

**Risk Management MN220:  
Seminar 8: Crisis  
management**



# SHERIDAN COLLEGE

PERTH | WESTERN AUSTRALIA

# Refresh - Implementation plan

## Contains:

- How the risk management plan (RMP) will be implemented in the business;
- Time line on activities;
- Milestones for achievement; and
- Training/ education/ awareness.

# Seminar 8.

## Crisis management and business continuity mgnt.

- Introduction
- What a crisis and how does it arise?
- What is a disaster?
- Crisis management and disaster recovery
- Crisis management team
- Crisis Management Plan (CMP)
- Business continuity planning and management
- Business impact and threat analysis
- AS/NZS 5050, Business continuity –Managing disruption-related risks
- AS/NZS HB 221, Business Continuity Management
- The Business Continuity Plan (BCP)
- Case study



pic007781

## Preventative

- **Risk Management Planning**
- **Business Impact Analysis (BIA)** *after Risk assessment is complete*
  - MAO
  - Duration of disruption
  - Critical Business Function
  - Crisis Response and Business Continuity Planning (BCP) is initiated

## Event

- **Disaster**- natural or man made
- **Crisis**- Unplanned Events
- Recovery begins
- Business Continuity Management (BCM) begins

## Recovery

- **Disaster Recovery Plan executed**
- **Business Continuity Planning executed**
- **CMT**- Crisis Management Team and Team Leader (CEO)
- **Crisis Command Centre** to roll out Crisis Management Plan

# Crisis

*“A crisis is a major unplanned event which either in itself is a major problem, or leads to the development of a major problem”.<sup>1</sup>*

Crises arise from:

- Accidents;
- Third party involvement;
- Events arising from an accident.

• 1 Campbell, R., Crisis Control, Preventing & Managing Corporate Crises.

# Crisis

*“Situation that is beyond the capacity of normal management structures and processes to deal with it effectively.”<sub>2</sub>*

- 2 AS/NZS 5050:2010, Business continuity –Managing disruption-related risks

# Crisis management

*“Crisis management is now an important part of strategic management because it enables an organisation to reduce the threats and vulnerabilities related to a crisis.”<sub>3</sub>*

- <sub>3</sub> Campbell, R., Crisis Control, Preventing & Managing Corporate Crises.

# Crisis Management

- <https://www.youtube.com/watch?v=mel31geq2LQ>

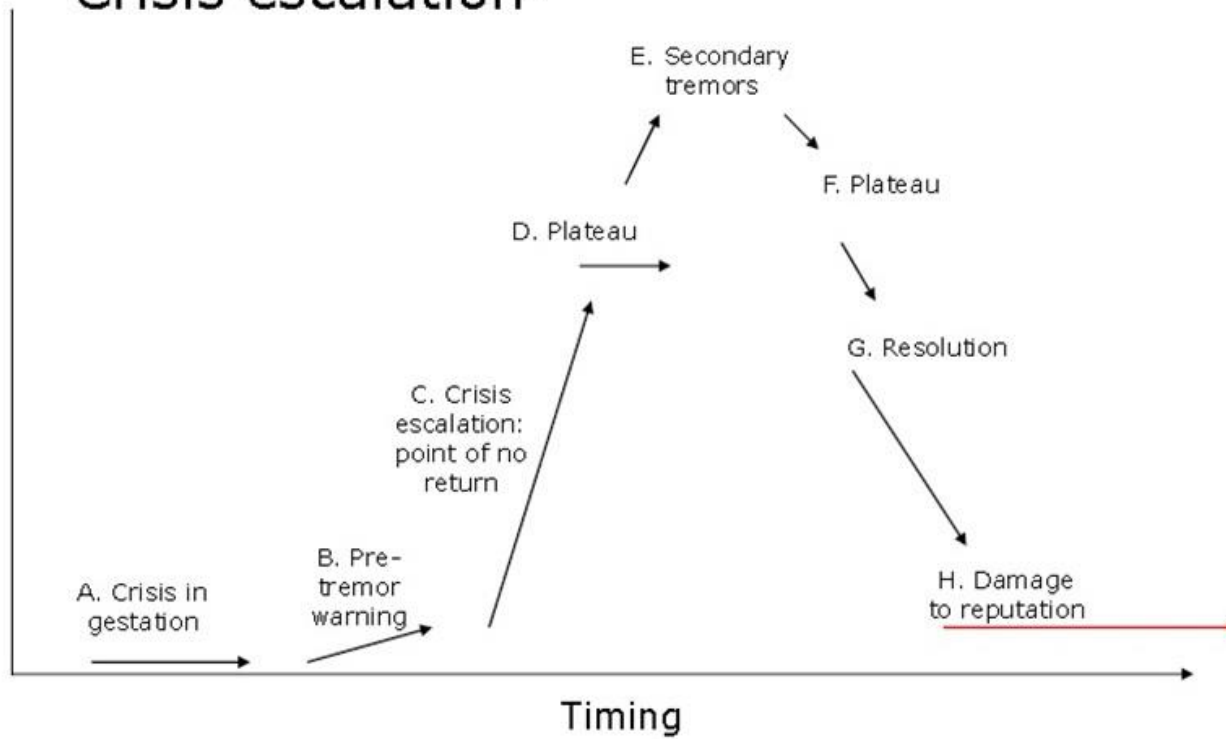
# Disaster

- (From Greek meaning, "bad star") is a natural or man-made event that negatively affects life, property, livelihood or industry often resulting in permanent changes to human societies, ecosystems and environment;
- A serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources;
- Any unplanned circumstance or event that results in an inability to support critical business functions within the current environment.

