# Disaster recovery


CISSP®
**Diarmuid Ó Briain**
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

# Business Continuity Planning (BCP)

- The creation and validation of a practised logistical plan for how an organisation will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.
- BCP is working out how to stay in business in the event of disaster.
- BS 25999 - Business Continuity Management (BCM) and acted as the base for the ISO/IEC 27000-series.

# Business Continuity Lifecycle

# Business Continuity Strategy

- BC Strategies will normally be determined by available budget, either:
  - Accept the risk.
  - Accept the risk but get a BC partner who can help in the event of an incident.
  - Reduce the risk.
  - Reduce the risk but get a BC partner who can help in the event of an incident.
  - Reduce the risk adequately that a BC partner is not necessary.

# Business Plan

- **Develop a Business Plan**
  - Now that risks have been identified and a strategy to deal with them decided a full business plan will be needed. Such a plan should be simple because employees will need to act quickly and decisively after an incident.
- **Rehearse Plan**
  - There is a military maxim that applies at this stage "*Train hard, fight easy*". The plan must be rehearsed so that employees will know exactly what to do in the event of an incident.

# Business Continuity Planning Process

# Project scope and planning

- Structured analysis of the whole business from the perspective of crisis management.
- Appointment of a BCP team with SMT approval. The team should consist of:
  - Representation from each department with responsibility for the company core systems
  - Representation from support departments
  - IT personnel with technical expertise in the core systems
  - Information Security officer
  - Legal representation with knowledge of the contractual requirements that may impact the plans
  - SMT representative
- Identification of all resources available to the team for BCP.
- Understanding of the regulatory and legal situation that governs the companies response to an major event requiring a BC response.

# Business Impact Assessment (BIA)

- Identify the key business processes and technology components that would suffer the greatest financial, operational, customer, and/or legal and regulatory loss in the event of a disaster.
- The BIA identifies all the critical resources, systems, facilities, records, etc., that are required for BC.
- For each entry in BIA identify the time it would take to recovery such resources.

# Business Impact Assessment (BIA)

- For each urgent function, two values are then assigned:
  - ***Recovery Point Objective (RPO)*** - the acceptable latency of data that will be recovered
  - ***Recovery Time Objective (RTO)*** - the acceptable amount of time to restore the function
- The RPO must ensure that the ***Maximum Tolerable Data Loss (MTDL)*** for each activity is not exceeded. The RTO must ensure that the ***Maximum Tolerable Period of Disruption (MTPD)*** for each activity is not exceeded.

# Risk Analysis

- Recovery requirements are now defined, so an identification and documentation of potential risks should be undertaken.
- Identify the risks which gives the opportunity to review each and define a specific set of work instructions.
  - Terrorism
  - Cyber attack
  - Sabotage
  - Disease
  - Fire
  - Flood
  - Utility outage
  - .....

# Assessment of Likelihood

- Now that we have identified risks what is the likelihood of these occurring?
- For each identified risk produce an ***Annualised Rate of Occurrence (ARO)***.
  - How often is it likely that this event will occur in any year?

