What Became of the Conditions for Connection?

Jonathan Ashton and Miranda Llewellyn, OUCS

Agenda

- Motivation for ISBP
- Progress made so far
- Results of self-assessment
- ISBP 2010
- “Best” Practice and ISO 27001/27002

Motivation

Motivation

- Internal Audit - to assess whether the University's ICT was fit for purpose and to assess the quality of IT security across the Collegiate University

Motivation

- Internal Audit - to assess whether the University's ICT was fit for purpose and to assess the quality of IT security across the Collegiate University
- Result was the Conditions for Connection and Security of Information policies - both endorsed by PICT

Motivation

Motivation

- However.....

Motivation

- However.....
  - How would compliance be measured?

Motivation

- However.....
  - How would compliance be measured?
  - What to do about it?

Motivation

- However.....
  - How would compliance be measured?
  - What to do about it?
  - Some very specific and unhelpful policies:

Motivation

- However.....
  - How would compliance be measured?
  - What to do about it?
  - Some very specific and unhelpful policies:
    - "Any data of a confidential or critical nature, or for which unauthorised access would have a deleterious effect on the collegiate University (financial reputational or otherwise), or on any individual, must be encrypted at all times"

Motivation

- However.....
  - How would compliance be measured?
  - What to do about it?
  - Some very specific and unhelpful policies:
    - “Any data of a confidential or critical nature, or for which unauthorised access would have a deleterious effect on the collegiate University (financial reputational or otherwise), or on any individual, must be encrypted at all times”
    - 0b7bedef5ef3f1aeebca2d0bd2e17fca

Motivation

Motivation

- On a personal level....
  - Didn’t want auditors dictating policy
    - e.g. password expiry every 3 months