# Crisis creating events

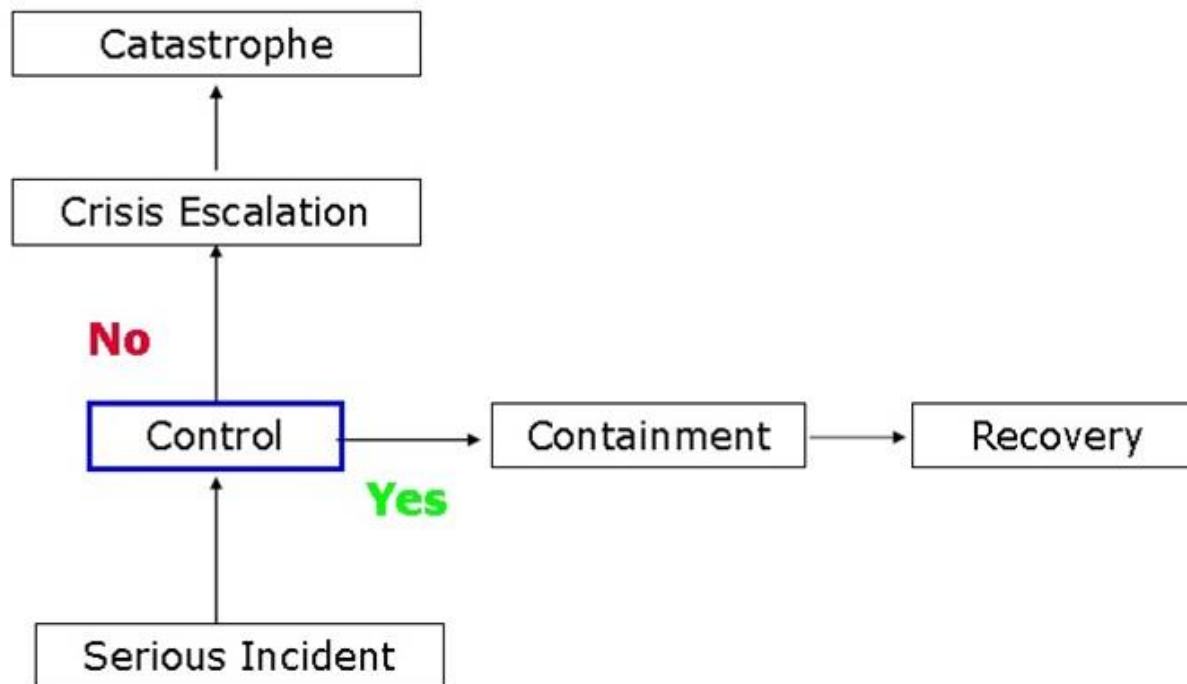
- Business scandal;
- Death or resignation of CEO;
- Bankruptcy;
- Government/tax department investigation;
- Major changes in the marketplace;
- Hostile takeover;
- Loss of sensitive or critical information;
- Security breach;
- Staff redundancies or lay-offs.

## Crisis escalation<sup>5</sup>



<sup>5</sup>Curtin, T., Hayman, D., Husein, N., Managing A Crisis, A Practical Guide

## Crisis control<sup>6</sup>



<sup>6</sup> Campbell, R., Crisis Control, Preventing & Managing Corporate Crises.

# Stakeholders in a crisis

- Employees & their families;
- Directors;
- Shareholders;
- Media;
- Regulators;
- Politicians;
- Public;
- Activists;
- Customers;
- Suppliers.

# Media in a crisis

## Bad news makes headlines

*“If the company does not control the management of information, the media will.”*

Media need to be briefed about the crisis.

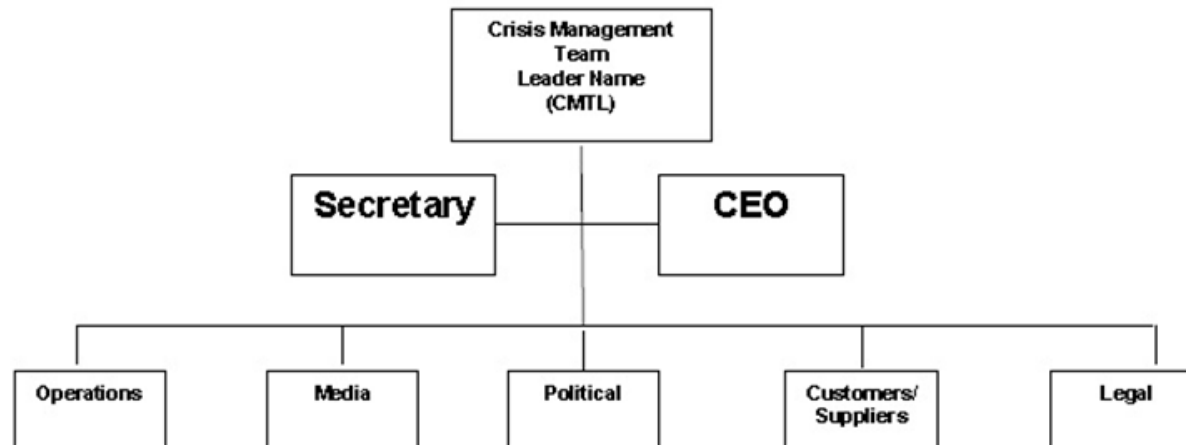
Communication must be:

- Appropriate;
- Timely;
- Consistent.

