Applying ISO27001 and risk assessment to records management

Richard Jeffrey-Cook

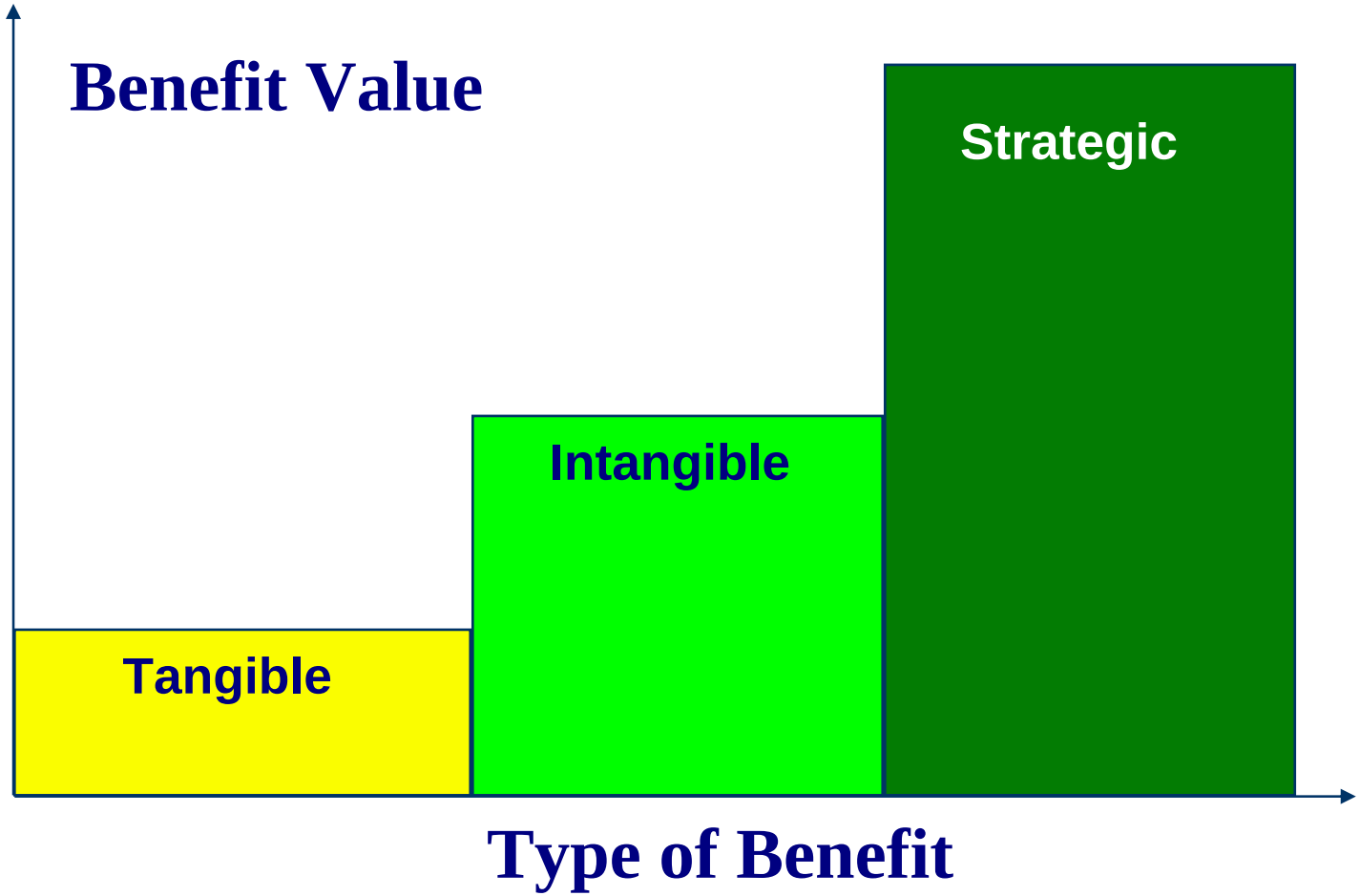
The Benefits of Records Management

- Compliance
  - Law
  - Regulation
- Governance
  - Demonstrate good decision making
- Efficiency

Conclusion looking at Benefits

- Tangible benefits are small
  - Storage space
- Intangible benefits are bigger
  - Sharing information etc.
- Strategic benefits potentially huge
  - Transformational government