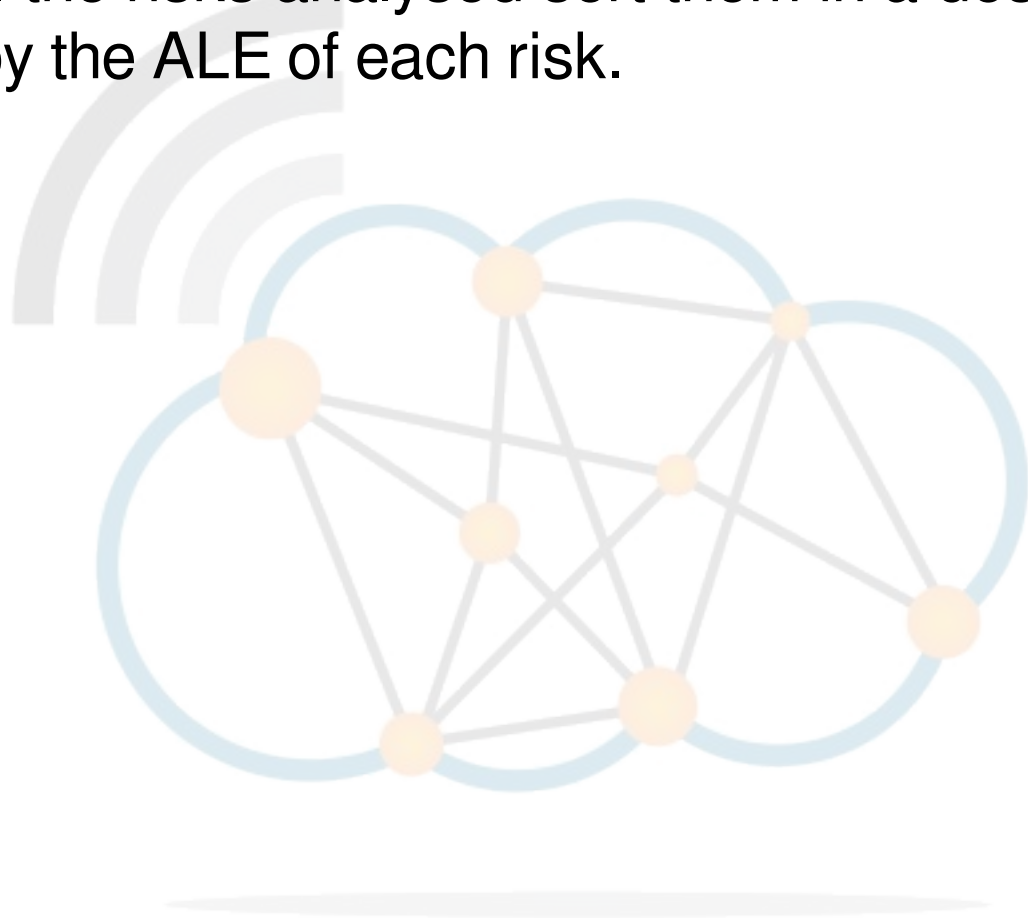
# Assessment of Impact

- Should an identified risk actually occur what is the likely impact of the event on the business?
- Determine the ***Exposure Factor (EF)*** to the business as a percentage of the ***Assets Value (AV)*** and from these figures calculate the ***Single Loss Expectancy (SLE)***:
  - SLE = AV x EF

- From the earlier ARO figure, it is a simple matter to calculate the Annualised Loss Expectancy (ALE):
  - ALE = SLE x ARO

# Prioritisation of Resources

- Taking all the risks analysed sort them in a descending list ordered by the ALE of each risk.



# Continuity Planning

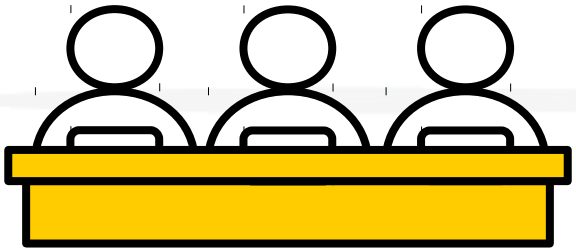
- **Strategic**: For each risk, is a BCP absolutely necessary.
- **Activity**:
  - People, workforce, skills and knowledge
  - Premises
    - Alternative Sites
  - Infrastructure
    - IT Backbone
    - Servers
    - Workstations
  - Information
    - Backup off site
  - Stakeholders partners and contractors
    - Alternative partners and contractors

# Documentation

- Continuity Planning Goals
  - “To ensure the continuation of the business in the event of an emergency”
- Senior Executive Statement
  - Statement  from the C-level management to indicate the importance of the BCP.
- Timetable
- Priority List
- Risk Assessment - BIA
- Records
- 'Action-on’ Emergency Incident
- Change process

# Group Exercise:
# Business Continuity and Disaster Recovery

- As CIO for a specialised Credit company that specialises in Cloud bases services to the Micro-loan market holding sensitive customer data that strictly cannot leave Uganda.
- The company currently operates a pair of High Availability (HA) Xen servers in a data centre in Nairobi and a private data centre in Kampala.
  - Develop a BIA for 3 key business processes and technologies.
  - Carry out a risk assessment and list 5 key risks.
  - Order the risks.
  - Describe the mechanism used to order the risks.
  - Assuming the only risks are the 5 identified and develop a short BCP for them.
  - Suggest a test regime for the BCP.



Thank you