Implementation of ISO 27001:2005 at HPC - the *new* route map

Finance & Resources Committee presentation 17th March 2011

Roy Dunn, Head of Business Process Improvement

Agenda

- **What is ISO27001 and why do it**
- **Who is doing it? – The Team, and implimentation**
- **Times scales & Project Roadmap**
- **Steps to implementation**
- **Application of ISO 27001,** (Assets and Asset Management)
- **Management System documentation** (requirements)
- **Next steps - Conclusion**
- **Any questions**

Based on

ISO27001:2005 Information technology – Security techniques – Information security management systems - Requirements

ISO27002:2005 Information technology – Security techniques – Code of practice for information security management

ISO27001 Lead Implementer Certificate course from IT-Governance;

ISO27001 Lead Auditor course – BSI/IRCA

ISEB Certificate in Information Security Management Principles

What is ISO27001:2005 and why do it

- An ISO standard specifically about **information confidentiality**, **integrity** and **availability**
- 39 security objectives managed by 133 controls
- It is about not losing information having spent an appropriate amount of time and money securing it
- ISO27001 is being undertaken by all UK government departments and is already mandatory for all Japanese government departments
- Where data is lost the Information Commissioner will be more harsh on those organisations that have not implemented ISO27001(upto £500k fine) or similar systems (Appendix A2)
- We are initially going for the low hanging fruit then getting more secure

Who is doing it? **The Team**

Spook,
planner,
Policy
author….

