



Securing Information Assets with ISO 27001

Alan Calder
IT Governance Ltd

AIFS 2009
16 January 2009

Welcome



- Alan Calder – my background and perspective
- *Businessman, not a technologist*
- *First accredited certification in 1999*
- *Founded IT Governance Ltd in 2002*
- *International IT Governance: an Executive Guide to ISO 27001/ISO 17799 (Open University Text Book)* <http://www.27001.com/products/16>
- ***Nine Steps to Success: an ISO27001 Implementation Overview:*** <http://www.27001.com/products/22>

Agenda



- *The Case for ISO27001*
 - *The information security environment for ISO27001;*
 - *The regulatory compliance context for ISO27001;*
 - *Benefits of certification/registration;*
- *Composite Case Study - Nine Steps to Implementation Success:*
 1. Initial approach
 2. Management support
 3. Scoping
 4. Planning
 5. Communication
 6. Risk Assessment
 7. Control Selection
 8. Documentation
 9. Testing

Evolving Threat Environment



- **Distributed computing**
 - Distributed network of desktop, laptop and micro computers
- **Mobile computing & porous perimeters**
 - Laptop computers, PDAs, mobile phones, digital cameras, portable projectors and MP3 players
- **Use of the Internet for business communication**
 - Email, Instant Messaging, wireless, VoIP, blogging and broadband - tools which have little or no enterprise-strength security capability.
 - Web 2.0
- **Proliferating hackers and hacker tools**
- **Co-operation between hackers, virus writers and spam operators to spread more spam.**
- **Phishing, pharming and other internet fraud activity**
- **Increase in blended threats.**
- **Increasingly sophisticated technology defences driving an increase in social engineering-derived hacker attacks.**
- **Cyberwar, cyberterrorism, cybercrime**

- **DEFENCE?**
 - Requires a structured, comprehensive, multi-level, management driven approach
 - It's not just IT!

Evolving Regulatory Compliance Environment



- Proliferation of new, information-related laws & regulations
 - rapid globalisation of governance requirements
 - the evolving business risk and threat environment, and
- EU Data Protection & Privacy Directives
- PCI – Payment Card Industry security standard
- Untested, untried, overlapping, far-reaching
- Regulations don't tell you what has to be in place, or how to do it

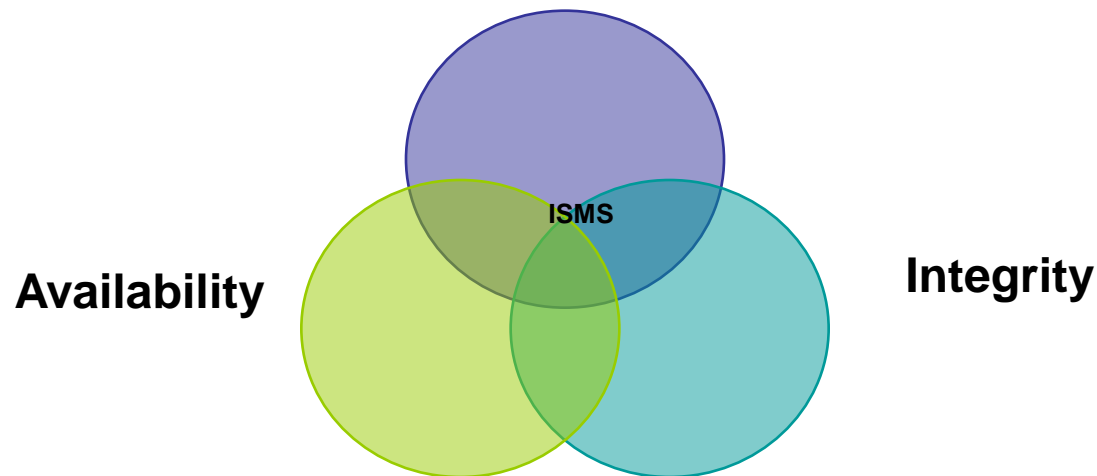
- Compliance?
 - Requires a structured, comprehensive, multi-level, management driven approach
 - It's not just IT!

