Introduction

• Main goals of the Task Force

• The task force promotes the use of common standards and procedures for responding to computer security incidents. Common standards have great potential for reducing the time needed to recognise and analyse incidents, and then taking appropriate countermeasures.
Introduction

ISO 20000 – IT Service Management

ISO 27001 – Information Security Management

BS 25999 – Business Continuity Management
Introduction

• Who are Certification Europe?
• An independent, state accredited certification, inspection and training body
• Certify or inspect over 1,400 organisation, every year, with a client base of over 500 international clients
• We certify in the field of information security (ISO 27001), business continuity (BS 25999), IT Service Management (ISO 20000), Energy (EN 16001), Quality (ISO 9001), Environment (ISO 14001) and H&S (OHSAS 18001)
Introduction

ISO 20000 – IT Service Management
What is the relevance of ISO 20000?

- It is ‘the’ international standard for IT Service Delivery Management.
- Incident Management Vs Problem Management
  » 1\textsuperscript{st} one is ‘fix it and fix it quick’
  » 2\textsuperscript{nd} one is root cause analysis, impact analysis, problem resolution
What is the relevance of ISO 20000?

- **Capacity Planning**
  - Not just hardware & software, but resources, people, skills sets and competency

- **Change Management**
  - Not stopping immediate action
  - It is about recording the action taken, allowing follow-up analysis of change
  - Impact of change
  - Retrospective review and approval
  - Establishing mechanism for ‘roll-back’
  - Configuration management (CMDB)
ISO 27001 – Information Security Management
What is the relevance of ISO 27001?

• It is the standard for Information Security Management

• Personnel Security (think as a customer)
  » Screening team
  » Ensuring skill sets and competency
  » Staff – new starters, leavers and movers
What is the relevance of ISO 27001?

- Physical Security
  - Secure areas (CSIRT)
  - Access control
  - Sensitive system isolation (Governmental Confidential)
  - General monitoring of sensitive clients / dealing with sensitive incidents
  - Incident Response Team Room (‘War Room’)

What is the relevance of ISO 27001?

• Compliance
  » Legislation (e.g. forensic investigations & legal admissibility / cross-frontier investigations
  » Data Protection – incidents involving personal data & subsequent use by the team of that data
  » Acceptable Use Policies (Clients)
    • Aware of them?
    • If they are lacking then your own investigations may fail due to inadequate/absent Policies
Introduction

BS 25999 – Business Continuity Management
What is the relevance of BS 25999?

• The standard for business continuity management
• Incident Response & Incident Management
  » Heart of BCM – standard defines best practice
  » Ensures organisations continue operating to an acceptable level of service – not shut down
  » Learning from incidents
What is the relevance of BS 25999?

- Key personnel/skills and competencies within the CISRT Team
  - People factor
  - Ensuring continued availability of service (staff and infrastructure)
  - Communications
  - Continuity of the CISRT Team essential for ensuring continuity of the client/organisation in the event of an incident
  - It is all about you
Thank You

mbrophy@certificationeurope.com
www.certificationeurope.com