Auditor

Auditor

The
Rottweiler

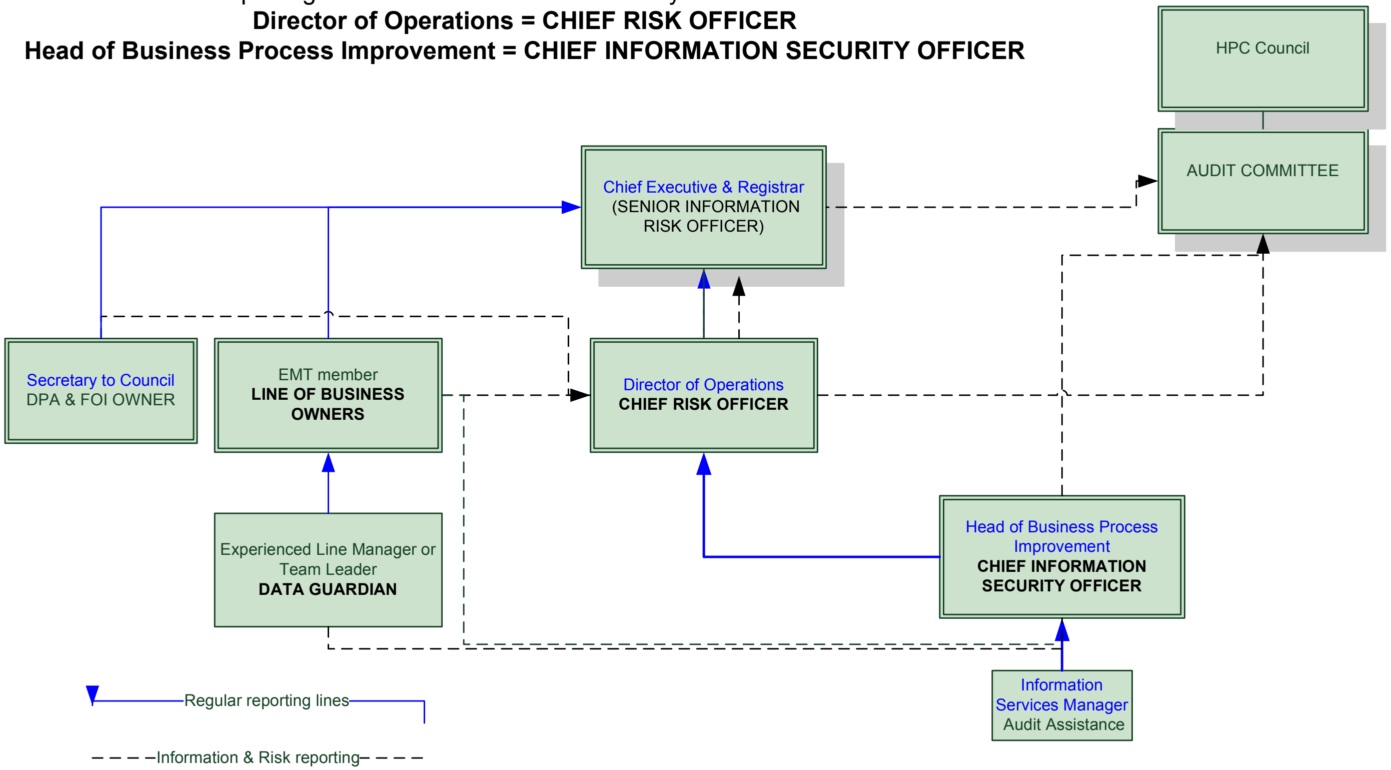
Whole organisation impact

How HPC are going to operate Information Security

Possible reporting structure for Information Security and its relation to Risk

Director of Operations = CHIEF RISK OFFICER

Head of Business Process Improvement = CHIEF INFORMATION SECURITY OFFICER

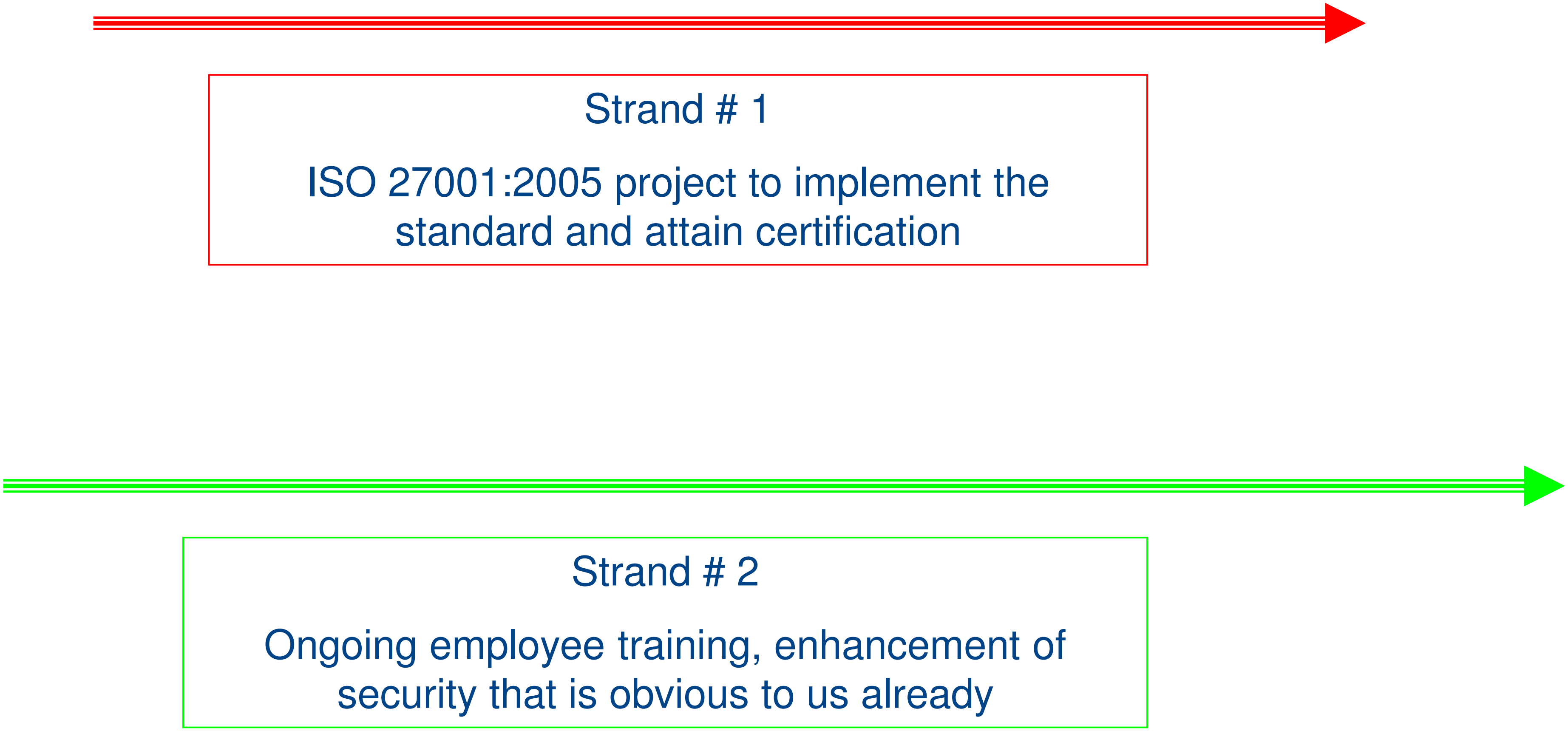

HPC Council
AUDIT COMMITTEE
Chief Executive & Registrar (SENIOR INFORMATION RISK OFFICER)
Secretary to Council DPA & FOI OWNER
EMT member LINE OF BUSINESS OWNERS
Director of Operations CHIEF RISK OFFICER
Experienced Line Manager or Team Leader DATA GUARDIAN
Head of Business Process Improvement CHIEF INFORMATION SECURITY OFFICER
Information Services Manager Audit Assistance
Regular reporting lines
Information & Risk reporting

Roles required:	HPC equivalent	Poynter review role
	RISK OWNER,	= **CHIEF RISK OFFICER**
	INFORMATION SECURITY OWNER,	= **CHIEF INFORMATION SECURITY OFFICER**
	DATA GUARDIAN,	= **Data Guardian**

The role of Senior Information Risk Owner may well be excessive for an organisation of HPC's size.

Reference: 20091124dOPTSTRATThe Poynter Review - Implications for Information Security at HPC 5

