The synergy of international standards: aligning RM practice with risk and information security models

Elizabeth Lomas
School of Computing, Engineering & Information Sciences
elizabeth.lomas@unn.ac.uk

northumbria UNIVERSITY

Agenda

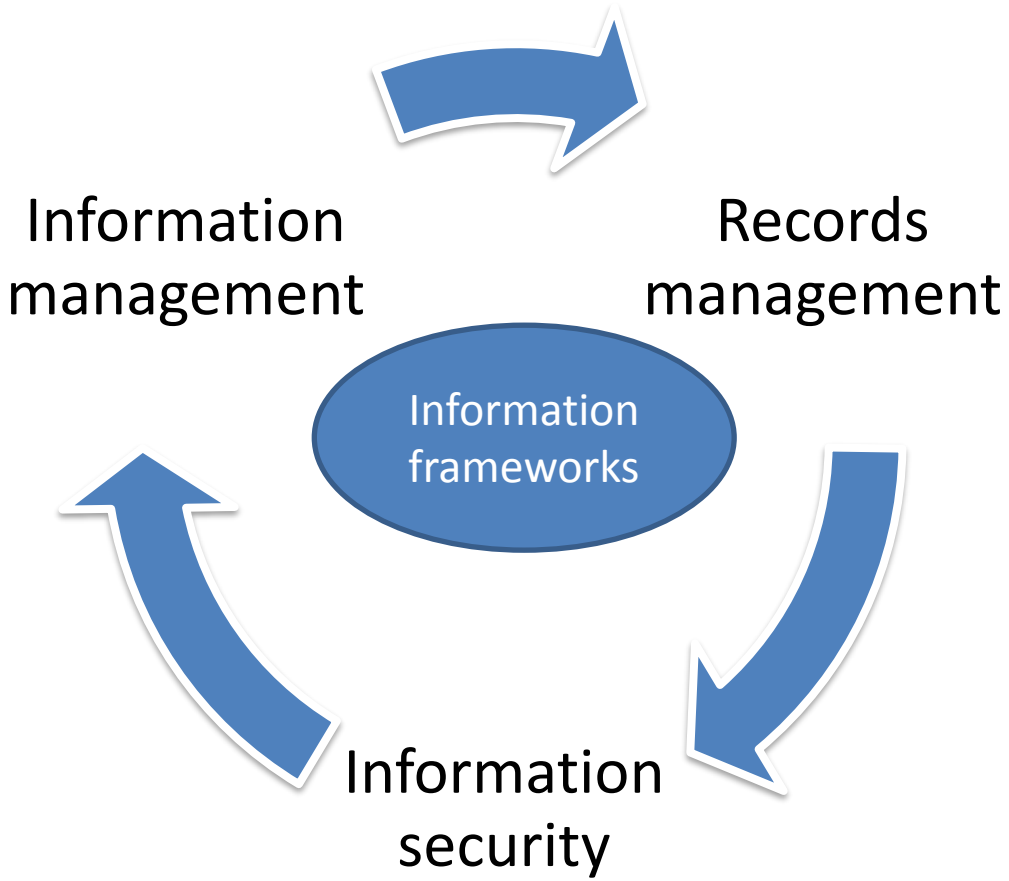
1. Records management practice (RM standard - ISO/TR 15489)
2. Information security (IS standard - ISO 27001 formerly BS 7799)
3. Web 2.0 world
4. Risk management

Continued communication...

Maximising information potential within computer mediated communications for organisational benefit through records management and business model constructs taking into account the impact of the individual