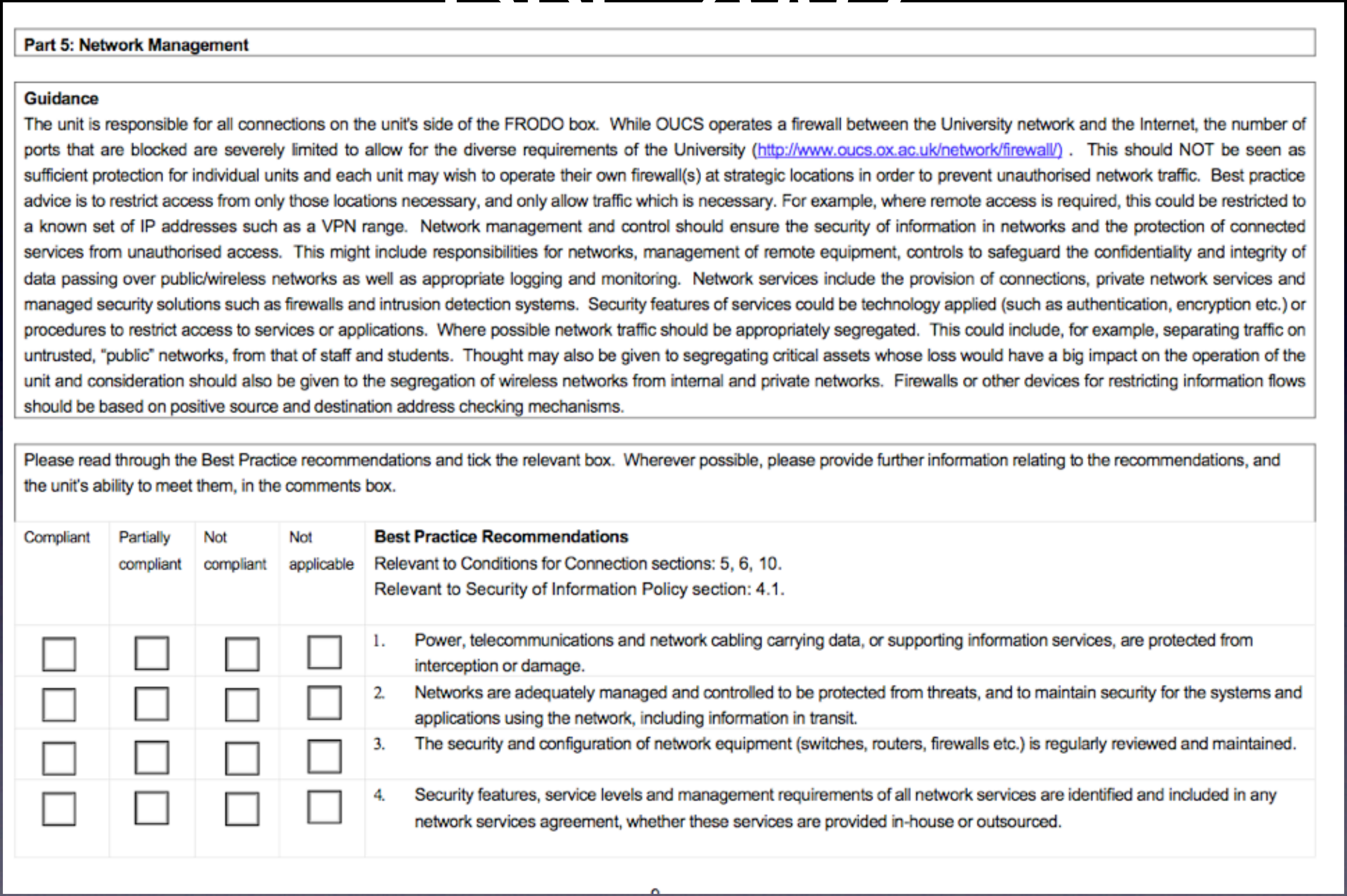
Motivation

- On a personal level....
  - Didn’t want auditors dictating policy
    - e.g. password expiry every 3 months
- From an OxCERT point of view we wanted to do something proactive rather than just responsive
  - Security as an enabler

ISBP 2009

- Produced set of 'Best Practice' guidelines
  - Conditions for Connection
  - Security of Information Policy
  - ISO/IEC 27002 code of practice
  - PICT requirement for self-assessment
  - Based on UCISA IS Toolkit
    - http://www.ucisa.ac.uk/ist

ISBP 2009



Part 5: Network Management

Guidance

The unit is responsible for all connections on the unit's side of the FRODO box. While OUCS operates a firewall between the University network and the Internet, the number of ports that are blocked are severely limited to allow for the diverse requirements of the University (http://www.oucs.ox.ac.uk/network/firewall/) . This should NOT be seen as sufficient protection for individual units and each unit may wish to operate their own firewall(s) at strategic locations in order to prevent unauthorised network traffic. Best practice advice is to restrict access from only those locations necessary, and only allow traffic which is necessary. For example, where remote access is required, this could be restricted to a known set of IP addresses such as a VPN range. Network management and control should ensure the security of information in networks and the protection of connected services from unauthorised access. This might include responsibilities for networks, management of remote equipment, controls to safeguard the confidentiality and integrity of data passing over public/wireless networks as well as appropriate logging and monitoring. Network services include the provision of connections, private network services and managed security solutions such as firewalls and intrusion detection systems. Security features of services could be technology applied (such as authentication, encryption etc.) or procedures to restrict access to services or applications. Where possible network traffic should be appropriately segregated. This could include, for example, separating traffic on untrusted, "public" networks, from that of staff and students. Thought may also be given to segregating critical assets whose loss would have a big impact on the operation of the unit and consideration should also be given to the segregation of wireless networks from internal and private networks. Firewalls or other devices for restricting information flows should be based on positive source and destination address checking mechanisms.

Please read through the Best Practice recommendations and tick the relevant box. Wherever possible, please provide further information relating to the recommendations, and the unit's ability to meet them, in the comments box.

Compliant	Partially compliant	Not compliant	Not applicable	**Best Practice Recommendations** Relevant to Conditions for Connection sections: 5, 6, 10. Relevant to Security of Information Policy section: 4.1.
□	□	□	□	1. Power, telecommunications and network cabling carrying data, or supporting information services, are protected from interception or damage.
□	□	□	□	2. Networks are adequately managed and controlled to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
□	□	□	□	3. The security and configuration of network equipment (switches, routers, firewalls etc.) is regularly reviewed and maintained.
□	□	□	□	4. Security features, service levels and management requirements of all network services are identified and included in any network services agreement, whether these services are provided in-house or outsourced.