We will be running two strands to the Information Security project



Strand # 1

ISO 27001:2005 project to implement the standard and attain certification

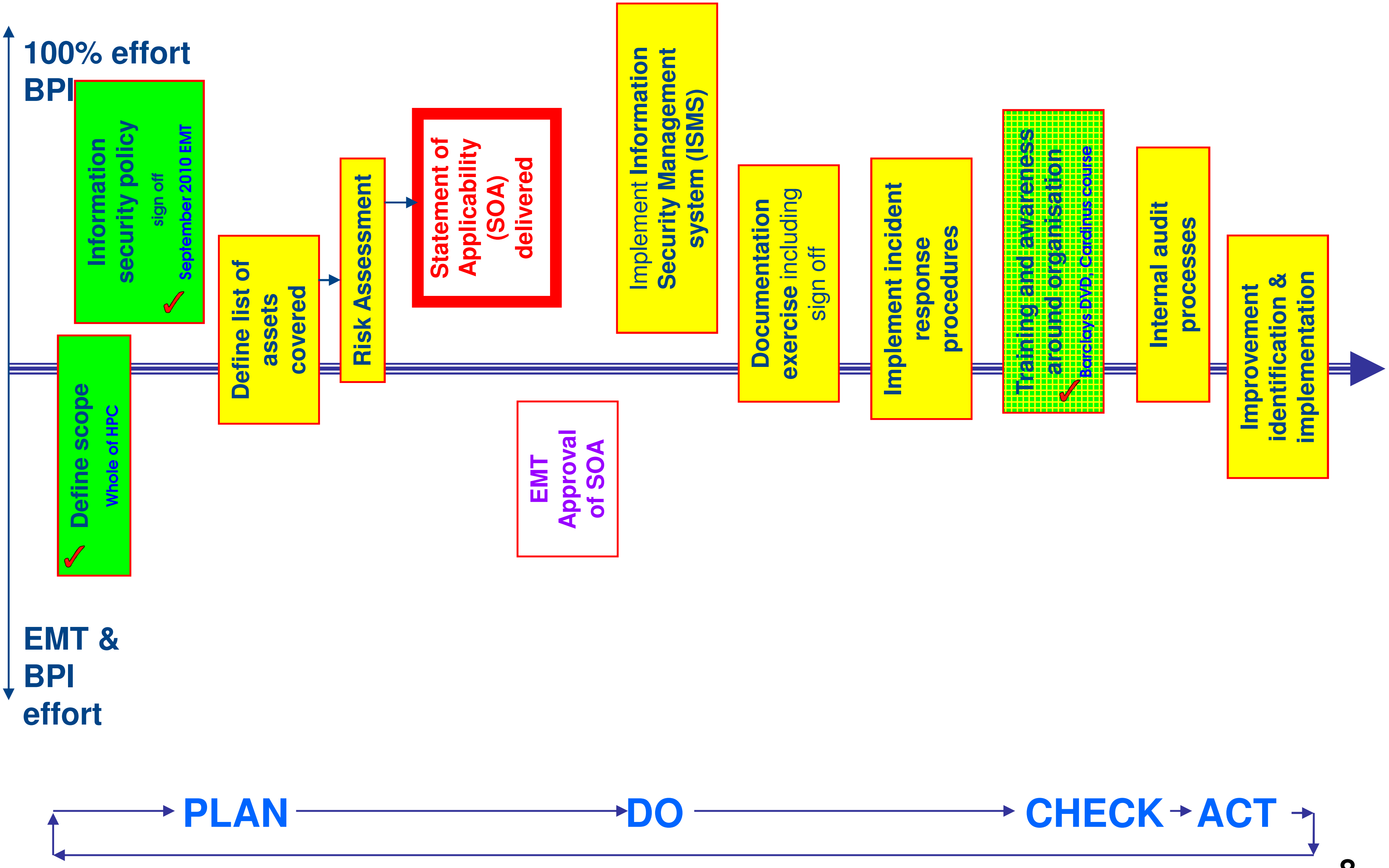
Strand # 2

Ongoing employee training, enhancement of security that is obvious to us already

Approximate Time scale and from whom effort is required

Task		2010-11	2011-12	2012-13	2013-14
Asset list creation		BPI 80% EMT 20%	BPI 80% EMT 20%		
Risk assessments			BPI 80% EMT 20%		
Mitigations to threats			BPI 80% EMT 20%	BPI 80% EMT 20%	
Statement of Applicability			BPI 90% Auditees 10%		
ISMS Documentation		BPI 95%	BPI 95%		
Internal Audits start			BPI 90% Auditees 10%	BPI 90% Auditees 10%	
Build history of internal audit			BPI 90% Auditees 10%	BPI 90% Auditees 10%	
External Gap Analysis - BSI				🟦	🟦
First BSI External Audit					🟦

ISMS Project Roadmap – Major deliverables – who does what



100% effort BPI

Information security policy sign off September 2010 EMT ✓

Define scope Whole of HPC ✓

Define list of assets covered

Risk Assessment

Statement of Applicability (SOA) delivered

EMT Approval of SOA

Implement Information Security Management system (ISMS)

Documentation exercise including sign off

Implement incident response procedures

Training and awareness around organisation Barclays DVD, Cardinus course ✓

Internal audit processes

Improvement identification & implementation

EMT & BPI effort

PLAN → DO → CHECK → ACT

ISO27001 Control A.5.1 INFORMATION SECURITY POLICY STATEMENT

Objective

The objective of information security is to ensure the business continuity of HPC and to minimise the risk of damage by preventing security incidents and reducing their potential impact.

Policy

- **The policy's goal is to protect the organisations information security assets**[1] against all internal, external, deliberate or accidental threats.
- The Chief Executive & Registrar has approved the information security policy
- The security policy ensures that;
  - Information will be protected against unauthorised access
  - Confidentiality will be assured
  - Integrity of information will be assured
  - Availability of information will be assured
  - Legislative and regulatory requirements will be met
  - Business continuity plans will be developed, maintained and tested [2]
  - Information security training will be available to all employees
  - All actual or suspected information security breaches will be reported to the Head of Business Process Improvement and will be thoroughly investigated with the assistance of appropriately trained colleagues
  - All employees and contractors will make themselves aware of the information security requirements of any data that they have access to
- Procedures exist to support the policy, including virus control measures, firewall use, password controlled access and continuity plans.
- The Head of Business Process Improvement (who acts as Information Security Manager at HPC) is responsible for maintaining the policy and providing support and advice during its implementation.

[1] Information can exist in various forms, including data stored on computers, transmitted over networks, printed or written on paper, sent by fax, stored on disk or USB memory key, magnetic tapes or telephone or direct conversations.

[2] This plan allows users to access information and essential services when required.

Steps to implementation ISO27001 – 1 Overview

Step

1. BPI gather a list of assets, eg. hardware, software, information – Roy
2. Populate our risk tool (vsRISK) with the information - Roy
3. Workout the levels of risk we can hold with the Directors & Dept heads - Roy
4. Work out the new mitigations required with the Directors & Dept heads – Roy (*likely to be few in number*)
5. Build the Information Security Management System (ISMS) - Roy

Steps to implementation Step 1- Types of Asset (ISO27002:2005)

health professions council

Type of assets already documented

- Software (*IT have a list*)
- Physical assets
  - Computer equipment, communications equipment, (*IT have a list*) removable media (*now controlled access*),
- Services
  - Computing and communications services (*IT have a list*), general utilities (*Facilities have a list*)
- People (*HR have a list of employees, regular contractors and Partners*)

Type of assets not yet documented

- Information
  - data, contracts, system documentation, manuals, archived information, transported files
- Intangibles
- Reputation and image of organisation

Eg. NetRegulate output print files for renewals containing names and addresses, D.o.B?