# Crisis Management Team (CMT)

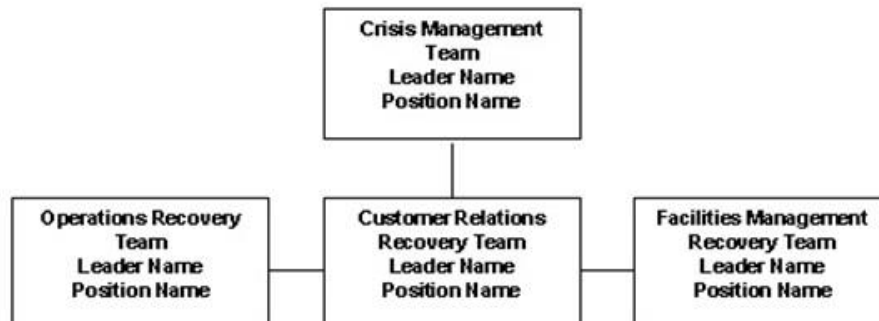
- The establishment of the Crisis Management Team is one of the most important elements of crisis management;
- Each person on the team has a designated role;
- No person will take another person's role;
- Each person must be equipped for the role;
- Each person must be tested for the role; and
- Each person must know the other team members.

## Crisis Management Team (CMT)<sup>7</sup>



<sup>7</sup> Curtin, T., Hayman, D., Husein, N., Managing A Crisis, A Practical Guide

# Crisis Management Team (CMT) - simplified



# Crisis Management Team Leader (CMTL)

- The Crisis Management Team Leader may or may not be the CEO;
- The Crisis Management Team Leader must have the following attributes:
  - Authoritativeness;
  - Decisiveness;
  - Ability to communicate effectively; and
  - Diplomacy.

# Crisis command centre<sup>8</sup>

- Central location for managing communications ;
- Central location for implementation of CMP;
- Room equipped with communications available outside the normal company's network;
- May be multi-purpose room (used for training or other purposes).

•<sup>8</sup>Campbell, R., Crisis Control, Preventing & Managing Corporate Crises.

# The Crisis Management Plan (CMP)

- The CMP must be endorsed by the CEO and the board;
- The CMP must be part of corporate policy;
- The plan must be simple and easy to use;
- Accountability is essential;
- It must be capable of application at each business location;
- The plan must have recording process to keep accurate records of events;
- The plan must be budgeted; and
- The plan must be tested.

# Recovery

- The business needs to continue during and after the crisis;
- The business will be stressed and will be operating under different conditions;
- Once the nature of the crisis has been determined and the CMT is managing the crisis, the business continuity plan(s) can be invoked.

# The Difference Between Business Continuity and Disaster Recovery

- <https://www.youtube.com/watch?v=qfjWhAmWYL8>

# Business Continuity Management

*“Business Continuity Management provides the availability of processes and resources in order to ensure the continued achievement of critical objectives.”<sup>9</sup>*

- 9 Australian/New Zealand Standards, HB 221:2004 Business Continuity Management

# Business Continuity RM<sup>10</sup>

- Principles
- Framework
- Process
- Verification

*Note: Draws on fundamentals of AS/NZS ISO 31000*

•10 AS/NZS 5050:2010, Business continuity –Managing disruption-related risks

# Business Impact Analysis (BIA)

*“Detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the consequences.”<sup>11</sup>*

- Method of determining the degree to which the business will be impacted;
- Carried out following the risk assessment;
- May be for part of the organization or whole of organization.

•<sup>11</sup> AS/NZS 5050:2010, Business continuity –Managing disruption-related risks“

# Business Impact Analysis (BIA)<sup>12</sup>

- Business unit/ department
- Contact details and information
- Type of impact
- Impact over time (hours, days, weeks, months)
- Operational impact over business objectives

• <sup>12</sup>Australian/New Zealand Standards, HB 221:2003 Business Continuity Management

# Duration of disruption

*“Detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the consequences.”<sup>13</sup>*

- Method of determining the degree to which the business will be impacted;
- Carried out following the risk assessment;
- May be for part of the organisation or whole of organisation.

# Maximum Acceptable Outage (MAO)

*“Maximum period of time that an organization can tolerate the disruption of a critical business function.”<sup>14</sup>*

- 14 AS/NZS 5050:2010, Business continuity –Managing disruption-related risks

# Critical Business Function<sup>15</sup>

*“A business function or part thereof identified as essential for survival of the organization and achievement of its critical objectives .”<sup>15</sup>*

- 15 AS/NZS 5050:2010, Business continuity –Managing disruption-related risks“

# Crisis response and BCP

## Three responses to a crisis:

- **Emergency** response (carried out by Crisis Management Team);
- **Continuity** response (processes and controls to meet critical requirements of the organisation);
- **Recovery** response (processes and resources to bring the organisation back to “pre-crisis” condition).

# Risk and Business Continuity Planning

- Risk management is preventative, business continuity is corrective;
- Risk and BCP are interrelated;
- Risk identification and analysis is the precursor to developing the BCP.

