

ISO27001

Presented by Rick Jones
British Telecom



BT has 15 ISO27001 certificates

- Data Centres
- Security Operations
- Firewall & Security
- Internet Hosting
- Risk Management
- Security Policies
- Network Mgt
- Defence Systems
- Various contracts



ISO27001 certificates in progress

- 21 Century
Network
- Internet Hosting &
Data Centres
- MPLS Core
Network
- European & US
sites



How does BT use ISO27001 ?

To support all the services we offer:

- Managed Security Services
- Firewall and IDS management
- Secure networks
- Business continuity
- Operational Risk Management
- **And as an alternative for SAS70 audits**

- We are not just a Telco...

Why is ISO27001 important ?

- All potential new customers for managed services expect BT to demonstrate how it maintains security
- ISO27001 helps BT to position it's bids – **there is no better endorsement than to have customers see an independent auditor verify the strength of your internal security story**
- It shows customers you are serious about protecting their data

What commercial benefits has BT seen ?



What commercial benefits has BT seen ?

Contracts won:



NATO – To provide a computer emergency response



UK Government & European Commission – To provide various eGovernment services



Reuters network management



Pepsico network management & security services

How do you achieve ISO27001 ?

- First – agree the scope of the certificate
- Establish a security forum to own the process
- Produce an ISMS (Information Security Management System)
- Develop a security plan and some aims
- Develop an internal audit programme
- Analyse security events & incidents
- Gather evidence to show how each of the 133 controls is complied with

How do you achieve ISO27001 ?

- Carry out a risk assessment
- Develop some risk treatment plans
- Develop a method of measuring effectiveness
- Constantly review and improve data security
- Governance / evidence / show your workings !

ISO27001 has 133 controls

Which controls cause the most pain ?

- The ones with human involvement - because the technology is usually more reliable

How much pain is ISO27001 ?

How much pain is ISO27001 ? - a lot



Challenge 1 – Define the scope and assets

- People
- Processes
- Hardware
- Software
- Applications / systems
- Networks
- Buildings
- Contracts
- Data

Challenge 1 – Define the scope and assets

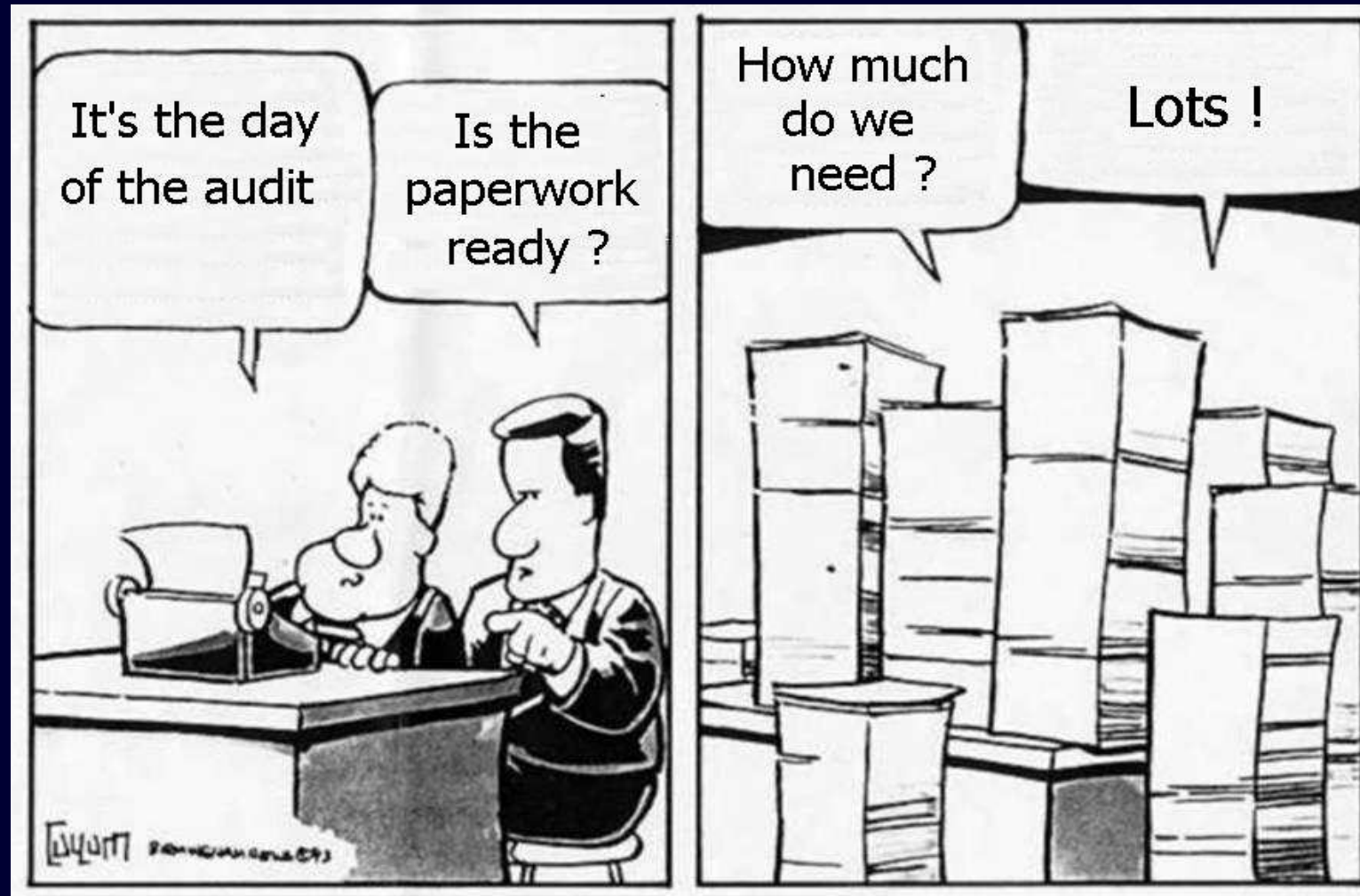
- People
- Processes
- Hardware
- Software
- Applications / systems
- Networks
- Buildings
- Contracts
- **Data – is the most important asset**