ISBP 2009

- Went out to every unit within the University
- Accompanied by promotional workshops
- Received returns from 60 units
- Each of which received their own confidential report
- All other units received a generic report

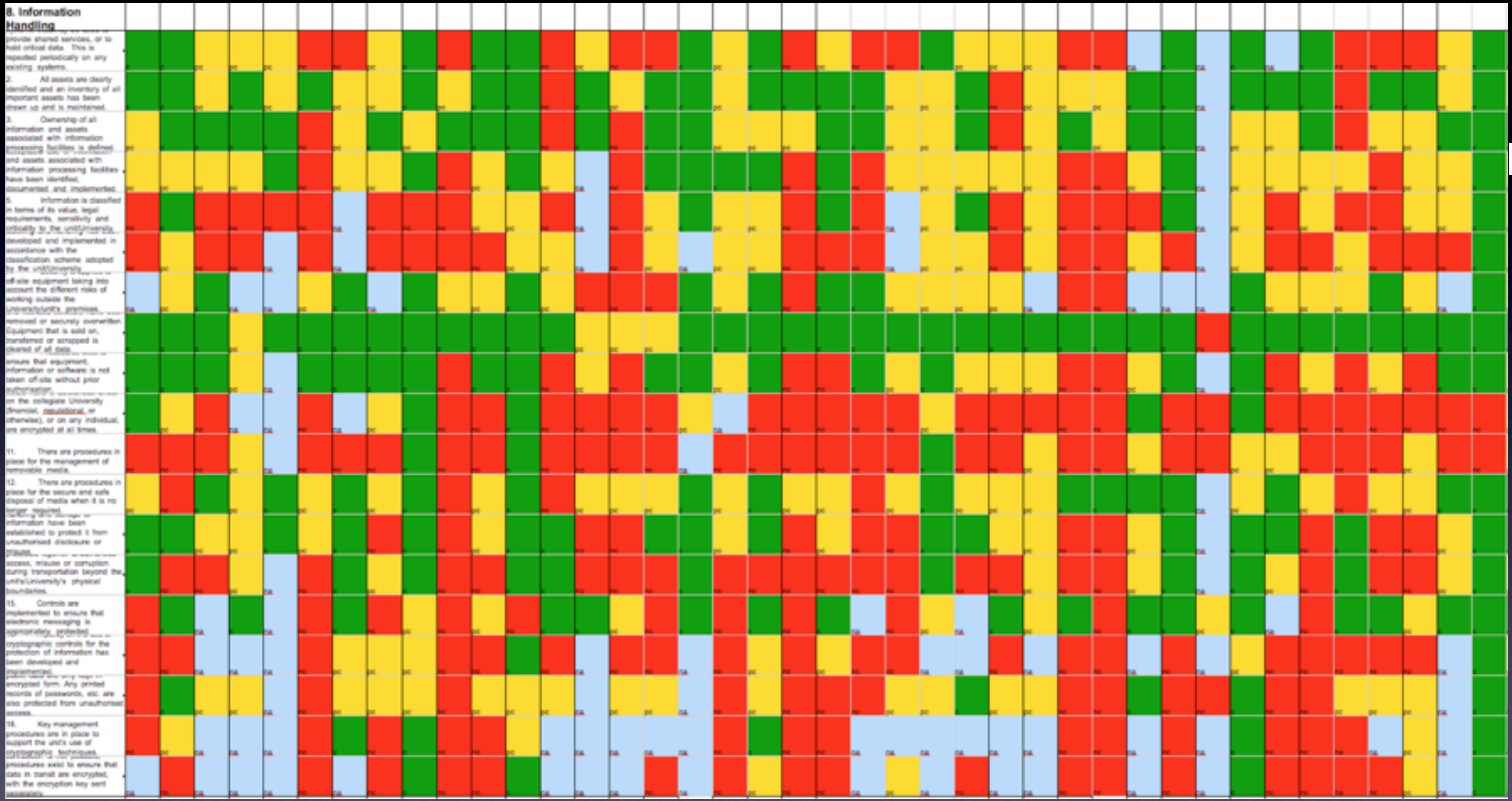
ISBP 2009 - Objectives

- Work towards an agreed set of desirable practices
  - Relied on Advisory Group and comments from ITSS
- See where assistance was needed
- ITSS to comment on the CfC and IS policies
  - Comments from ITSS
- Look at allocation of resources
  - Save duplication of effort