northumbria UNIVERSITY

Information Management



northumbria UNIVERSITY

Information Management

Information is an asset = fourth resource

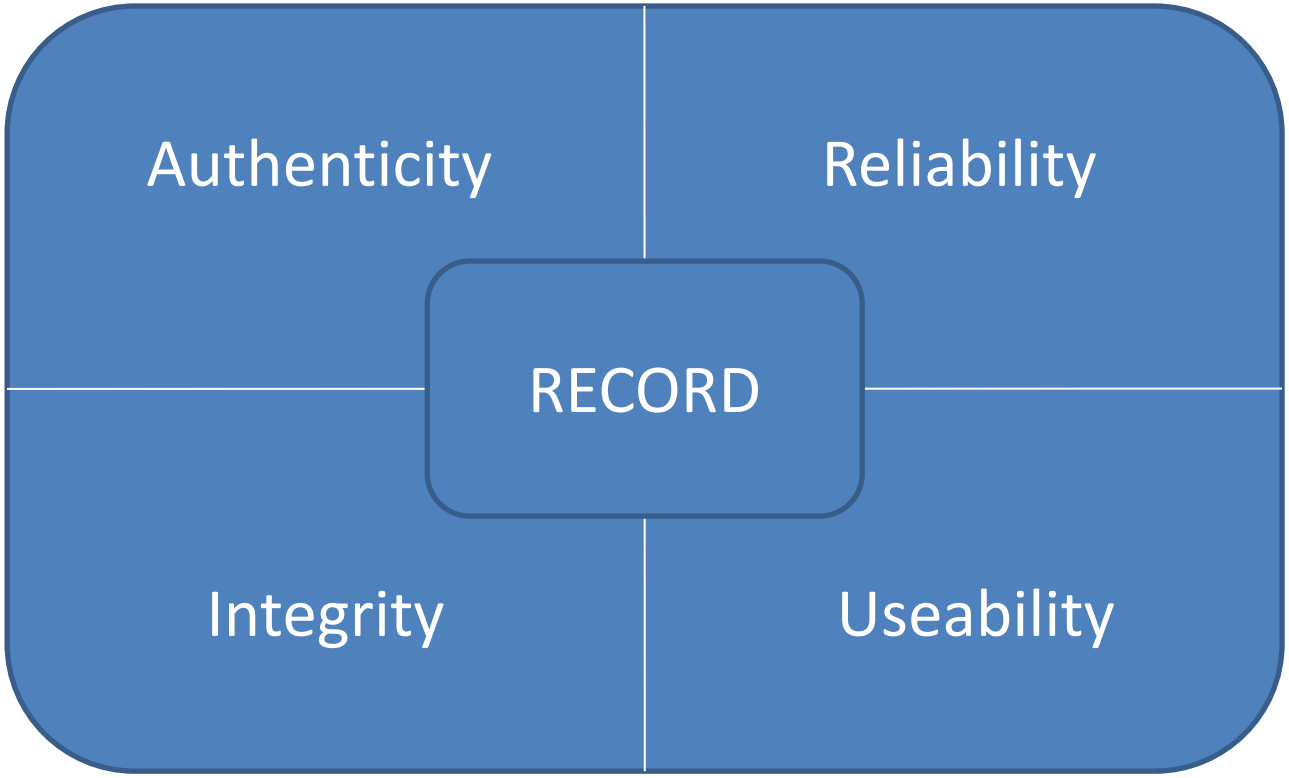
(1-people, 2-money, 3-property, 5-IT)

Information Management

- Operational efficiency
- Legal accountability
- Reputation and trust

northumbria UNIVERSITY

Records Management



northumbria UNIVERSITY

Records Management Instruments

ISO/TR 15489-2 (2001) identifies 3 principle RM instruments:

- a business activity based classification scheme
- a retention/ disposal schedule
- a security and classification scheme

Retention Schedule

Record of transaction	Format	Retention action	Reason for retention	Security level
Sales ledger	Electronic/ SAP	Destroy at 7 years (6 yrs + CY)	Companies Act 1985 s225(5)	Restricted
Application forms	Hard copy	Destroy at 3 months	Equal opportunities legislation (Age, Race and Sex Discrimination Acts)	Confidential

northumbria UNIVERSITY

Records Management Tools

ISO/TR 15482-9 (2001) identifies tools that support RM:

- an organisational delegations authority
- a register of employees and system user permissions
- a business risk analysis

Records Management Tools

Record values:

- Vital
- Important
- Valuable
- Useful
- Non-essential

northumbria UNIVERSITY

Developed Retention Schedule

Record of transaction	Format	Retention action	Reason for retention	Security level	Value	Delegated Authority
Sales ledger	Electronic	Destroy at 7 years (6 yrs + CY)	Companies Act 1985 s225(5)	Restricted	Important	Finance Dept
Application forms	Hard copy	Destroy at 3 months	Equal opportunities legislation (Age, Race and Sex Discrimination Acts)	Confidential	Non-essential	HR Dept

