Course Outline and Structure

• Week 1 – Security Governance
• Week 2 – Managing Security in the organisation
  • Risk Management
• Week 3 – Risk management
  • Breaches, threats, vulnerabilities
• Week 4 – IS security
  • access controls
• Week 5 – IS Security
  • Computer forensics
• Week 6 – The impact of e-commerce on the organisation
  • The role of e-security
• Week 7 – Security over the internet
• Week 8 – Security as a critical business function
  • Designing a Secure System
  • Is this achievable?
• Week 9 – Risk Management Part 4
  • Security policies and procedures
• Week 10 – Business continuity plans
  • Disaster recovery
• Week 11 – Security standards, Privacy and law
• Week 12 – Current issues and future trends
• Week 13 – Revision and exam preparation
The Problem
The Problem – The Coverage

Business Continuity in the Press

If an avian flu pandemic breaks out, the WHO believes that the scale of infection might be considerably greater than it was with SARS, which infected 8,096 people and killed 774 in 2003.

“A survey of 430 organizations revealed that of the 138 respondents who could put a figure on losses, 38% said application downtime costs them between £55,000 and £550,000 an hour, with 4% saying it was even more expensive than that.

“94 percent of businesses that experience a disaster are out of business within 2 years.”

According to Gartner Inc, 70% of companies that suffer a major IT disaster without a valid recovery plan, fail within the next year. Of those that do survive, only 10% make a full recovery.

90% of businesses that lose data from a disaster are forced to shut down within 2 years of the disaster.

43% of companies who have a business continuity plan do not test it annually to ensure it works.

“In a recent survey of the Top 5 issues that most concern IT decision makers, ‘Disaster Recovery and Business Continuity Planning’ came in at number 4.”

“85% of organizations that did not have a valid recovery plan in place as of September 11, 2001, failed to recover within two years.”

“94 percent of businesses that experience a disaster are out of business within 2 years.”

“43 percent of businesses experiencing a disaster never reopen, and 29 percent of those that do reopen close within two years.”

“43 percent of businesses experiencing a disaster never reopen, and 29 percent of those that do reopen close within two years.”

“‘85% of organizations that did not have a valid recovery plan in place as of September 11, 2001, failed to recover within two years.”

“Two out of five businesses do not survive a catastrophic blow to their computer systems and data.”

“43 percent of businesses experiencing a disaster never reopen, and 29 percent of those that do reopen close within two years.”
The Answer....
Key Definitions

- **Disaster** - An unplanned outage of sufficient duration to cause unacceptable loss to an organisation

- **Business Continuity Planning** - The process that utilises prevention and crisis management as well as alternate resources and procedures to sustain minimum required business functionality during a crisis. In many cases, prior to IT recovery
Business Continuity (BC) has historically been viewed as an Information Technology effort, with minimal input (or none at all) from Business Process owners. Recent events have proven this to be a defective planning model.

Minimizing Business Continuity risks requires thorough planning! Ensure you have gathered all the business requirements before continuing!

Business Continuity (BC): The process which utilizes prevention and crisis management as well as alternate resources and procedures to sustain minimum required business functionality during a crisis. In many cases, prior to IT recovery.

Disaster Recovery (DR): Provides the technical ability to maintain critical services in the event of any unplanned incident that threatens these services or the technical infrastructure required to maintain them.

High Availability (HA): Ability to automatically switch to alternate resources when a portion of the system is not or cannot remain functional.
Business Continuity – What is it?

Business Continuity Management is concerned with **managing risk to ensure that, at all times, an organisation can continue operating to a pre-determined minimum level.**

**Business Continuity includes:**

- Security goals
- Risks
- Levels of authority
- How to address security breaches
- Protect people and information
- Set the rules for expected behaviour by users, system administrators, management, and security personnel
- Authorise security personnel to monitor, probe, and investigate
- Define and authorise the consequences of violation
- And more…

**Business Continuity – Is MORE than protecting computers!**
Business Continuity

Business Continuity Management involves…. 

- **assessing** and then reducing the risk as far as possible,
- **planning** for the resumption of key business processes should a risk materialise and a business disruption actually occur, and
- **testing** those plans on a regular basis.

It is not only about **IT systems** but includes other physical assets such as people, office space and critical documents.

Business continuity management is known by many names including:
- business continuity planning
- disaster recovery planning
- business recovery planning
- business resumption planning
- crisis management
- contingency planning.

Business disruption incidents include:
- Environmental disaster: Fire, flood, earthquake etc.
- Acts of terrorism
- Loss of Utilities & Services
- Systems or Equipment Failure
- Information Security Breach
- Malicious Damage
- Civil protest/unrest
- Disruptions in 3rd Parties and Business Partners.

