### Course Outline and Structure

- **Week 1 – Security Governance**
  - Risk Management
  - Breaches, threats, vulnerabilities
  - Access controls
- **Week 2 – Managing Security in the organisation**
  - Computer forensics
  - Business continuity plans
- **Week 3 – Risk Management**
  - Breaches, threats, vulnerabilities
  - Access controls
- **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**
- **Week 11 – Security standards, Privacy and law**
- **Week 12 – Current issues and future trends**
- **Week 13 – Revision and exam preparation**

### The Problem

Over half of IT and business executives interviewed report that IT spending on security and business continuity at their organisation has increased in the last 12 months.

*Source: IDC, July 2004*

Gartner Group, October 2001

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.

### Business Continuity in the Press

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.

*Computer Weekly; April 16th 2004*

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.*

*43 percent of businesses experiencing a disaster never reopen, and 29 percent of those that do reopen close within two years* (U.S. Department of Labor)

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.

*85% of organizations have altered their BC plans since September 11.*

Every five years, 20% of companies will suffer a major disruption through fire, flood or storm, power failures, terrorism, or hardware/software failures. Of those companies which do not have a Business Continuity Plan, 80% fail within 13 months of such an incident. Those who successfully restore their business have seen the company value rise.

*Source: Business Continuity Institute*

Are you worried…!? You should be…

- 85% of businesses that lose data from a disaster never reopen, and 29% of those that do reopen close within two years (U.S. Department of Labor)
- Two out of five businesses do not survive a catastrophic blow to their computer systems and data (Gartner Group)
- 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
The Answer…

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.

Key Definitions

Business Continuity/Disaster 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!

High Availability (HA)

Ability to automatically switch to alternate resources when a portion of the system is not or cannot remain functional.

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.

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 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
- Emergency 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
- Physical Damage
- Malicious Damage
- Civil protest/unrest
- Disruptions in 3rd Parties and Business Partners.

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

Plan Documentation
Impact Assessments

Recovery Strategies
Incident Response Team
Plan Testing
Data Backup
Evacuation Plans
Crisis Communications

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
   - 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

Business Continuity – The Process

Define Objectives and Assumptions

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.

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!

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!

Remember: If your company is gone... SO IS YOUR JOB!

Key Questions:

- 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?
- Were the key assumptions you had in the correct direction?
- 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!

Remember: If your company is gone... SO IS YOUR JOB!

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 a single event
  - Assessing the likelihood of the impact

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

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 and assumptions
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>Category</th>
<th>Non Financial Impacts</th>
<th>Financial Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Medium</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>High</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Recovery Point Objectives (RPO): Recovery Point is the point in time to which systems and data must be recovered.

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

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

Prevention Strategy Mitigation Strategy

- Backup/redundant infrastructure
- Trained employees
- Detailed change management processes
- Recovered utilities and services
- Adequate IT support

Early warning detection
- Contingency
- Contracts with reputable vendors
- Created business continuity plan
- Work around solutions
- Misplaced data and documents

Recovery Strategy

- Documented and tested business recovery plan
- Assurance under management
- Knowledgeable employees
- Prearranged assets
- Prearranged agreements

Identify what processes are important to the business
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

Develop the Strategy

• 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

Evaluate alternative approaches to provide business continuity:
• Make sure the following things have been included:
  – Look at the questionnaire!

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

Recovery Process

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

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

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.

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

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

Major Steps

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
   • Modifying the plans as needed

3. Begin the planning process by:
   • Analyzing the problem
   • Filling 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.

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

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)

Implementation is about communication and involvement!

Test the plan

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

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

Maintain the plan

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

Security: The benefits

... costs vs benefits

Benefits

- Reduced Security Incidents
- A good Business Continuity Plan is one that is NEVER enacted!!
- Increased Opportunities
  - It is a competitive advantage if you can ensure that your operations will be around if there is a disaster. Organizations can potentially ‘win’ clients through uptime requirements.
- Improved Productivity
  - With new re-active and proactive controls and processes – potential for increased productivity as organizations move to becoming ‘security aware’.
- Cost Savings
  - How much is your organization worth? If it is worth something – it is often worth protecting.

Costs

- Very time consuming.
- It is very subjective and often best practice is not ‘perfect’
- Contingency Costs
  - Contingency costs must be weighed against the downtime costs. Very subjective!
- Professional Services
  - Most large organizations cannot do this alone.
  - Auditors/consultants – $$$$

... costs vs benefits

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.isaca.org (COBIT)
  - Online Data Security email
    - CISOnline.com.au
  - Disaster Strategies for Record Keeping
    - www.recovery.sungard.com
    - www.isaca.org (COBIT)

Questions?