## Six key elements of BCP<sup>16</sup>

1. Understanding the environment in which the organisation operates;
2. Determining the parts of the business critical to its short term and long term success;
3. Quantifying the disruptive impact of threats on critical business processes;

•16 Adapted from Australian/New Zealand Standards, HB 221:2004 Business Continuity Management

## Six key elements of BCP (cont'd)

4. Documenting the key resources, infrastructure, tasks and responsibilities to support critical processes;
5. Establishing processes that ensures information remains current in a changing risk environment;
6. Ensuring relevant stakeholders and employees are aware of the BCP arrangements.

# BCP processes and risk management<sup>17</sup>

- 9 steps in the BCP process;
- 7 elements in the risk management process;
- Risks are identified through the business impact analysis and risk and vulnerability analysis;
- BCP deals with risk impact over time.

<sup>17</sup>Australian/New Zealand Standards, HB 221:2003 Business Continuity Management

# Nine steps in BCP<sub>18</sub>

1. Commencement – establishing scope and objectives of the process, management commitment and the project team;
2. Risk and vulnerability analysis – determines which risks will impact critical processes;
3. Business impact analysis – impact over time on critical business processes. Scenario development, and Maximum Acceptable Outage (MAO), and workarounds;

- 18 Australian/New Zealand Standards, HB 221:2003 Business Continuity Management

## Nine steps in BCP (cont'd)

4. Response strategies – emergency (crisis), continuity, and recovery;
5. Resources and interdependencies – resources required and external interdependencies;
6. Documentation – documenting the continuity plans for scenarios;

# Nine steps in BCP (cont'd)

7. Communication strategy – development of the communication strategies;
8. Training, maintaining and testing – testing the plan(s), training team members, and maintenance of plans;
9. Activation and deployment – plan activation and governance (during plan activation).

# BCP team

Similar to crisis management team approach.

Core components:

- Technology recovery;
- Facilities recovery;
- Human resource management.

Need to communicate with stakeholders.

- 19Barnes, J., A Guide to Business Continuity Planning

# Criteria for analysis

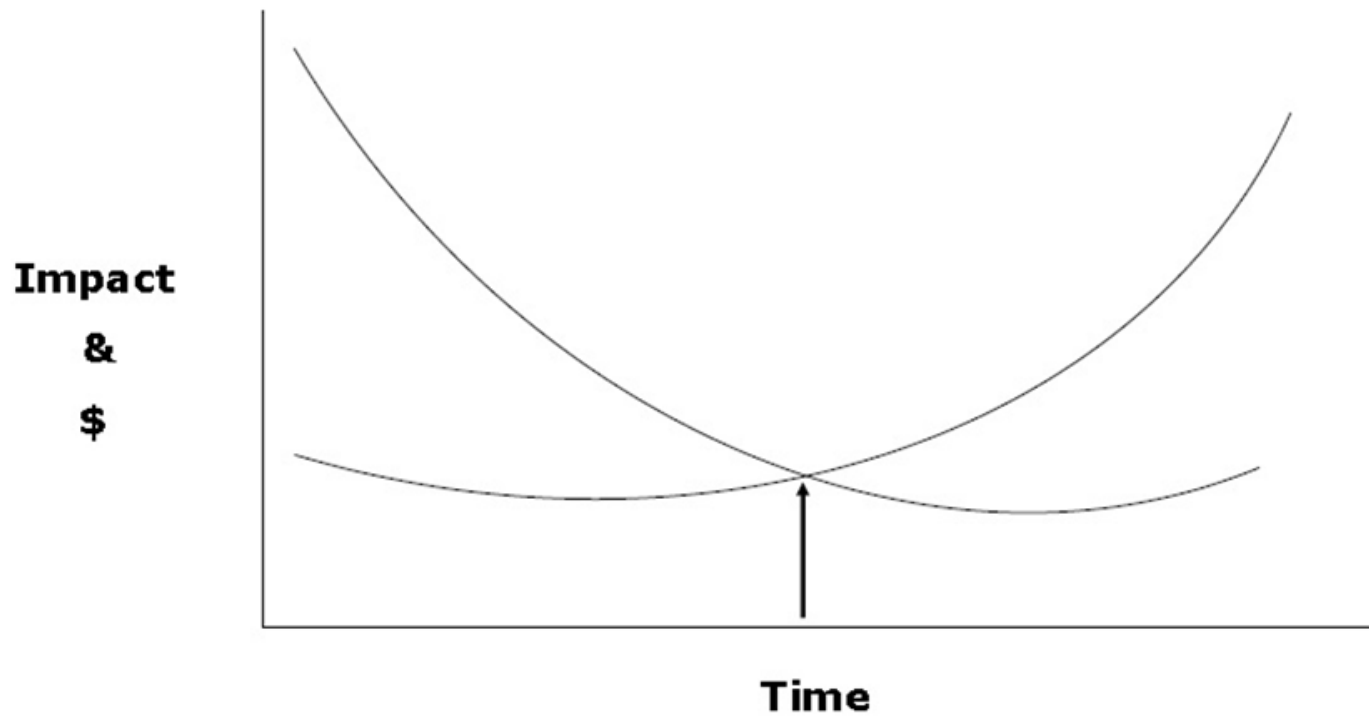
Similar to AS/NZS ISO 31000:

- Consequence ratings 1-5 (insignificant to catastrophic);
- Impact covering financial and non-financial (operations).