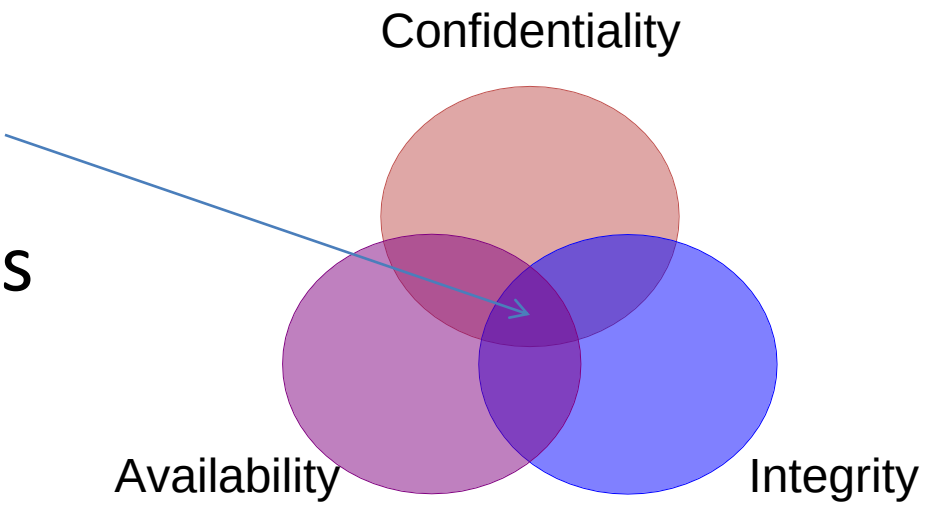
Information Asset Definitions

ISO 27001:2005 defines confidentiality, integrity and availability (often referred to by the acronym CIA) as follows:

- *Confidentiality:* The property that information is not made available or disclosed to unauthorised individuals, entities or processes
- *Integrity:* The property of safeguarding the accuracy and completeness of assets
- *Availability:* The property of being accessible and usable upon demand by an authorised entity

Information Asset Definitions

Organisations must balance these objectives



northumbria UNIVERSITY

Information Security Frameworks

Information assets include:

Data/records and also...

- People
- Physical environment including utilities
- Equipment/Hardware
- Software

Information Security Frameworks

Information Asset Register

Information asset	Format	Owner	Value/ Impact	Likelihood	Risk exposure
Payroll system	Electronic/ SAP	Finance	4	5	20
Application forms	Hard copy	HR	3	2	6

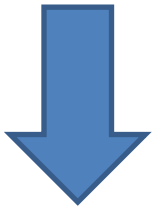
Information Security Frameworks

- Scope
- Information Security Management System
- Information asset register
- Risk assessment policy and processes

