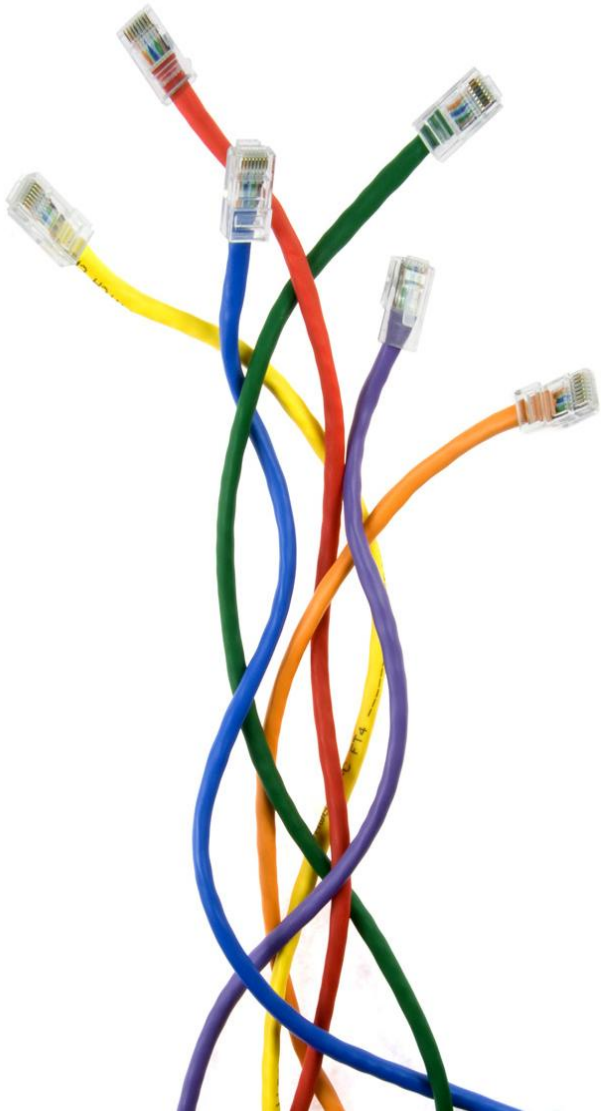
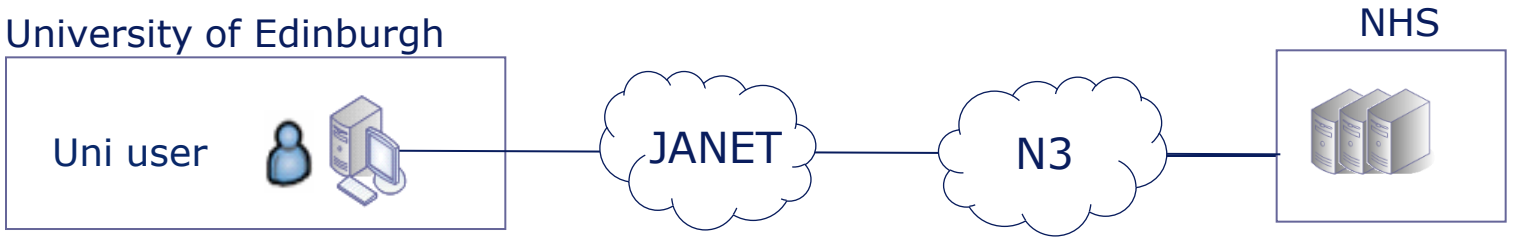
NHS HE Forum

16 October 2012

Colin Howarth



What do we want to achieve



Who

What

Why

Application

Data

NHS Board

Data Protection 7th Principle

- **Appropriate** technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

How do we work out what are appropriate measures

- Information Technology – Security Techniques -
- ISO27001: Information security management systems — Requirements
- ISO27002: Code of Practice for Information Security Management
- ISO27005: Information security risk management
- ISO27799: Health informatics — Information security management in health using ISO/IEC 27002

It is **not** the achievement of **one** person.