# Strategy selection

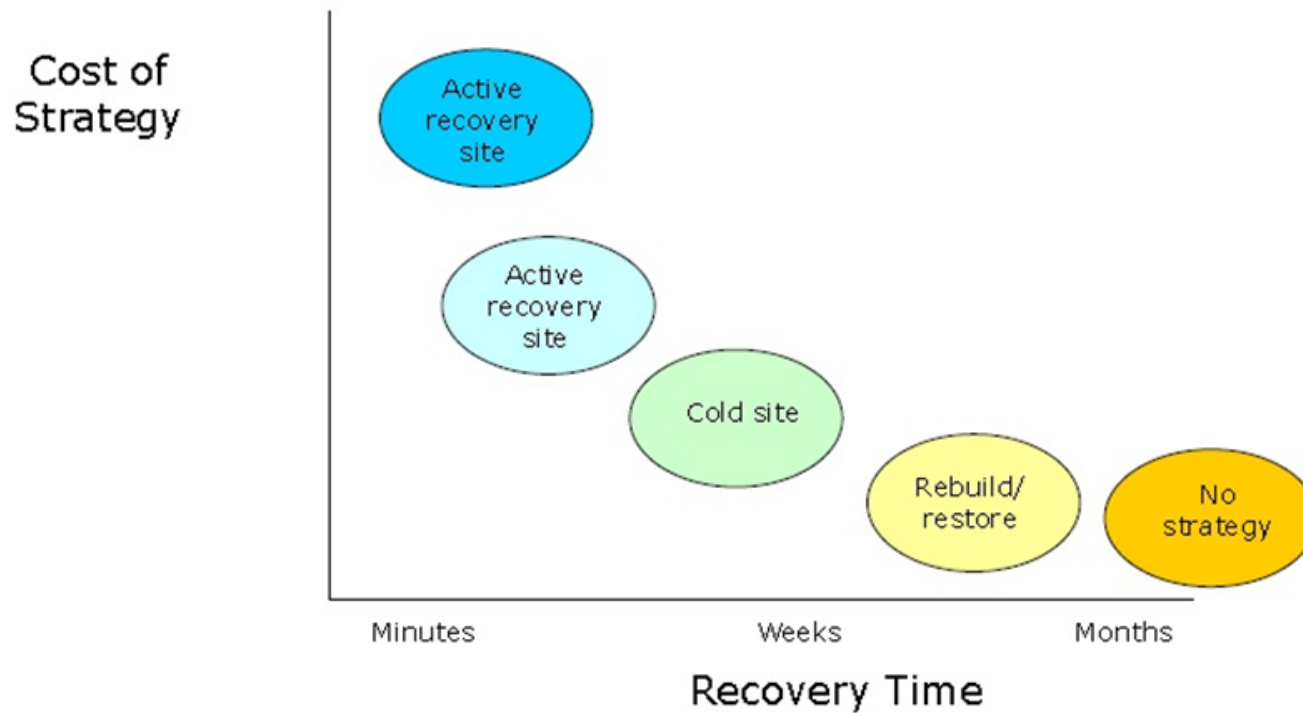
- What are the emergency/ recovery/continuity strategies?
- What is the most cost effective strategy?
- How will it be implemented?
- What resources are required to implement the strategy?
- Where are the contact details for the stakeholders?

## Strategy selection<sup>20</sup>



<sup>20</sup>Barnes, J., A Guide to Business Continuity Planning

## Example – computer centre recovery<sup>21</sup>



<sup>21</sup>Barnes, J., A Guide to Business Continuity Planning

# Resourcing

What physical resources are required?

- Desks, chairs, office furniture;
- Telecommunications, computers, email/messaging.

What human resources are required?

- Third party (contract) personnel.

What financial resources are required?

- Additional costs of office/equipment rental;
- Temporary outsourced process management.

# Communication strategy

- Responsibilities for communication (reference CMP if in place);
- Stakeholder message (staff/personnel, board, fire/police/government, media);
- Management of the communication
- Deployment .

# Testing

## Desktop review:

- Examination of documentation and plans (for viability, integrity, deployability).

## Desktop scenario:

- Walkthrough of each of the BCP's examining the scenarios.



# Testing (cont'd)

## Notification and call-out:

- Notify team members of business disruption;
- Evaluate effectiveness of response.

## Live scenario:

- Testing on scenarios, limited or across the business.

## Business recovery:

- Close down of processes/systems;
- Fully deploy BCP.

# Issues

- Developing a BCP takes time and resources;
- Often the attitude is “it won’t happen to us”
- BCP’s are difficult to fully test;
- Fully testing a BCP can bring risks to maturity should the BCP’s fail.

# Summary

- What is a crisis and how does it arise?
- What is a disaster?
- Crisis management and disaster recovery;
- Crisis management team;
- Crisis Management Plan (CMP);
- Business Continuity Planning (BCP) and management;
- Business impact and threat analysis;
- AS/NZS HB 221:2004, Business Continuity Management (BCM);
- Relationship between AS/NZS ISO 31000 and AS/NZ 5050:2010;
- The Business Continuity Plan (BCP).