Example of analysis of a single type of asset NetRegulate print files

Asset category	Information / Data
Asset name	NetRegulate exported print files
Asset owner	Director of Operations
Asset type	data file
Information Asset classification	SL4 Highly confidential information
Vulnerabilities	Unprotected sensitive traffic – eavesdropping, uncontrolled copying - theft
Threats to asset	Misrouting or routing of messages, theft, transmission errors
Current mitigations	Encryption, secure VPN transmission, restricted access to file in house. Prompt removal from FTP sites

Worked example – print files from NetRegulate

Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR**/**BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
Communications and Operations Management	10.8	Exchange of Information							
	10.8.1	Information exchange policies and procedures		Existing controls					Encrypted files exchanged via secure ftp.
	10.8.2	Exchange agreements		Existing controls					Agreement refers to DPA and liability levels
	10.8.3	Physical media in transit		Physical media are not used for data exchange					Not used
	10.8.4	Electronic Messaging							
	10.8.5	Business Information systems		Existing controls					

Range of Application of ISO27001

- Standard covers all forms of information, including voice and graphics, and media such as mobile phones and fax machines.
- Standard recognises various ways of doing business:
  - e-commerce
  - Internet
  - Outsourcing
  - tele-working and mobile computing
- Paper based processes
- *+ factors in possibility for what hasn’t even been invented yet*

Strand # 1

ISO27002:2005 High level Code of Practice control objectives (same as Annex A of ISO27001:2005)

- 5 Security Policy ✓
- 6 Organisation of Information Security ✓
- 7 Asset Management ✓
- 8 Human Resources Security ✓
- 9 Physical & Environmental Security
- 10 Communications & Operations Management ✓
- 11 Access Control ✓
- 12 Information Systems Acquisition, Development & Maintenance
- 13 Information Security Incident Management ✓
- 14 Business Continuity Management ✓
- 15 Compliance (incl DPA, FOI, IPR, RIPA) ✓