Information Security Frameworks

Risk treatment plan (tolerate, terminate, treat, transfer) -

133 Controls (IT and physical security, business continuity, third party audits for outsourcing etc)



Statement of applicability

northumbria UNIVERSITY

Information Security Frameworks

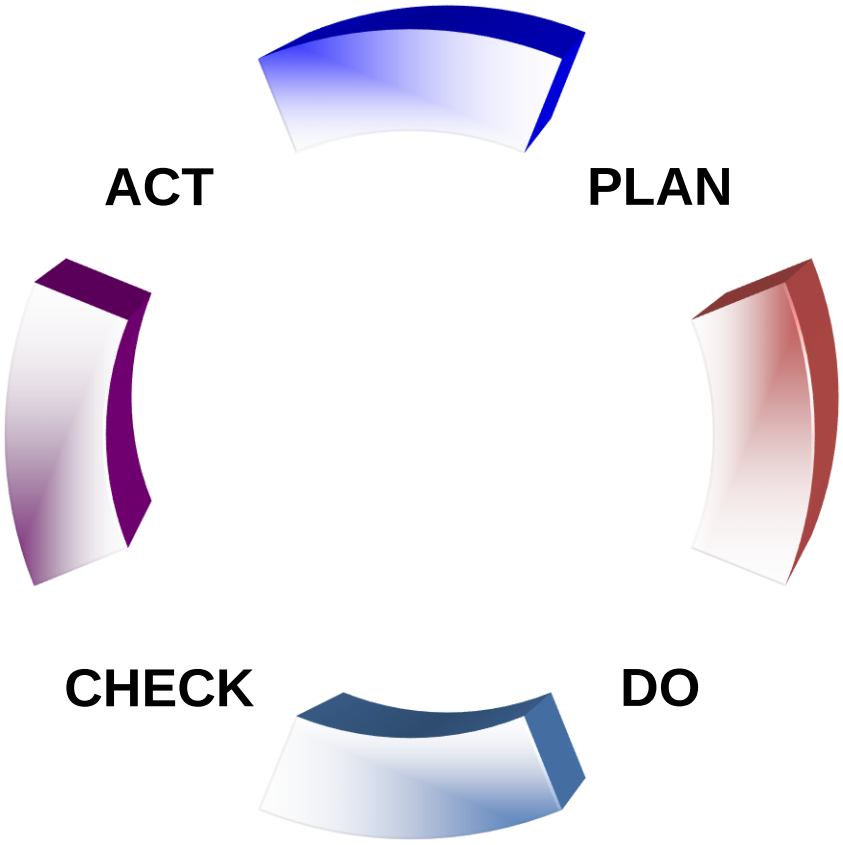
Statement of Applicability

A.9 Physical and environmental security

A.9.1 Secure areas

Control	Description	Adopted	Justification	Reference
A.9.1.1	Physical Security Perimeter	N	Do not have the finance to resource this. Willing to accept any potential risk	N/A
A.9.1.2	Physical Entry Controls	Y	To prevent unauthorised access to the organisation's' premises and monitor the movement of authorised personnel	Security Manual
A.9.1.3	Securing Offices & Rooms and facilities	Y	Some teams have restricted access due to the nature of the assets in these areas.	Staff Handbook

Information Security Frameworks



northumbria UNIVERSITY

Information Asset Definitions

- ISO 27001 (2005) *Information security*
- ISO 9001 (2008) Quality management systems requirements
- BS 10008. (2008) *Code of practice for legal admissibility and evidential weight of information stored electronically*
- BS 31100 (2008) *Code of Practice for Risk Management*

northumbria UNIVERSITY

Web 2.0 – O'Reilly's view

Upload vs. Download

- Level 0 applications: same existence on /off the Web

- Level 1 applications: can operation offline but derive features from being online

  e.g. Google Docs

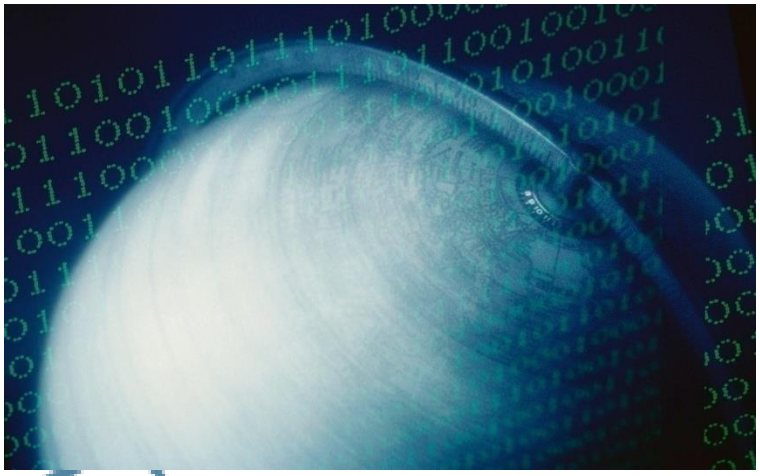
Web 2.0 – O Reilly's view

- Level 2 applications: can operation online but derive advantages from being online Flickr

- Level 3 applications: exist only on Web 2.0, derive their effectiveness from inter-human connections, Wikipedia, del.icio.us, Skype

Web 2.0 applications

Educause - 7 Things you should know about... Emerging learning technologies
http://www.educause.edu/7495&bhcp=1



Each technology

- How it works
- Where it is going
- Why it matters

Wikipedia to Lulu

northumbria UNIVERSITY

Web 2.0 applications

- *Blogs Technocrat*
- *"Micro-update/micro -blog" - Mia Ridge Twitter*
- *RVV feeds*
- *Media sharing Flickr, SlideShare*

http://www.slideshare.net/sean.mcclowry/mike20-information-governance-overview

northumbria UNIVERSITY

Web 2.0 applications

- *Social bookmarking* del.icio.us
- *Wikis*
- *Collaborative editing tools Google Apps*
- *Social networking/ e-learning systems Facebook, SecondLife, Moodle*

northumbria UNIVERSITY

Capture and preservation

- Adobe Acrobat – PDF converted for web pages

- Brown, A. (2006) *Archiving web sites: a practical guide for information management professionals*. Facet