Types of Benefits



Focus on Compliance

- What is likely to happen if you don't comply?
  - Data Protection Act
  - Freedom of Information Act
  - Environmental Information Regulations
  - …

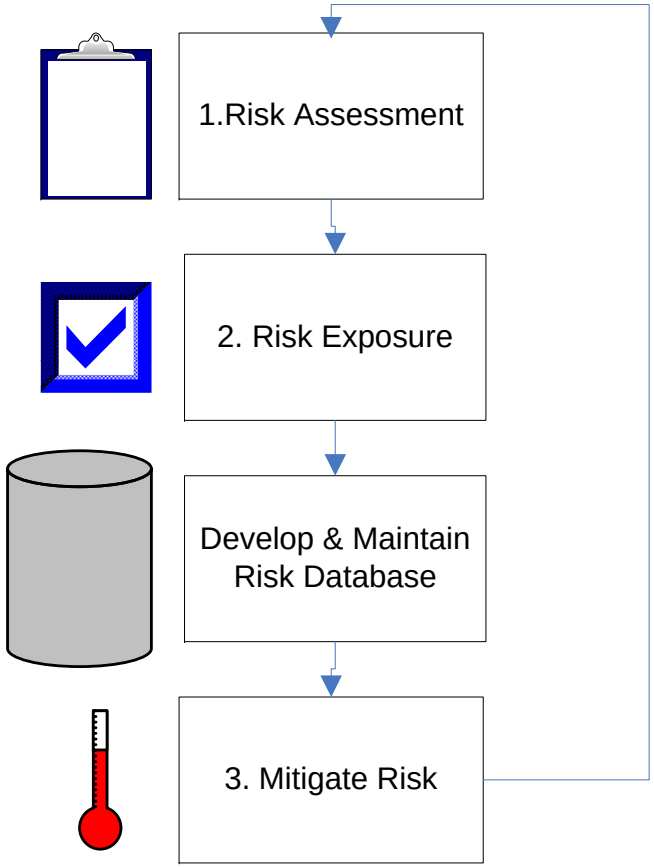
Risk Management

- Operational risk
  - An organisation owns its processes therefore can own the risk associated with that process
- Reputational risk
  - The public and an organisation's stakeholders own the reputation of the organisation
  - Reputation is managed through the actions that the organisation takes

How does this affect RM?

- Business processes use and transform information
  - Inadequate or inappropriate information can cause a process to fail
  - Reputation can be badly damaged by incorrect or missing information
- Records managers
  - Guard corporate memory
  - Should be involved in entire information lifecycle

Risk Management Programme



Identify information controls

- Example

  Information Management Policy – Does the organisation have an IM Policy? Are staff aware of it – do they follow it?
- A sub-set of ISO 17799 information security controls relate to information management
- Other controls can be identified from standards, sources of good practice, legislation and regulation

Identify applicability

- Not all controls apply to all organisation
- Example
  - Public sector – need to take FOIA into account when entering into confidentiality agreement
  - SOx requirements wouldn't apply to UK private company

In-Form Consult

Why take this approach?

- Many of the benefits of RM systems are
  - Intangible
  - Strategic
  - Business often takes a short term view
  - Difficult to justify budget
- A risk management approach can
  - Provide a reasoned basis for spending resources
  - Decide between alternative courses of action

Example

- Gas supplier – cut off gas to elderly couple for non-payment
  - Failed to inform local authority
- Couple died from hypothermia
  - Gas supplier PR department tried to claim information not given to local authority due to DPA
  - Information management matters – two people lost their lives!
  - Operational aspects – failure in process to inform local authority
  - Reputational aspects – explanation was wrong and resulted in severe censure from Information Commissioner

In-Form Consult

Example

- Recently privatised NHS Service
- Patient dies after waiting 9 hours for a delivery of oxygen
- Failure in operation planning
  - Inadequate change management in transfer of operation

Example

- London Council – exposed for “recycled waste” turning up in far east
- Failure of sub-contractor to adhere to regulations
  - Need to monitor activity of sub-contractors

Example

- County Council website
  - Links to sites that were not compliant with DDA
- Needed to review policies with affiliated organisations

Any Questions ?

In-Form Consult Ltd