Information Security: Key Attributes



Critical for security, compliance and organisational effectiveness

Confidentiality



The ISO27001 ISMS



- Comprehensive guidance on protecting Information Assets and enabling today's information-based businesses
- Best Practice for delivering the key regulatory requirements:
 - Confidentiality, integrity, availability
- Vendor-neutral, sector-agnostic, internationally recognised
- Provides international framework for 1st, 2nd, and 3rd party auditing of information security
- Increasing global presence

ISO 27001 vs ISO 27002



- Management System Specification – ISO/IEC 27001:2005:
 - ‘*shall*’
 - All elements are mandatory
 - Standard against which (1st, 2nd, 3rd party) audits can be performed
- Control Implementation Code of Practice – ISO/IEC 27002:2005
 - ‘*should*’, ‘*may*’
 - No elements are mandatory
 - No audit possible
 - Does contain ‘best practice’ guidance
- ‘The standard is the thing’
- Intrinsically linked
 - Annex A of ISO27001 lists 133 controls, and cross-refers to ISO27002
 - ISO27002 provides guidance on implementation of each of those controls

ISO27001: A MANAGEMENT Standard



- Requires information security-business alignment
- Must be driven 'from the top'
- Must be signed off by business management
- Business risk-based
- Controls must be proportionate to the risks
- Must be regularly reviewed, in the light of changing business circumstances

Benefits of an ISO 27001 ISMS



- Differentiates an organization from its peers – ie competitive advantage in relation to customers, staff and suppliers
- In some instances, is a pre-requisite to be considered for a contract
- Demonstrates that legal, regulatory, contractual and business requirements for information security are addressed in a coherent, cost-effective and comprehensive manner
- Comfort that information security risks are properly identified and dealt with from a business perspective
- Information security enables the business, rather than providing hurdles for operations
- External, third party validation of effectiveness of control activity
- Reduction in costs of demonstrating information security adequacy in invitations to tender and similar activities

Nine Steps to Implementation Success



1. Initial approach
2. Management support
3. Scoping
4. Planning
5. Communication
6. Risk Assessment
7. Control Selection
8. Documentation
9. Testing

1. Initial Approach

Know:

- Why information security is important for ***your*** organization – and be able to communicate it
 - (the ‘fear list’)
- The ISMS/ISO27001 Champion
 - Why ISO27001 is the right way to do it, and what’s involved
 - How the project will be structured
 - How the project will be resourced – internal action and external support
- Client 1: Key contract renewals required certification

1. Initial Approach:

ISMS Implementation as a change project



- Information security affects the whole organization
 - *All information assets*
 - *All users*
- Controls consist of
 - Technology
 - Procedure
 - Behaviour
- Implementation therefore felt enterprise-wide
- Must be tackled as a business-change project
 - Business objectives
 - Business leadership
 - Integrated methodologies
 - IT, infosec and compliance support
- Client 1: Project led by Quality Manager

2. Management Support

- Standard requires management commitment:
 - To provide management direction and support in accordance with business requirements and relevant laws and regulations
 - To manage information security within the Company
 - To maintain the security of organizational information and information processing facilities accessed, processed, communicated to, or managed by external parties
- Client 1: Project had board support at parent company level, but not in subsidiary
- Client 2: Change of CEO led to project faltering

2. Management Support

Information Security Policy



- Corporate policy sets out an organisation's intentions and principles regarding information security
- Should be timeless in that it should alter little from year to year
- Policy should be endorsed at the highest level – for example, by the Chief Executive
- Client 3: No clarity about prioritisation of controls because CEO didn't see point of a policy