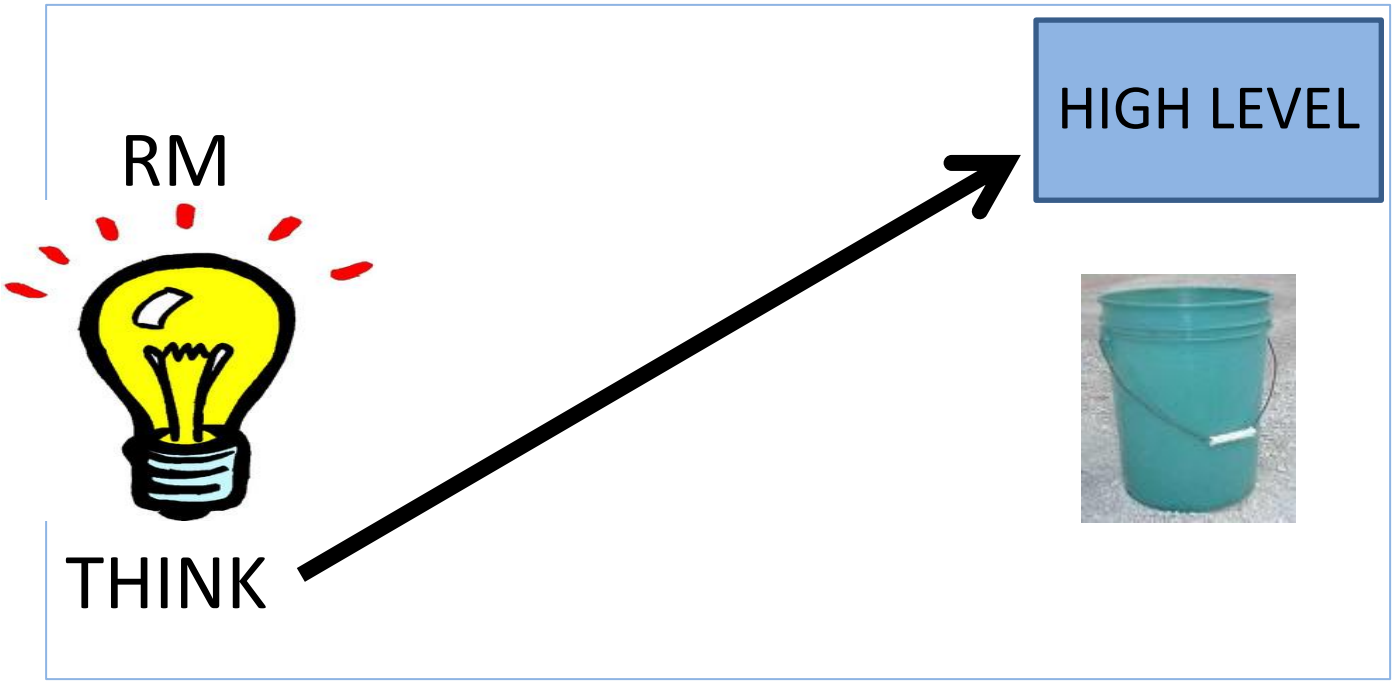
Risk Management

"the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside)"

AIRMIC, ALARM, IRM, 2002. *The risk management standard.* http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