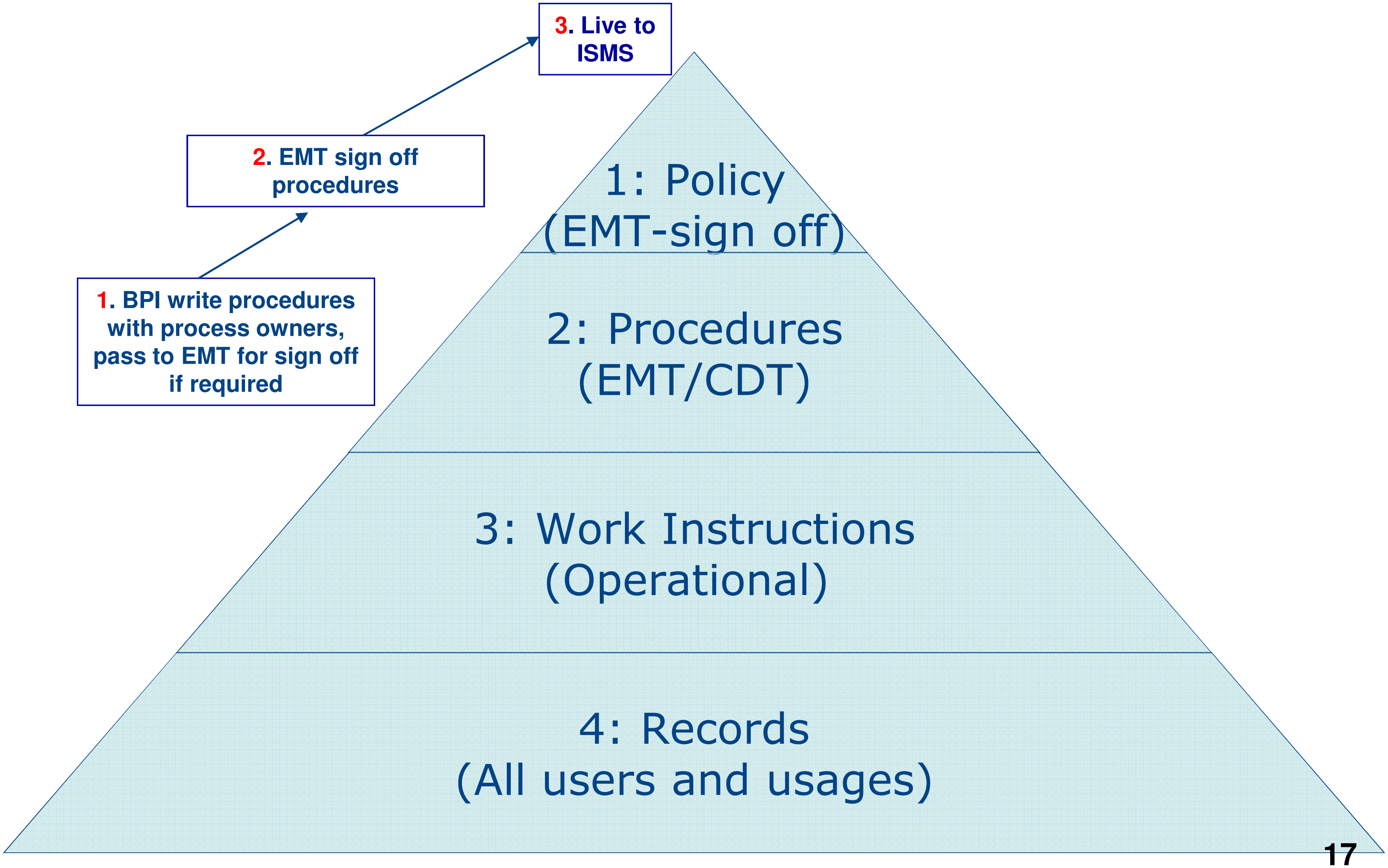
Strand # 1

Management System Documentation

- **Records of key management decisions** (at EMT = Jane's minutes)✓
- **Information security policy set, including ISMS policy** (policy signed off Sept 2010) ✓
- **ISMS scope** (whole of HPC)✓
- **Information security procedures**
- **Controls documentation**
- ***Risk assessment methods** (Information Security Risk Management for ISO27001/ ISO27002 Calder & Watkins 2007/2010)
- ***Risk assessment reports**
- ***Risk treatment plan**
- **ISMS operating procedures**
- **Information security metrics** (does the DR test work, how often do we loose things)
- ***Statement of Applicability** (comes out of Risk Assessment tool vsRisk)
- **Document control procedure** (reused from QMS ISO 9001?) ✓
- **Records control procedure** (reused from QMS ISO 9001?) ✓
- **Security awareness, training and education records, including test results** (Cardinus system) ✓
- **Internal ISMS audit plans and procedures**
- ***Management review plans and reports**
- **Corrective action procedure** (reused from QMS ISO 9001?) ✓
- **Preventive action procedure** (reused from QMS ISO 9001?) ✓

Strand # 1

Management System Documentation – sign off



3. Live to ISMS

2. EMT sign off procedures

1. BPI write procedures with process owners, pass to EMT for sign off if required

1: Policy (EMT-sign off)

2: Procedures (EMT/CDT)

3: Work Instructions (Operational)

4: Records (All users and usages)

Ongoing employee training, enhancement of security

- Cardinus Security awareness course – employees and contractors
- Internal poster campaigns *(ENISA)*
- Information security week events
- Initial Security audit contained within ISO 9001 quality audits *(what information do you use or store?)*
- Any other free resources we can use *(Barclays Bank DVD based on The Office); home movies….*

Next steps - Conclusion

- BPI gather a list of assets, hardware, software, information
- Populate our risk tool with the information
- **Workout the levels of risk we can hold with the asset owners**
- **Record the current mitigations or work out new mitigations required with the asset owners**
- Build the Information Security Management System (ISMS)