# **BCP Reverse-Engineering**

## **Role Play**

- Group Activity on Scenario
  - 3 Groups are formed
    - Crisis Team Leaders (CEO & Exec. Team)- 3 people
    - Crisis Command Centre – 4 people
    - Execution Team – 4 People
    - Reporter/Runner ( Lecturer)

# Video

- <https://www.youtube.com/watch?v=ilYVNR00reQ>
- Airplane Crash Melbourne

## Lecture 8-Cont.

# Enterprise risk management (ERM)

- Enterprise Risk Management (ERM)
- Establishing a risk management culture
- Leadership, management and commitment
- Interdependency between policy, goals, reward and sanction
- Methodologies, processes, and outputs
- Structure
- Consolidation and mapping
- Tools and technology
- Training and development
- Timetable and programme
- Integrating quantitative and qualitative elements of risk management
- Developing the ERM system – case studies



# What is enterprise risk management ?

- [https://www.youtube.com/watch?v=w\\_y6S8yF7WA](https://www.youtube.com/watch?v=w_y6S8yF7WA)

# Enterprise risk management<sup>1</sup>

*“The process required to establish effective risk management as part of the day-to-day business at an **organisational level** and subsequently at **operational, project or team levels** is likely to require a **change of culture** for many organisations.”<sup>1</sup>*

<sup>1</sup>AS/NZS 4360:2004, Risk Management

# ERM

- Term once frequently used to discuss the management of risk across the enterprise;
- Related to “whole of business” rather than individual business process;
- Used less often today as risk management becomes more pervasive across and within the business.

# BASIC EXTERNAL ANALYSIS

- PESTLE
- Using Coso

# Organisational culture

Organisational culture is shaped by the following<sup>2</sup>:

- Rules and policies;
- Goals and measures;
- Rewards and recognition;
- Staffing and selection;
- Training and development;
- Ceremonies and events;
- Leadership and behaviour;
- Communications;
- Physical environment;
- Organisational structure.

<sup>2</sup> Holmes, A., Smart Risk

# Enterprise risk management culture

- Senior management must be engaged;
- Risk management needs to be “seen” at all levels of the organisation;
- Training conducted throughout the organisation assists in ERM;
- Success stories need to be “sold;”
- A “champion” or sponsor is required to engender a positive risk management culture;
- Staff need to be supported by management to manage risk.



# Response to failure<sup>3</sup>

| Fear of failure | High | Forget    | Blame       |
|-----------------|------|-----------|-------------|
|                 | Low  | Learn     | Sanitise    |
|                 |      | Forgiving | Unforgiving |

**Underlying organisational culture**

<sup>3</sup> Holmes, A., Smart Risk

# “Hands up – cover up”

- A “hands up” culture occurs when **fear of failure** is **low** and where the organisation is forgiving;
- A “cover up” culture occurs when **fear of failure** is **high** and where the organisation is unforgiving;
- A “hands up” culture encourages risk taking, whilst managing negative risk.

# Leadership and management

- The board needs to be committed to risk management;
- The CEO needs to be committed;
- Commitment needs to be demonstrated by both leadership (doing and saying), and through management (policy, procedures and processes).

# Commitment

- Risk management responsibilities need to be allocated;
- Risk Manager or Manager of Risk?
- Build risk into Key Performance Indicators (KPI's).

# Methodologies, processes and outputs

## AS/NZS ISO 31000:2009

- Risk assessments;
- Risk treatment;
- Risk monitoring;
- Risk reviews/audits;
- Communication and consultation;
- Risk register that is incorporated into strategic and business planning.

# Structure

- Risk management committee (for **large** companies);
- **Risk champion** for smaller companies;
- Establish risk into the **board agenda**;
- Establish risk into the **executive committee agenda**;
- Establish risk into the **strategic planning process**;
- Apply **reward and sanction** in embedding risk management;

# Consolidation and mapping

- Corporate (enterprise) risk register;
- Division/business unit risk register;
- Branch office risk register;
- Risk register consolidation;
- Risk consequence mapping.

# Corporate risk mapping

- Contextualises relative **risk impact** within the business;
- Provides a mechanism for business unit and project risk analysis;
- Reduces “noise” in the corporate risk register;
- Allows lower level common risks to be aggregated and escalated.

# Corporate risk mapping<sup>4</sup>

| Division Consequences | Enterprise Consequences |  | Business Unit Consequences | Enterprise Consequences |
|-----------------------|-------------------------|--|----------------------------|-------------------------|
| Catastrophic          | Major                   |  | Catastrophic               | Moderate                |
| Major                 | Moderate                |  | Major                      | Minor                   |
| Moderate              | Minor                   |  | Moderate                   | Insignificant           |
| Minor                 | Insignificant           |  | Minor                      | Insignificant           |
| Insignificant         | Insignificant           |  | Insignificant              | Insignificant           |

<sup>4</sup> Moore, P.

# Corporate risk mapping

| <b>Consequence</b> | <b>Corporate Financial Impact</b> | <b>Divisional Financial Impact</b> | <b>Business Unit Financial Impact</b> |
|--------------------|-----------------------------------|------------------------------------|---------------------------------------|
| Catastrophic:      | > \$10M                           | >\$500,000                         | > \$200,000                           |
| Major:             | \$500,000 -\$10M                  | \$200,000 - \$500,000              | \$100,000 -\$200,000                  |
| Moderate:          | \$50 000 - \$500,000              | \$100,000 - \$200,000              | \$50,000 - \$100,000                  |
| Minor:             | \$5,000 - \$50,000                | \$5,000 - \$100,000                | \$5,000 - \$50,000                    |
| Insignificant:     | <\$5,000                          | <\$5,000                           | <\$5,000                              |