Business Continuity – Is MORE than protecting computers!
Challenges and Observations

• In BIA it is difficult to break through parochial and departmental view on what is critical and most important.

• In disaster scenarios, changing mindset from ‘normal operations’ to ‘recovery and contingency’.

• Requirements (RTO and RPO) must be balanced by business impact (cost of non-availability) and cost of solution. This makes the method an iterative process balancing requirements, cost, schedule etc.

• Prerequisite for good BIA basis is decent value-chain, business process, system architecture and business to system mapping. If this does not already exist it can be a huge undertaking. Our amount of reuse in this area is not good.
Complexity facing BCP/DR Integrators

Sounds Good....?

So How Do I Build It?
Business Continuity Planning – The process

Overview

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   - A. Risk Assessment
   - B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

- 1. Define objectives and assumptions
- 2. Gather facts and analyse requirements
  - Risk Assessment
  - Business Impact Assessment
- 3. Design the strategies
- 4. Create the plan
- 5. Implement the plan
- 6. Test the plan
- 7. Review/Update/Maintain the Plan

Remember: Be aware of the threats! Yes – It can happen to you.
Define Objectives and Assumptions

(1) Define objectives and assumptions

- Draft assumptions on business critical IT services/ systems
- Get high-level overview on IT determinants to deliver that services
- Assess threats, likelihood and draft impact
- Set initial IT Continuity Objectives & Guidelines
- Identify key individuals
- Identify the objectives of the organisation
  - What does the organisation want to protect?
  - What is the scope of the business continuity project?
  - What are any current assumptions the organisation may have?
  - What are the key strategies of the organisation?

Key Questions:
- What data is important?
- Where is the data stored?
- What are my key business critical processes?
- What are my key physical assets?
- How long can my business survive without these services?
- What will the business impacts be?
- What people, processes, infrastructure do I need in place to recover?

If the organisation can’t answer these questions – there is a BIG problem!
Key Questions:

- Will business operations stop if a particular operation fails?
- How much lost revenue will be incurred per each hour of downtime?
- How will I support my customer base?
- How long can the systems go down before I close my business?
- Who will co-ordinate and manage the recovery operations?
- What will the business impacts be?

Your company could go out of business…

Remember: If your company is gone… SO IS YOUR JOB!
Business Continuity – The Process

Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

(2) Risk Assessment

- Determine business continuity risks
- Rank risks by probability and impact

- Good practice considerations on effective controls against identified risks (the wished for status)
- Checks for
  - assessing availability of controls in place
  - assessing effectiveness of controls in place
  - assessing the potential impact of an incident
  - assessing the likelihood of the impact

If the organisation can’t answer these questions – there is a BIG problem!
Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/ Maintain the plan

(2) Business Impact Assessment

- Draft assumptions on business critical IT services/systems
- Get high-level overview on IT determinants to deliver that services
- Assess threats, likelihood and draft impact
- Set initial IT Continuity Objectives & Guidelines

Identify what processes are important to the business

Identify RTO and RPO objectives

Recovery Time Objectives (RTO): Is the amount of time an organisation is willing to wait before recovering their systems/processes

Recovery Point Objectives (RPO): Recovery Point is the point in time to which systems and data must be recovered after an outage as determined by the Business Unit (BIA)
Business Continuity – The Process

Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

<table>
<thead>
<tr>
<th>Impact Category Impact</th>
<th>Strategic Performance</th>
<th>Brand damage</th>
<th>Regulatory</th>
<th>Management effort and technical policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Non</td>
<td>Low</td>
<td>Medium</td>
<td>Elevated</td>
</tr>
<tr>
<td>Determination of Impact Rating</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non Financial Impacts</td>
<td>Complaints from small number of customers Internal impact only</td>
<td>Complaints from customer base Adverse customer comments</td>
<td>Adverse local/regional media coverage Adverse comments in press</td>
<td>Short term adverse national media coverage Sustained press coverage Intervention by Parent Company</td>
</tr>
</tbody>
</table>

Identify what processes are important to the business
## Business Impact Assessment

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   - A. Risk Assessment
   - B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/ Maintain the plan

### Determination of Impact Rating

<table>
<thead>
<tr>
<th>Non Financial Impacts</th>
<th>Non</th>
<th>Low</th>
<th>Medium</th>
<th>Elevated</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brand damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management effort and technical policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Non Financial Impacts

- **Strategic Performance**
- **Brand damage**
  - Complaints from small number of customers
  - Internal impact only
- **Regulatory**
  - Cautioned for minor breaches
- **Management effort and technical policy**
  - Repeated caution for minor breaches
  - Focused audit / investigation by regulator
  - fines and other possible sanctions
  - Area closed