ISBP 2009 - Objectives

ces

m



8. Information Handling																																								
provide shared services, or to hold critical data. This is repeated periodically on any existing systems.	c	c	pc	pc	pc	nc	nc	pc	c	nc	c	c	nc	pc	nc	nc	c	pc	c	nc	pc	nc	nc	c	pc	pc	pc	nc	nc	na	c	na	c	na	c	nc	nc	nc	pc	c
2. All assets are clearly identified and an inventory of all important assets has been drawn up and is maintained.	c	c	pc	c	pc	c	pc	pc	c	pc	c	c	nc	c	pc	c	c	pc	c	c	c	c	pc	pc	c	nc	pc	pc	pc	c	c	na	c	c	c	nc	c	c	pc	c
3. Ownership of all information and assets associated with information processing facilities is defined.	pc	c	c	c	c	nc	pc	c	pc	c	c	c	nc	c	nc	c	c	pc	pc	pc	c	c	pc	pc	c	nc	pc	c	pc	c	c	na	pc	pc	c	nc	pc	pc	c	c
and assets associated with information processing facilities have been identified, documented and implemented.	pc	pc	pc	pc	c	nc	pc	pc	c	nc	pc	c	pc	na	nc	c	c	c	c	nc	c	nc	pc	pc	pc	pc	pc	nc	nc	pc	c	na	pc	pc	pc	pc	nc	pc	pc	c
5. Information is classified in terms of its value, legal requirements, sensitivity and criticality to the unit/University.	nc	c	nc	nc	nc	nc	na	nc	nc	nc	pc	pc	nc	na	nc	pc	c	pc	pc	nc	c	nc	na	pc	c	nc	pc	nc	nc	nc	c	na	pc	nc	pc	nc	nc	pc	pc	c
developed and implemented in accordance with the classification scheme adopted by the unit/University.	nc	pc	nc	nc	na	nc	na	nc	nc	nc	nc	pc	pc	na	nc	pc	na	pc	pc	nc	nc	nc	na	pc	pc	nc	pc	nc	nc	pc	nc	na	pc	nc	nc	pc	nc	nc	nc	c
off-site equipment taking into account the different risks of working outside the University/unit's premises.	na	pc	c	na	na	pc	c	na	c	pc	pc	c	pc	nc	nc	nc	c	pc	c	nc	c	c	pc	pc	pc	pc	na	nc	nc	na	na	na	c	pc	pc	pc	c	pc	na	c
removed or securely overwritten. Equipment that is sold on, transferred or scrapped is cleared of all data.	c	c	c	pc	c	c	c	c	c	c	c	c	c	pc	pc	pc	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	nc	c	c	c	c	c	c	c	c
ensure that equipment, information or software is not taken off-site without prior authorisation.	c	c	c	pc	na	c	c	c	c	nc	c	c	nc	pc	nc	c	c	pc	c	nc	nc	c	pc	c	pc	pc	pc	nc	nc	pc	c	na	c	nc	pc	nc	pc	nc	c	c
on the collegiate University (financial, reputational, or otherwise), or on any individual, are encrypted at all times.	c	pc	nc	na	na	nc	na	pc	c	nc	nc	c	nc	nc	nc	nc	pc	na	nc	nc	nc	nc	nc	pc	nc	nc	nc	nc	nc	c	nc	nc	c	nc	nc	nc	nc	nc	nc	nc
11. There are procedures in place for the management of removable media.	nc	nc	nc	pc	na	nc	nc	nc	c	nc	nc	c	nc	nc	nc	nc	na	nc	nc	nc	nc	nc	nc	c	nc	nc	pc	nc	nc	pc	nc	nc	pc	pc	nc	nc	nc	pc	nc	nc
12. There are procedures in place for the secure and safe disposal of media when it is no longer required.	pc	nc	c	pc	c	pc	c	pc	c	nc	pc	c	nc	pc	pc	pc	c	pc	c	pc	pc	nc	pc	c	pc	pc	pc	c	c	c	c	na	pc	c	pc	nc	pc	pc	c	c
information have been established to protect it from unauthorised disclosure or misuse.	c	c	pc	pc	c	pc	c	nc	c	nc	pc	c	c	nc	nc	c	c	pc	c	nc	pc	nc	nc	c	c	pc	pc	nc	nc	pc	c	na	c	c	nc	c	nc	nc	pc	c
access, misuse or corruption during transportation beyond the unit's/University's physical boundaries.	c	nc	nc	pc	na	nc	c	pc	c	nc	nc	c	c	nc	nc	nc	c	nc	nc	nc	nc	nc	nc	c	nc	nc	pc	nc	nc	pc	c	na	c	pc	nc	c	nc	nc	pc	c
15. Controls are implemented to ensure that electronic messaging is appropriately protected.	nc	c	na	c	na	nc	c	nc	pc	nc	pc	nc	c	c	pc	nc	c	nc	c	nc	c	na	nc	pc	na	c	pc	c	nc	c	c	pc	c	na	nc	c	c	pc	c	c
cryptographic controls for the protection of information has been developed and implemented.	nc	nc	na	na	na	nc	pc	pc	pc	nc	nc	c	nc	na	nc	nc	na	nc	pc	nc	pc	nc	nc	na	na	nc	na	nc	nc	na	nc	na	pc	nc	nc	nc	nc	nc	na	c
encrypted form. Any printed records of passwords, etc. are also protected from unauthorised access.	nc	c	pc	pc	na	nc	pc	pc	pc	nc	pc	pc	pc	na	pc	pc	na	nc	pc	nc	nc	nc	pc	pc	c	pc	pc	nc	nc	c	nc	nc	c	nc	nc	pc	pc	pc	na	c
18. Key management procedures are in place to support the unit's use of cryptographic techniques.	nc	pc	na	na	na	nc	c	nc	c	nc	nc	pc	na	na	na	na	na	nc	c	nc	nc	na	na	na	na	na	na	nc	nc	na	nc	na	c	nc	nc	nc	na	pc	na	c
procedures exist to ensure that data in transit are encrypted, with the encryption key sent separately.	na	nc	na	na	na	nc	na	nc	c	nc	nc	c	na	na	na	nc	na	nc	pc	nc	nc	na	pc	na	nc	na	na	nc	nc	na	nc	na	c	nc	nc	nc	nc	pc	na	c

