
  - Recovery Time Objectives
- Determining the impact of an interruption
  - Operational
  - Financial



# Business Impact Analysis

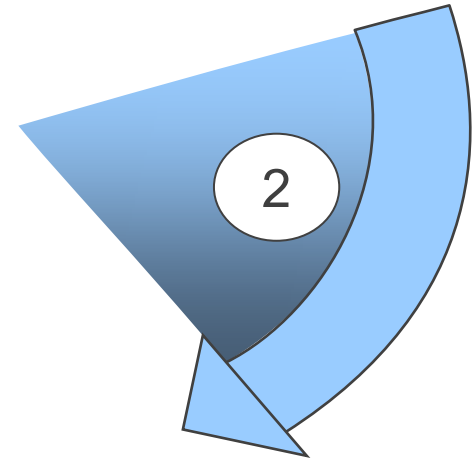
- Operational
  - Identification of key processes
  - Set Recovery Time Objectives
  - Process Flow of Organisation
- Financial
  - Maximum loss of earnings due to incident
  - Estimated period to recover





## BIA (Summary example of Questions)

- What are the key business functions and main activities?
- What resources are needed for these?
- What is managements opinion on the key risks that could impact the business (loss of machine, IT data)?
- What are the recovery actions that would be taken following a loss in this area?





# Information Technology

# When discussing IT, what do we mean?

- Information Security Management
- Information Security requires a truly integrated approach to link all aspects of security (organisational, technical, administrative and physical) to:
  - a strategic combination of IT architecture
  - business driver and processes
  - legal requirements
  - threat scenarios
- One integrated standard ISO 27001 (successor to BS7799)
- This system address information assets security from a risk based perspective by ways of policies and best practices.

# What problems can we try to solve?

- **Lack of Systematic Approach**

Many information security programmes lack a systematic risk management approach

- **Silo Effect**

Security expectations and delivery are often disconnected. Board level interest in security drives improved compliance and governance. However, security solutions remain largely reactive and silo based and focused on technology (Marsh example WTC)

# MARSH



MARSH MERCER KROLL  
GUY CARPENTER OLIVER WYMAN