**Identify what processes are important to the business**
Business Continuity – The Process

Design the strategies

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

(3) Design the Strategies

- Identify recovery options
- Undertake cost/benefit analysis
- Recommend continuity strategy

Time and cost effective ‘displacement’ solution
High level overview of Business recovery time objectives
Solution met cost and time requirements (cost vs benefit analysis)

Prevention Strategy  Mitigation Strategy  Recovery Strategy

- Backup / redundant resources to avoid incidents
- Trained employees
- Detailed change management process
- Redundant utilities and hardware
- Adequate fire suppression
- Early warning detection
- Contractual agreements with vendors
- Detailed business continuity plan
- Work around solutions
- Mirrored data and documents
- Documented and tested business recovery plan
- Responsive vendor relationships
- Knowledgeable employees
- Predefined assets, prearranged assets, or continuous availability
Business Continuity – The Process

Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

(3) Create the plan

IT management should ensure that a written plan is developed containing the following:
- Guidelines on how to use the continuity plan
- Emergency procedures to ensure the safety of all affected staff members
- Response procedures meant to bring the business back to the state it was in before the incident or disaster
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster
- Procedures to safeguard and reconstruct the home site
- Co-ordination procedures with public authorities
- Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media

DEVELOP THE STRATEGY

Evaluate alternative approaches to provide business continuity:
- Develop options for protecting critical processes and assets
- Select cost-effective combination of Risk Reduction projects, Recovery Arrangements and Recovery Plans for business processes and supporting resources

- Make sure the following things have been included:
  - Look at the questionnaire!

ISACA – COBIT Control Objectives
What

- A recovery script is a document that provides step-by-step instructions about:
  - The process required to recover the system
  - Who will complete each step
  - The expected time for long steps
  - Dependencies between steps

Why

- A script is necessary because it helps you:
  - Develop and use a proven series of steps to restore system
  - Prevent missing steps
  - Missing a critical step may require restarting the recovery process from the beginning, which delays the recovery.
  - If the primary recovery person is unavailable, a recovery script helps the backup person complete the recovery.

Recovery Process

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

- To reduce recovery time, define a process by:
  - Completing as many tasks as possible in parallel
  - Adding timetables for each step

Major Steps

1. During a potential disaster, anticipate a recovery by:
   - Collecting facts
   - Recalling the latest offsite tapes
   - Calling all required personnel
   - Preparing functional organizations (sales, finance, and shipping) for alternate procedures for key business transactions and processes.

Recovery process continued

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

• 2. Minimize the effect of the disaster by:
  – Stopping all additional transactions into the system
  – Waiting too long could worsen the problem
  – Collecting transaction records that have to be manually re-entered

• 3. Begin the planning process by:
  – Analysing the problem
  – Fitting the disaster to your predefined scenario plans
  – Modifying the plans as needed

• 4. Define when to initiate a disaster recovery procedure.
  – What are the criteria to declare a disaster, and have they been met?
  – Who will make the final decision to declare a disaster?
Recovery process continued

- 5. Declare the disaster.
- 6. Perform the system recovery.
- 7. Test and sign off on the recovered system.
  - Key users, who will use a criteria checklist to determine that the system has been satisfactorily recovered should perform the testing.
- 8. Catch up with transactions that may have been handled by alternate processes during the disaster.
  - Once completed, this step should require an additional sign-off.
- 9. Notify the users that the system is ready for normal operations.
- 10. Conduct a postmortem debriefing session.
  - Use the results from this session to improve your disaster recovery planning.

A good implementation process will consider the following:

- Awareness and training
  - BCM becoming an integral part of the organization’s strategic and day-to-day management ethos;
  - Who needs to be trained?
  - What do they need to be trained in?
  - Distribute documentation!!

- Communication
  - Communicate the plan to all areas of the business
  - Let people ask questions (keep them informed)
### Business Continuity – The Process

#### Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   - A. Risk Assessment
   - B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

---

**Test the plan**

- Essential!
- A plan is useless without testing it
- Different types of tests needed for different scenarios
- Must always have executive management support