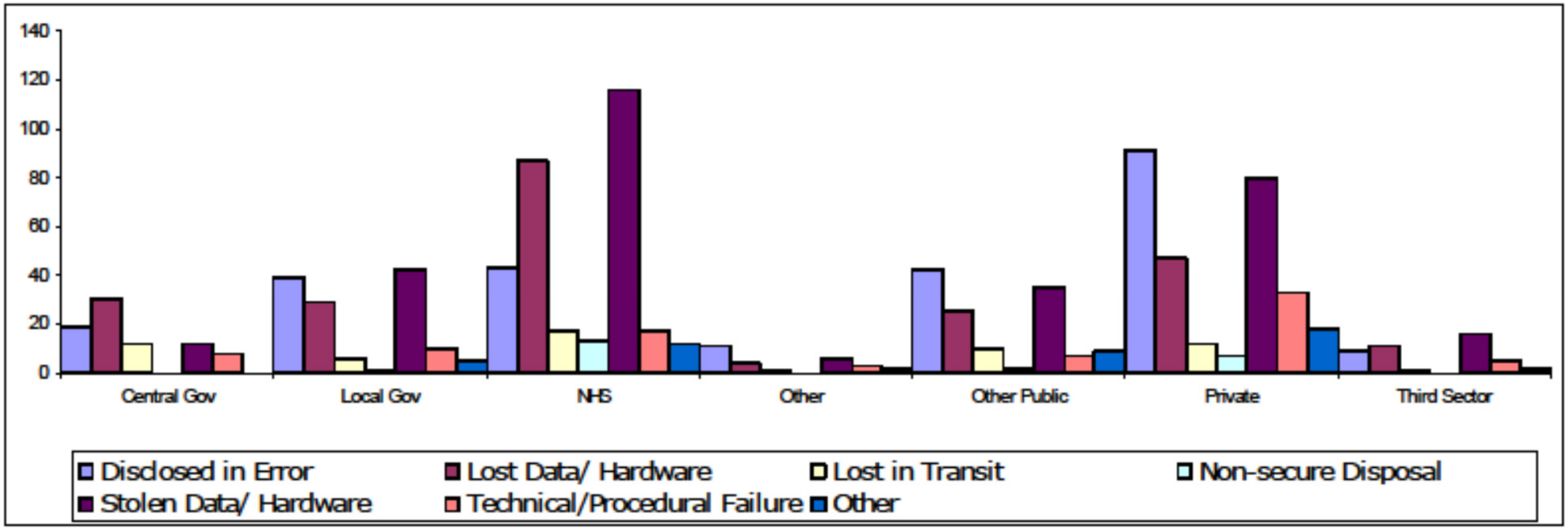
- Any questions?

We do not want to find ourselves in a list like this.

hpc health professions council

Security Breaches Reported to the ICO

Sector	Disclosed in Error	Lost Data/ Hardware	Lost in Transit	Non-secure Disposal	Stolen Data/ Hardware	Technical/Procedural Failure	Other	Grand Total
Central Gov	19	30	12		12	8		81
Local Gov	39	29	6	1	42	10	5	132
NHS	43	87	17	13	116	17	12	305
Other	11	4	1		6	3	2	27
Other Public	42	25	10	2	35	7	9	130
Private	91	47	12	7	80	33	18	288
Third Sector	9	11	1		16	5	2	44
Grand Total	254	233	59	23	307	83	48	1007



ico.
Information Commissioner's Office

What are the **reasonable steps** the Commissioner expects the data controller to take?

The Commissioner is more likely to consider that the data controller has taken reasonable steps to prevent the contravention if any of the following apply:

a) The data controller had carried out a risk assessment or there is other evidence (such as appropriate policies, procedures, practices or processes in place or advice and guidance given to staff) that the data controller had recognised the risks of handling personal data and taken steps to address them;

b) The data controller had good governance and/or audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type;

c) The data controller had appropriate policies, procedures, practices or processes in place and they were relevant to the contravention, for example, a policy to encrypt all laptops and removable media in relation to the loss of a laptop by an employee of the data controller;

d) Guidance or codes of practice published by the Commissioner or others and relevant to the contravention were implemented by the data controller, for example, the data controller can demonstrate compliance with the BS ISO/IEC 27001 standard on information security management.