# Corporate risk mapping - examples

**Risk : Inadequate insurance**

File Edit Window Help

3 Inadequate insurance

Description Cause/consequence Comments Attachments

Inadequate insurance cover for the business

Sum of Costs

|              |              |
|--------------|--------------|
| Ctrl Total   | Control Cost |
| 0            | 0.00         |
| Treat. Total | Treat. Cost  |
| 1            | 0.00         |

Assessment Quantification Corporate Assessment Audit Assessment

Assessment

☒ Relevant

Consequence Likelihood Control Effectiveness Risk Score

Absolute Catastrophic Almost Certain 25

Controlled Moderate Possible Reservations 9

Treated Minor Unlikely 4

Level of Risk Severity

☒ Very High ☐ Acceptable

☒ High ☐ Acceptable

☒ Low ☐ Acceptable

Attributes Additional Information Controls Treatments Findings Loss Events Review Notes Linked Risk Areas Linked Accounts Linked Objectives Linked Processes Tests

Risk Owner Simon High

Risk Status

Review By

Reference

Control Risk Self Assessment

☐ Control RSA

CRSA Status

Audit Assessment

Corporate Assessment

Impact

☒ Environmental

☐ Financial

☐ Public Image

Business Units

Business Unit

Risk Category 2

Risk Category 3

Creator Groups

Start R:\Programs\ERA V6\Cle... L11 PM.ppt CCIWA Enterprise Risk A... Home Window: Revie... 12:50 PM



Home Window: Review Perth

File Edit Window Help



Review Perth  
Perth office

REVIEW3  
3/03/2005

enterprise  
risk|assessor

ERA | Reporting | Risk Areas | Objectives | Accounts | Processes | Risks | Controls | Treatments | Action Plans | Loss Events | Tests | Findings | Review Notes



|    | #  | Name                                                          | Ctrl Consequence | Ctrl Likelihood | Ctrl Risk Level | Owner          | rp Ctrl. Consequence | Corp Ctrl. Risk Level | Ctrl. Risk S |
|----|----|---------------------------------------------------------------|------------------|-----------------|-----------------|----------------|----------------------|-----------------------|--------------|
| 1  | 14 | Failure to develop new client base                            | Major            | Almost Certain  | Very High       | Sue Stevens    | Minor                | High                  | 10           |
| 2  | 19 | Loss of key personnel                                         | Major            | Almost Certain  | Very High       | John Smith     | Minor                | High                  | 10           |
| 3  | 10 | Poor project management performance                           | Major            | Likely          | High            | John Smith     | Minor                | Medium                | 8            |
| 4  | 20 | Dust and noise                                                | Major            | Likely          | High            | Simon High     | Minor                | Medium                | 8            |
| 5  | 1  | Industrial action                                             | Major            | Possible        | High            | Fred Green     | Minor                | Medium                | 6            |
| 6  | 4  | Poor design resulting in product failure                      | Major            | Possible        | High            | Simon High     | Minor                | Medium                | 6            |
| 7  | 2  | Inadequate sub-contractor agreements                          | Moderate         | Possible        | High            | John Smith     | Insignificant        | Low                   | 3            |
| 8  | 3  | Inadequate insurance                                          | Moderate         | Possible        | High            | Simon High     | Insignificant        | Low                   | 3            |
| 9  | 6  | Poor supplier delivery timeframes                             | Moderate         | Possible        | High            | John Smith     | Insignificant        | Low                   | 3            |
| 10 | 23 | Inability to deal with major impact to business               | Moderate         | Possible        | High            | John Smith     | Insignificant        | Low                   | 3            |
| 11 | 8  | Use of unskilled equipment operators                          | Moderate         | Unlikely        | Medium          | Simon High     | Insignificant        | Low                   | 2            |
| 12 | 13 | Increased competition                                         | Moderate         | Unlikely        | Medium          | Stephen Rogers | Insignificant        | Low                   | 2            |
| 13 | 15 | Inadequate insurance leading to limited products and services | Moderate         | Unlikely        | Medium          | Sue Stevens    | Insignificant        | Low                   | 2            |
| 14 | 17 | Unsafe work environment leading to injuries                   | Moderate         | Unlikely        | Medium          | Greg Miller    | Insignificant        | Low                   | 2            |
| 15 | 24 | Vandalism to equipment                                        | Moderate         | Unlikely        | Medium          | Steve Jones    | Insignificant        | Low                   | 2            |
| 16 | 26 | Computer hardware failure                                     | Moderate         | Unlikely        | Medium          | Steve Jones    | Insignificant        | Low                   | 2            |
| 17 | 27 | Impact on schedule due to failure of contractor               | Moderate         | Unlikely        | Medium          | Sue Stevens    | Insignificant        | Low                   | 2            |
| 18 | 7  | Subcontractor poor performance                                | Minor            | Possible        | Medium          | Fred Green     | Insignificant        | Low                   | 3            |
| 19 | 9  | Failure to achieve project objectives                         | Minor            | Possible        | Medium          | Steve Jones    | Insignificant        | Low                   | 3            |
| 20 | 21 | Loss of data (IT failure)                                     | Minor            | Possible        | Medium          | Steve Jones    | Insignificant        | Low                   | 3            |
| 21 | 25 | Fraud or theft                                                | Minor            | Possible        | Medium          | Stephen Rogers | Insignificant        | Low                   | 3            |
| 22 | 5  | Loss of license                                               | Minor            | Unlikely        | Low             | Tony George    | Insignificant        | Low                   | 2            |
| 23 | 16 | Inadequate scoping of work                                    | Minor            | Unlikely        | Low             | Bill Brown     | Insignificant        | Low                   | 2            |
| 24 | 18 | Inadequate resources                                          | Minor            | Unlikely        | Low             | Greg Miller    | Insignificant        | Low                   | 2            |
| 25 | 22 | Use of outdated technology                                    | Minor            | Unlikely        | Low             | Simon High     | Insignificant        | Low                   | 2            |

Risk : 25 of 25. Selection:1

# Tools and technology

Managing the information;

Risk management software:

- Proprietary
- Generic (i.e., MS Excel)

Maintaining currency.