<table>
<thead>
<tr>
<th>Test type</th>
<th>Activities</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Desktop review                     | Normally conducted as one of the first plan 'tests', it involves a physical examination and review of the plan documentation. Aims to ensure that:  
  - Plan document is complete and relevant to the expressed business needs (operational and strategic).  
  - The relevance and currency of the risk assessment, business impact assessment and continuity plan are tested.  
  - Inconsistencies in logical flow, resources allocations or conflict between individual plans are recognised. | • Inexpensive and relatively easy to organise.  
• Allows a rapid test to be undertaken on completion of the plans. |
| Desktop scenario test              | Involves a desktop walkthrough of the plan(s), with discussion guided by the use of one or more potential scenarios.  
The activities are based around a series of questions and answers relating to the deployment of the plans in response to changing issues in the scenarios. | Has similar benefits to the ‘desktop review’, with the additional advantage that it requires more challenging thinking from the participants. However, it does require a more significant commitment in time and skills to conduct. |
| Notification and call-out  
communications test                   | Activities are based around the verification of the accuracy, currency and utility of notification and call-out lists, call out trees (who you have to call) and deputised positions. | Tests notification and call-out procedures. Provides a real time validation of individuals’ ability to respond to the first (and crucial) stage of plan activation. |
| Live scenario tests                | Can be conducted as a limited activation (narrow specific scenario and/or targeted areas of the organisation) up to a full scale activation of all continuity arrangements for the organisation. | Such testing provides the most robust testing (and training) of the plan. However, it takes significant time and resources to plan for and conduct. It may also provide a major distraction from normal operations for the organisation. Provides a robust means of testing the integration and interaction of the suite of response plans. |
| Business recovery tests            | Involves the closing down or removal of access to infrastructure or resources and test the capability of recovery measures. | Can involve significant disruptions to the business, this can be minimised by holding such tests out of hours. |

Business Continuity – The Process

Define Objectives and Assumptions

1. Define objectives and assumptions
2. Gather Facts and analyse requirements
   A. Risk Assessment
   B. Business Impact Assessment
3. Design the strategies
4. Create the plan
5. Implement the plan
6. Test the plan
7. Review/Update/Maintain the plan

(3) Maintain the plan

- Essential!
- A plan is useless without testing it
- Different types of tests needed for different scenarios

<table>
<thead>
<tr>
<th>Maintenance</th>
<th>Plans are revised on a regular basis to ensure that content reflects current risks, priorities, functions, personnel responsibilities and resource requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage maintenance of the plan and program as a regular management cycle (Figure 3).</td>
<td></td>
</tr>
<tr>
<td>Conduct regular audits of:</td>
<td></td>
</tr>
<tr>
<td>• Business continuity management process.</td>
<td></td>
</tr>
<tr>
<td>• Plans.</td>
<td></td>
</tr>
<tr>
<td>• Testing regimes.</td>
<td></td>
</tr>
<tr>
<td>• Training processes.</td>
<td></td>
</tr>
<tr>
<td>Conduct an ongoing review and evaluation of the risk environment.</td>
<td></td>
</tr>
<tr>
<td>Conduct a regular review of the BIA, Resource Requirements and Strategies.</td>
<td></td>
</tr>
<tr>
<td>Conduct a regular review of the contracts of all third parties contributing to plan requirements.</td>
<td></td>
</tr>
<tr>
<td>Subsequent to any activation of the plans, conduct post-implementation reviews and audits of the responses.</td>
<td></td>
</tr>
</tbody>
</table>

But is it worth it?
Security: The benefits

... costs vs benefits

<table>
<thead>
<tr>
<th>Costs</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis &amp; Business Impact Assessment</td>
<td></td>
</tr>
<tr>
<td>Very time consuming. It is very subjective and often best practice is not ‘perfect’</td>
<td></td>
</tr>
<tr>
<td>Contingency Costs</td>
<td>Cost Savings</td>
</tr>
<tr>
<td>Contingency costs must be weighed against the downtime costs. Very subjective!</td>
<td></td>
</tr>
<tr>
<td>Professional Services</td>
<td>Improved Productivity</td>
</tr>
<tr>
<td>Most large organisations cannot do this alone. Auditors/consultants - $$$$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It is a competitive advantage if you can ensure that your operations will be around if there is a disaster. Organisations can potentially ‘win’ clients through uptime requirements.</td>
</tr>
<tr>
<td></td>
<td>Reduced Security Incidents</td>
</tr>
<tr>
<td></td>
<td>A good Business Continuity Plan is one that is NEVER enacted!!</td>
</tr>
</tbody>
</table>

Is it worth it? I believe so....
Business Continuity & Disaster Recovery

• Where else can I get information?
  – Free publications:
    • Disaster Recovery Journal
    • Contingency Planning & Management
  – Web Sites:
    • www.drj.com
    • www.contingencyplanning.com
    • www.globalcontinuity.com
    • www.recovery.sungard.com
    • www.disaster-resource.com
    • www.fema.gov
    • www.isaca.org (COBIT)

• Online Data security email
  – CSOonline.com.au

• Disaster Strategies for Record Keeping

References:
• Slide 27 + 28 – Taken from:

• Slide 21 – Taken from:

• Foster, S. (2004). IMS5002 slides – disaster recovery
Questions?