A2

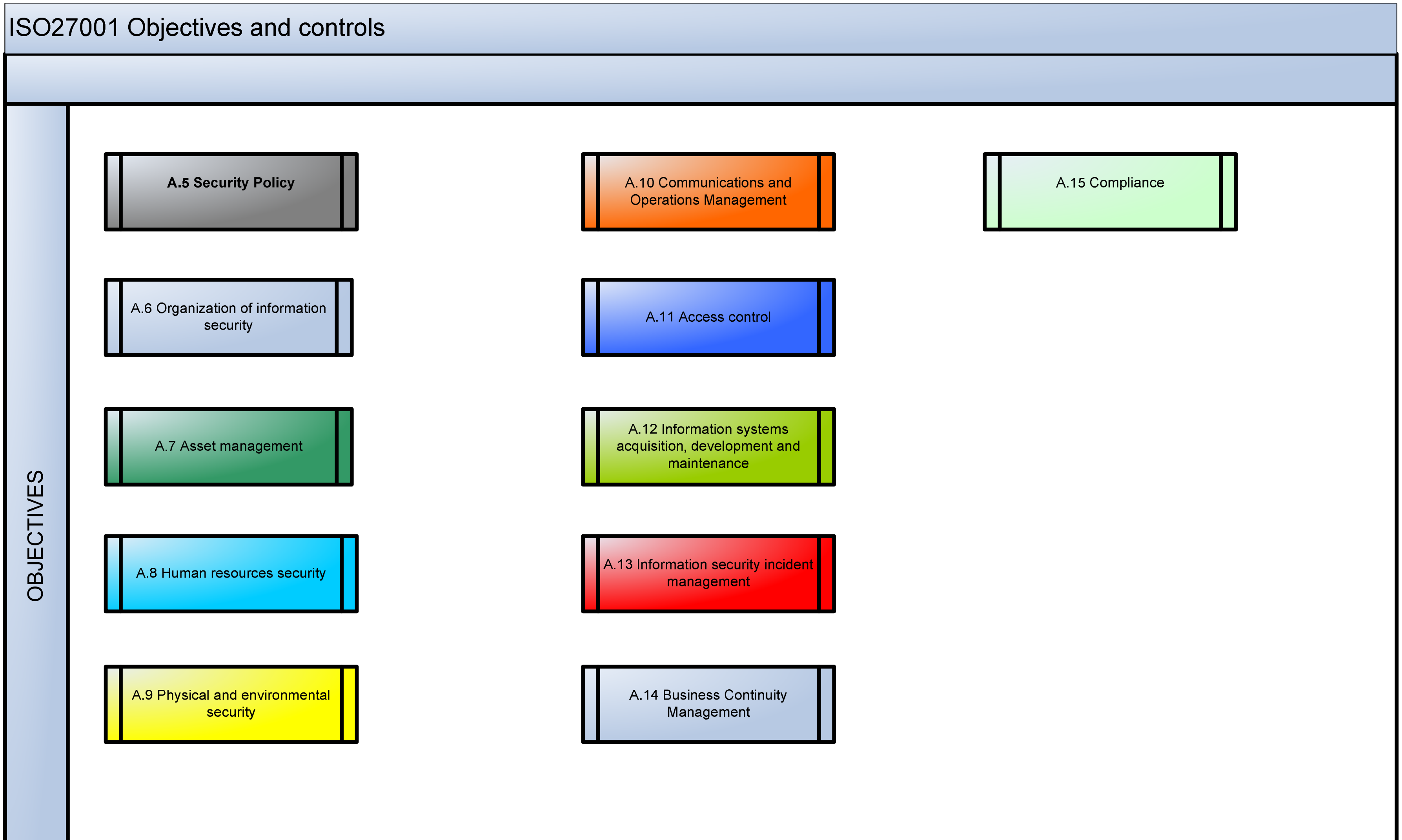
Hardware assets

- Hardware pc
- Hardware laptop
- Hardware servers
- Hardware network equipment
- Hardware phone system servers
- Hardware Blackberry / mobile phone
- Hardware scanners
- Hardware photocopier / scanner / fax
- Hardware fax only
- Hardware printers

Information assets

- Netregulate data
- Reporting system data
- FTP system data
- Education system data
- HR Partner data
- Finance dept data (non registration/application)
- Export/print files Netregulate
- Generic back up data
- Website content pre publication
- Website contenet live
- Intranet content
- QMS content
- ISMS data

Information Security Management system = ISMS



ISO27001 Objectives and controls

OBJECTIVES

A.5 Security Policy

A.6 Organization of information security

A.7 Asset management

A.8 Human resources security

A.9 Physical and environmental security

A.10 Communications and Operations Management

A.11 Access control

A.12 Information systems acquisition, development and maintenance

A.13 Information security incident management

A.14 Business Continuity Management

A.15 Compliance

ISO27001:2005 Annex A maps to greater detail in ISO27002:2005

A.5 Security Policy A.6 Organization of information security A.7 Asset management A.8 Human resources security A.9 Physical and environmental security
A.10 Communications and Operations Management A.11 Access control A.12 Information systems acquisition, development and maintenance A.13 Information security incident management
A.14 Business Continuity Management A.15 Compliance