northumbria UNIVERSITY

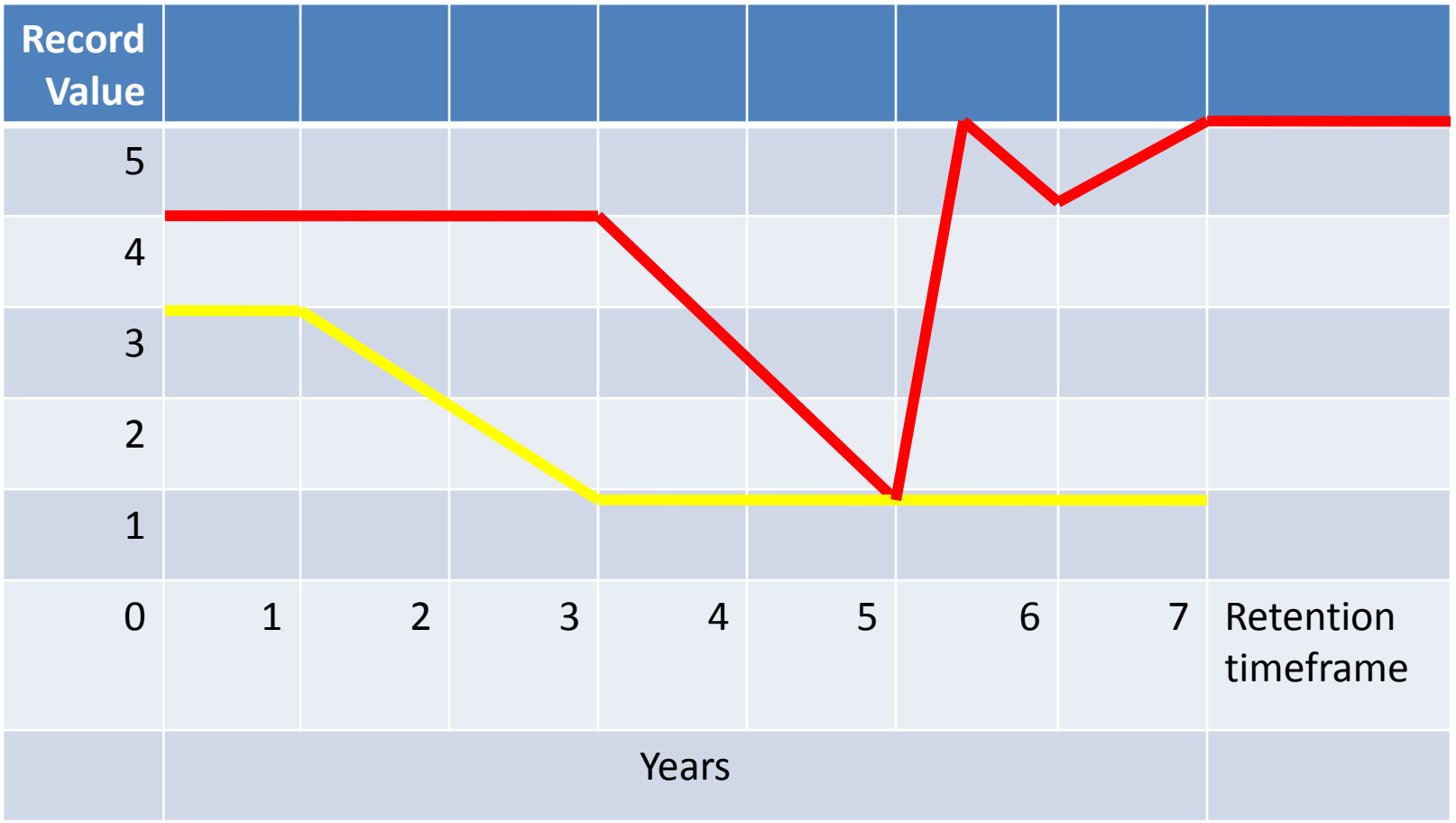
Risk Management



Risk Management

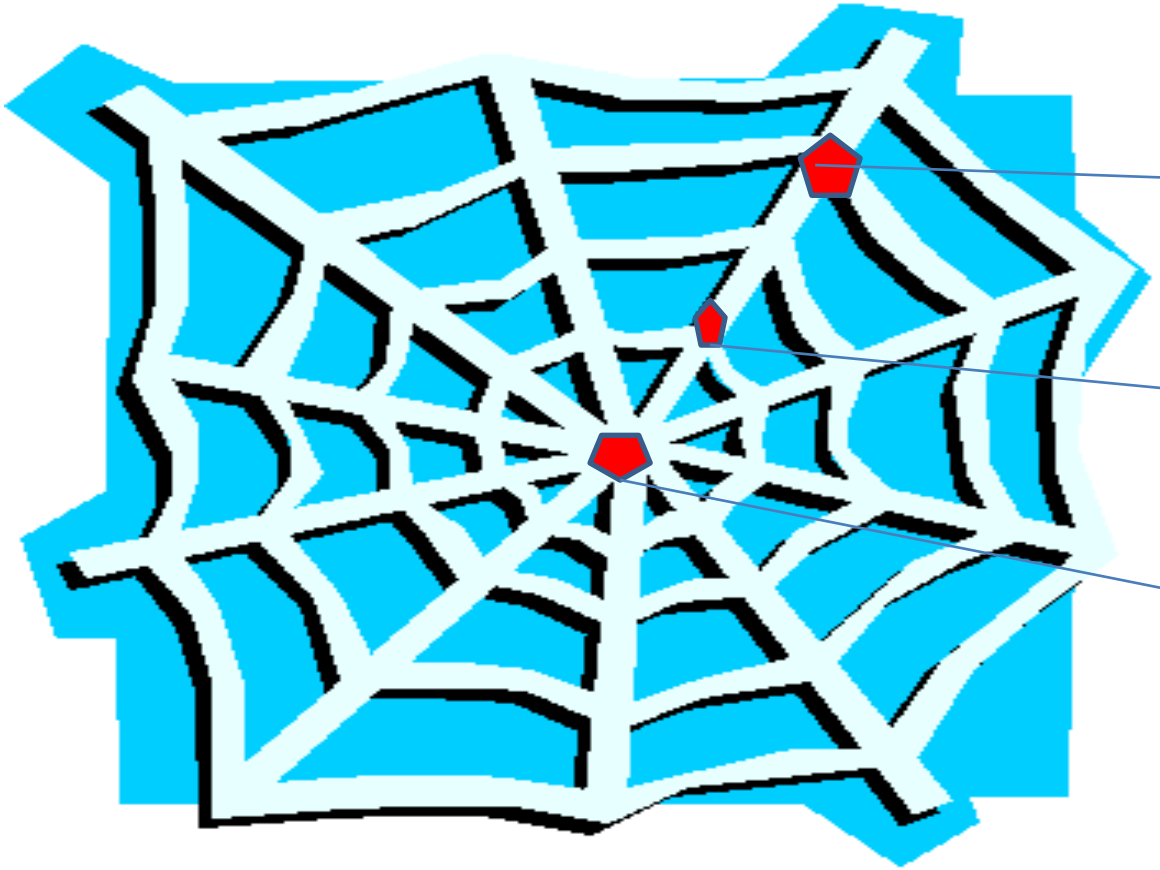
Record/information value is not a constant

Risk Management



northumbria UNIVERSITY

Risk Management



Data created, Ret. policy 3 months destroy

FOI request at 2 months

Litigation

Intricate retention web

Risk Management

**"I'm the Clutter Fairy. I'll come back ...
I'm gonna need a much bigger wand!"**

northumbria UNIVERSITY

Risk Frameworks

Government frameworks:

- Cabinet Office/Security Services
http://www.cabinetoffice.gov.uk/strategy/
http://www.strategy.gov.uk/

- OGC http://www.ogc.gov.uk/

- Treasury *Orange book* http://www.hm-treasury.gov.uk./media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf

northumbria UNIVERSITY

Risk Frameworks

Wider public sector frameworks:

- ALARM http://www.alarm-uk.org/

- Committee of Sponsoring Organisation of the Treadway Commission: *Enterprise Risk Management (ERM) standard* available at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

northumbria UNIVERSITY

Risk Frameworks

- ARMA Risk Committee records management risk publication *in progress*

http://www.arma.org/

Risk Frameworks

Standard framework:

- review the organisation's strategic objectives
- risk assessment (combination of analysis and evaluation)
  - risk analysis (including risk identification, description, and estimation)
  - risk evaluation (business impact analysis)
- risk reporting (threats and opportunities)
- decision
- risk treatment (tolerate, terminate, treat, transfer)
- residual risk reporting
- ongoing monitoring

northumbria UNIVERSITY

Risk Assessment

Asset valuation through impact analysis

IMPACT	Financial	Operational
Very High (5)	>500k	Cancellation
High (4)	£100 - £500k	Severe disruption
Medium (3)	£50 - £100k	Significant disruption
Low (2)	£25k - £50k	Requires corrective action
Very Low (1)	<£25k	Requires noting

northumbria UNIVERSITY

Risk Assessment

Asset valuation through impact analysis

Political	Change of government, cross cutting policy decisions, machinery of government changed
Economic	Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect global economy on UK economy
Socio cultural	Demographic change affects demand for services; stakeholder expectations change
Technological	Obsolescence of current systems; cost of procuring best technology available, opportunity arising from technological development
Legal/regulatory	EU requirements/ laws which impose requirements (such as Health and Safety legislation)
Environmental	Buildings need to comply with changing standards; disposal of rubbish and surplus equipment needs to comply with changing standards