- Save duplication of effort

ISBP 2009 - Results

- Observations:
  - In most areas compliance was pretty good
  - Not so good for ‘Information Handling’
  - Not simply an IT issue
  - Desire to keep the ICTF involved

ISBP 2009 - Results

- Recommendations:
  - Develop an Information Security Policy
  - Review ‘Best Practice’ guidelines
  - Develop an Information Security Toolkit
    - Sample policies
    - Documentation
    - Make use of existing resources etc.

ISBP 2009 - Results

- Recommendations:
    - Closer look at area of ‘Information Handling’
    - Scope possible future (centralised?) projects
        - e.g. encryption
    - http://www.oucs.ox.ac.uk/network/security/ISBP/

ISBP 2010 - Organisation

- Funding secured for 2 FTEs for 18 months
  - Post to be created within OxCERT
  - OxCERT to expand remit
  - Still driven by IS-AG
  - Miranda to continue in her role

ISBP 2010 - Objectives

- Scope - not just an IT issue
- Information Security Policy
- Redraft 'Best Practice' Guidelines
- Develop an IS toolkit
- Information Handling
  - Risk Analysis
- Recommended controls/future projects
- http://www.oucs.ox.ac.uk/network/security/ISBP/

ISBP 2010 - The Future?

ISBP 2010 - The Future?

- An opportunity for the ICTF

ISBP 2010

- Information Security Policy?
  - To define the University's IS objectives
  - Scope, roles and responsibilities
  - Available and communicated to all
  - 'What' not 'how'

ISBP 2010 - Critical Success Factors - 1

- Policy must be signed off
  - Demonstrate support at a high-level
  - To give ‘weight’

ISBP 2010 - Critical Success Factors - 2

- Correctly define scope and objectives
    - Representation from all user groups (ITSS, Administrators, HoDs, HR, users....)
    - Role of Advisory Group?
    - How to expand?

ISBP 2010 - Critical Success Factors - 3

- Defining and communicating areas of responsibility
  - Whose information is it anyway?
  - Responsibility for breaches

ISBP 2010 - Critical Success Factors - 4

- Security as an enabler
  - Must be desirable to achieve
  - Ensure the University/Unit meets their functional requirements

ISBP 2010 - Information Handling

- Start thinking about ‘how’
  - Identification of assets
  - Risk analysis
    - Different approaches
  - Appropriate controls

‘Best’ Practice and ISO 27001-27002

- Good starting point
- Internationally recognised - why re-invent the wheel?
- State ‘what’ not ‘how’
- Selective application
- External pressures (contractual requirements)
- Other Universities are implementing
- Useful for audit
- UCISA Information Security Toolkit

Why Care?

- Have achieved much with very limited resources
- An opportunity for the ICTF
  - To have a voice
  - To shape University policy
  - Deliver high profile project
- May just help YOU to meet YOUR objectives
- If WE don’t do this someone else will
  - i.e. auditors

Why Care?

- It may become a requirement even if you don’t realise it
  - e.g. if you provide services to those units where it is already a requirement
  - Ultimately we are one organisation
- It is also in our interests to protect our users’ data
  - High profile incidents can damage reputation
  - New powers of the ICO to impose fines

ISPB 2010 - Contacts

- http://www.oucs.ox.ac.uk/network/security/ISBP
- infosec@oucs.ox.ac.uk