Challenge 2 – Gather the evidence

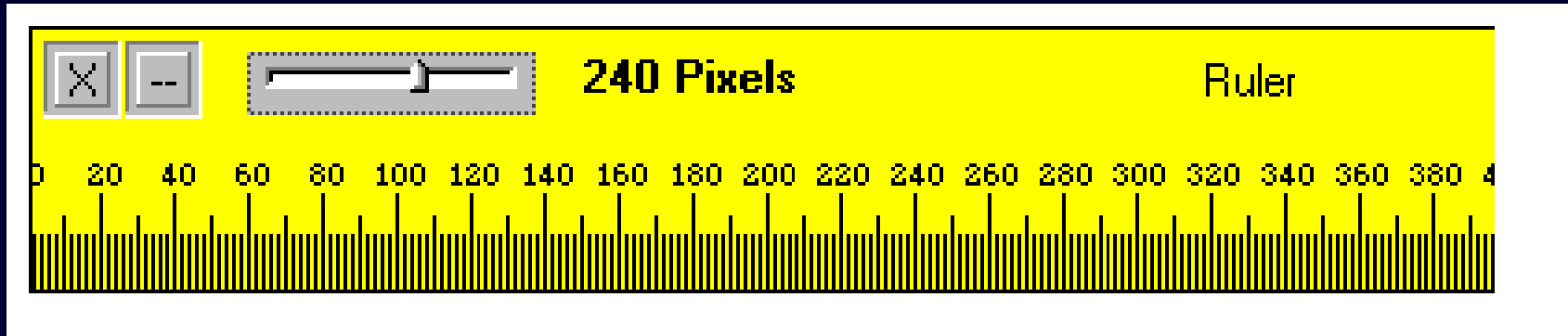
How much evidence ?

Challenge 2 – Gather the evidence

How much evidence - **lots**



Challenge 3 – How do you measure effectiveness ?



- Look for trends
- Measure compliance during audits
- Calculate the cost of security incidents
- Show how risks are being reduced

Challenge 4 – Data retention / data deletion

- Is data kept too long ?
- Is data deleted too soon ?
- Agree your approach to deleting data – and make sure this is documented
- Make sure you follow any contractual requirements for data retention

Implementing ISO27001 - some statistics

How many resources are needed ?

- From 0.5 to 1.0 person per site

How much time is needed ?

- Allow a minimum of 6 to 9 months

What about the future ...



ISO27002

A Code of Practice

ISO27003

Implementation
Guidance

ISO27004

Metrics

ISO27005

Risk Management

ISO27006

Accreditation Body
Guidelines

Thank you
Any questions ?