It **is** a process that can be managed by one person, used to capture the understanding and expertise of **many**.

Existing IA approaches

	NHS England	NHS Scotland	ISO	CESG/HMG IA
Organisational / policy / overarching	IGT and SoC	National security manual	ISO/IEC 27001 ISMS	SPF
Technical / architectural / control set	LCA	LCA	ISO/IEC 27002 Controls	Baseline Control Set

HMG IA – GPG 47 Accreditation process

- Accreditation is defined as a formal, independent assessment of an ICT system or service against its IA requirements, resulting in the acceptance of residual risk in the context of the business requirements and information risk appetite. This will be a prerequisite for approval to operate.

What is Accreditation?

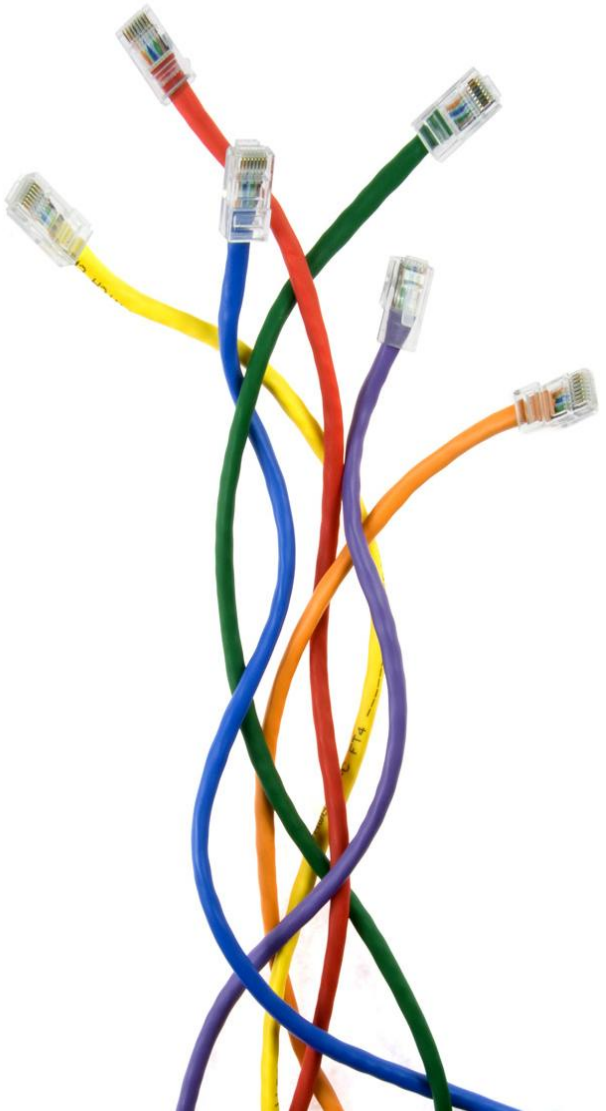
- The organisation must apply a structured risk management approach
- There are **no** prescribed technologies that **must** be implemented
- There is a body of knowledge and accepted good practice, that security practitioners use to establish designs, baselines, and make subsequent recommendations to treat risk appropriately (mainly CESG manuals/memos/standards/etc)

Risk management

Overview

Conclusion

- Times are changing:
  - Networks: SWAN, PSN
  - Technology: BYOD, Cloud, more off shoring
  - Pressure: cost, efficiency
- Interaction between security controls is complex
  - End to end solution is generally essential
  - Two levels of assurance: organisation and system
- A well made case is the starting point
  - And will often be very close to finishing point to
- Recommendation
  - ISO27001 – for organisation/ISMS
  - ISO27002 + ISO27005 – for solution
  - Focus on solution/application level IA proposals



- Questions

- Colin.howarth@nhs.net