Orange book available at http://www.hm-treasury.gov.uk./media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf

northumbria UNIVERSITY

Risk Assessment

Likelihood

	Likelihood
Very High (5)	Definite
High (4)	Probable
Medium (3)	Possible
Low (2)	Unlikely
Very Low (1)	Extremely unlikely

northumbria UNIVERSITY

Risk Assessment

LIKELIHOOD X IMPACT = RISK EXPOSURE VALUE

5 X 5 = 25

northumbria UNIVERSITY

Risk Assessment

IMPACT						
I	5	5	10	15	20	25
M	4	4	8	12	16	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5

LIKELIHOOD

northumbria UNIVERSITY

Risk Frameworks

Wider public sector frameworks:

- Monte Carlo risk models
- Weighted risk appetites

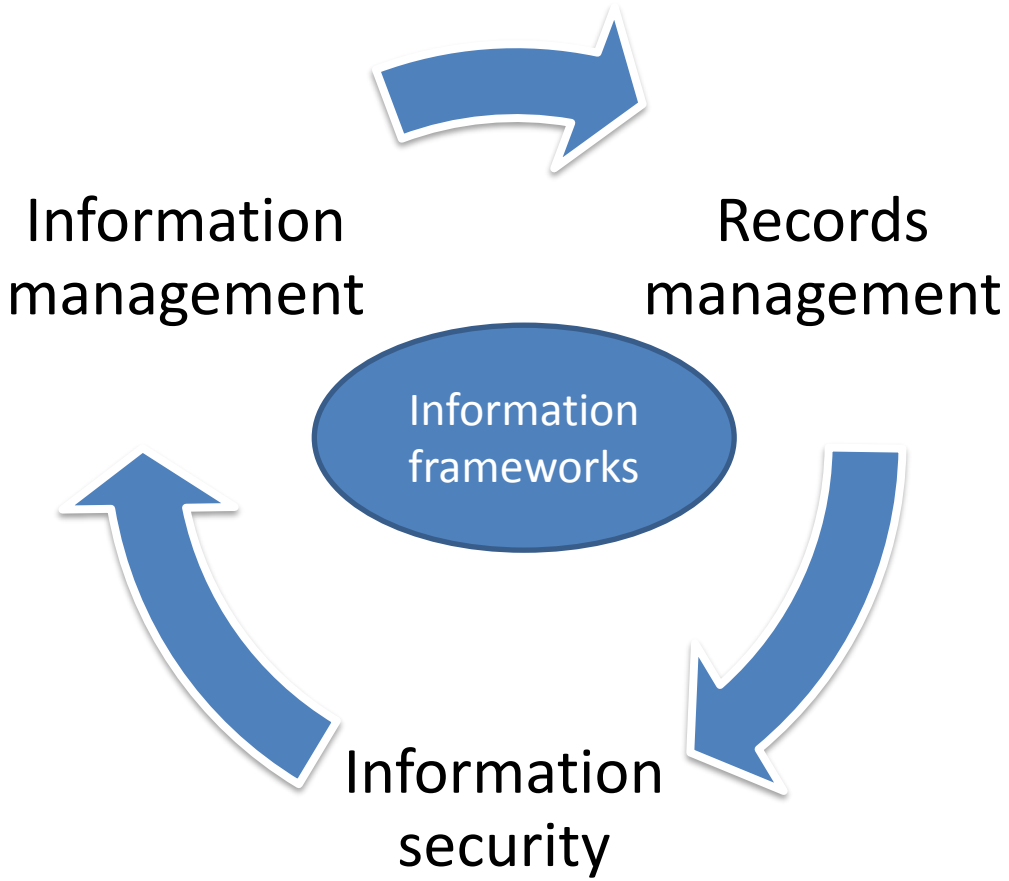
Information Asset Definitions

"Information is an **asset** which, like any other important business assets, has value to an organisation and consequently needs to be suitably protected"

(BS ISO 17799-1:2000)

northumbria UNIVERSITY

Information Management



northumbria UNIVERSITY

- Records Management MSc; Information Rights LLM, Northumbria University

- Continued communication...a co-operative action research confronting the challenges of managing records/data held within information communication systems

  www.continuedcommunication.org

- Contact: elizabeth.lomas@unn.ac.uk

northumbria UNIVERSITY

Thank you

northumbria UNIVERSITY