# Training and development

Training can be carried out at different levels within the organisation:

- Strategic risk management at senior management level;
- Operational risk management at the business process management level;
- Awareness and training for operating personnel.

# Timetable and program

- Set **realistic timetable and timeframe**;
- Develop the **program of activities**;
- Ensure **adequate resources** are applied to the program.

# Integrating quantitative & qualitative measures

- Develop formal structures and processes;
- Embed risk management into job descriptions for business process owners;
- Implement reward and sanction measures;
- Lead, guide and train personnel in risk management;
- Engage personnel at all levels;
- Adopt a “push-pull” approach to risk management.

# Enterprise risk management

*“Enterprise-wide risk management represents a **paradigm shift** in the way businesses **manage the uncertainties** that stand in the way of achieving their **strategic, operational, and financial objectives**.”<sup>5</sup>*

<sup>5</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# Developing ERM Risk Register

- <https://www.youtube.com/watch?v=kagXUDLDUlo>

# Future of ERM

- <https://www.youtube.com/watch?v=nQoJj6FBxrY>

# Companies studied<sup>6</sup>

- Chase Manhattan Corporation;
- E.I. du Pont de Nemours and Company;
- Microsoft Corporation;
- **United Grain Growers Limited;**
- Unocal Corporation

<sup>6</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# United Grain Growers

*“The second way I get comfortable (about risk) is the quality and institutionalisation of the controls at the micro level. The credit approval process and the trading monitoring process – we are probably the most vigilant about those two processes, and that’s where I think we have very good systems.”<sup>6</sup>*

<sup>6</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# United Grain Growers Case study- Lecturer to discuss questions below with students

- What has happened? (the **event**)
- What was the root **cause**? (contributing factors)
- What could have been done to prevent it? (controls)
- How could the UGG managers better managed ERM Risks? (executives, managers and staff)
- What were the risks and outcomes for the Public/clients, the company , internal stakeholders and staff? (take different perspectives and contexts)

# Unocal Corporation

*“(Now we’ve had) an organisational shift to saying, “Look, the only way we’re really going to get our line people to truly embrace safe operations, effective operations, control operations as a part of their job is to take away the crutch of (overreliance on) staff support and, at the same time, go from a compliance-based loss control system to a more commitment-based system – here is how you run your business, and by the way, if you run your business in an effective way, the loss control numbers should follow.”<sup>7</sup>*

<sup>7</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# Lessons learned<sup>8</sup>

1. A **cookbook recipe** for implementing enterprise-wide risk management is not feasible because so much depends on the **culture** of the company and the **change agents** who lead the effort.
2. To manage effectively in today's environment, companies should make a **formal, dedicated effort** to identify all their **significant risks**.
3. **Various techniques** are available to identify risk, and once identified, the process of identification should be **dynamic and continuous**.
4. Risks should be ranked on some **scale** that captures their **importance, severity, or dollar amount**.
5. Risk should be ranked on some **scale of frequency of probability**.
6. Measure **financial risk** with the most sophisticated and relevant tools available, such as **VAR and stress testing**.

<sup>8</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# Lessons learned<sup>10</sup>

7. **Develop sophisticated tools and measures** to meet the organisation's needs and that management can easily understand.
8. Know your **company's** and your **shareholders' appetite for risk**.
9. Apply **more rigour to measuring nonfinancial risks** whenever possible.
10. Companies are choosing **various combinations of acceptance, transfer, and mitigation** to manage risk.
11. Decisions regarding control (an application of mitigation), acceptance, and transfer are **dynamic** – they must be **continuously re-evaluated**.
12. Seek **creative solutions** and **transfer risk where economic opportunities exist**.

<sup>10</sup>Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# Lessons learned from case studies<sup>11</sup>

13. Organisations should adopt an **enterprise-wide view** of risk management.
14. **Consultants**, if they are used, should **supplement**, not replace, senior management involvement in the risk management effort.
15. Successful companies are good at managing silos of risk. Enterprise-wide risk management offers them **more effective risk management** at potentially **lower costs**.
16. **Making risk consideration** a part of the decision-making process is an essential element to enterprise-wide risk management.
17. Risk management **infrastructures vary in form** but are essential to driving throughout the organisation the idea that decision makers should consider their risks.
18. A prerequisite for implementation of enterprise-wide risk management is the **commitment of one or more champions at the senior management level**.

<sup>11</sup> Barton. T., Shenkir, W., Walker, P., Making Enterprise Risk Management Pay Off.

# Summary

- Enterprise Risk Management (ERM);
- Establishing a risk management culture;
- Leadership, management and commitment;
- Interdependency between policy, goals, reward and sanction;
- Methodologies, processes, and outputs;
- Communication and consultation;
- Training and development;
- Integrating quantitative and qualitative elements of risk management.

We trust you enjoyed participating in the journey of risk management. All the best for the exam!