2. Management Support: Program/project Team



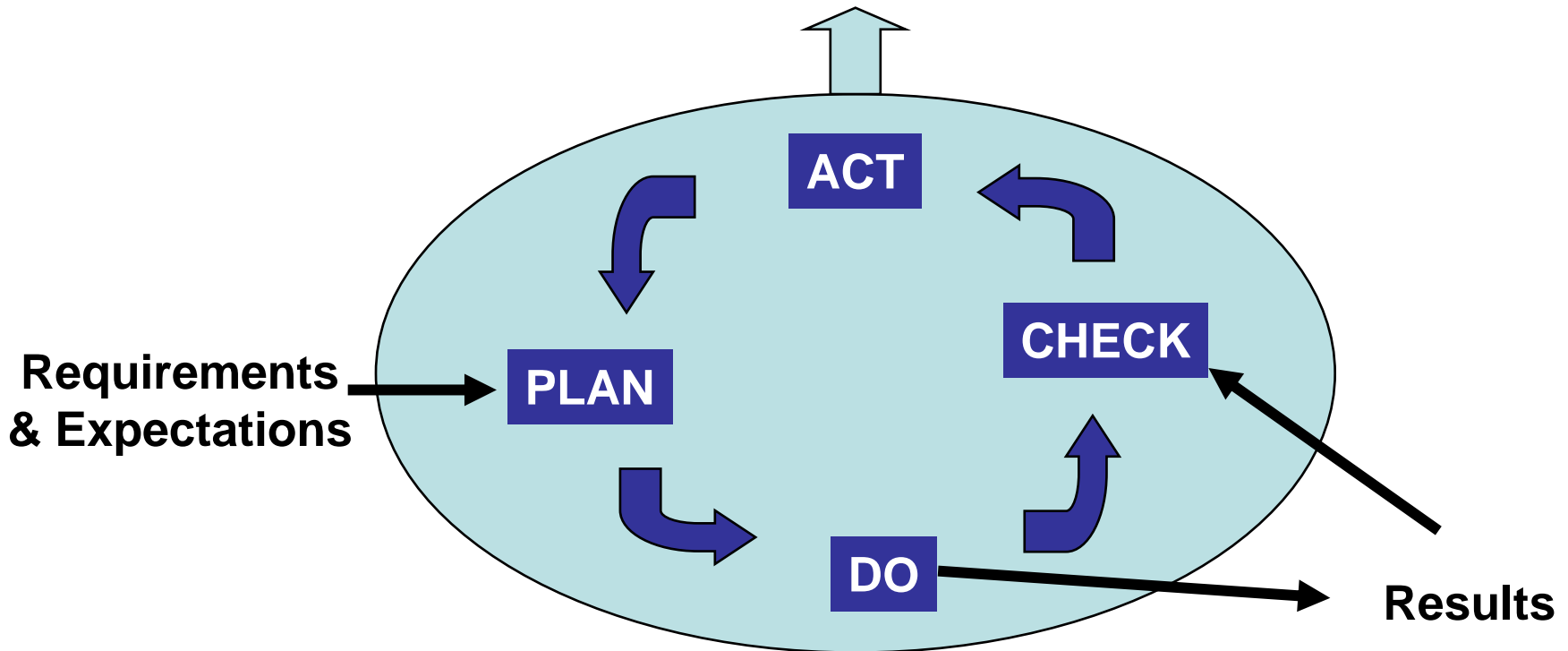
- Senior management support
 - CEO
 - Steering Group – particularly in large and public sector organisations
 - Senior business line executive (lead)
- Project Team
 - Chair: Change and project expertise
 - Initial training for team
 - Cross-functional
 - Information Security Specialist
- Client 1: Chaired by Quality Manager, contained sales director, operations director, and functional heads (HR, IT, Finance, Marketing)

3. Scoping

- Boundary of the ISMS as far as:
 - the Business
 - Geography/premises
 - Dependencies and Interfaces
- Countries
- Premises
- Business functions
- Key processes
- Client 1: Six ISMSes (UK first, followed by Germany then other EU subsidiaries)
- Client 2: Head office and Central IT organisation (decentralised management structure)

4. Planning

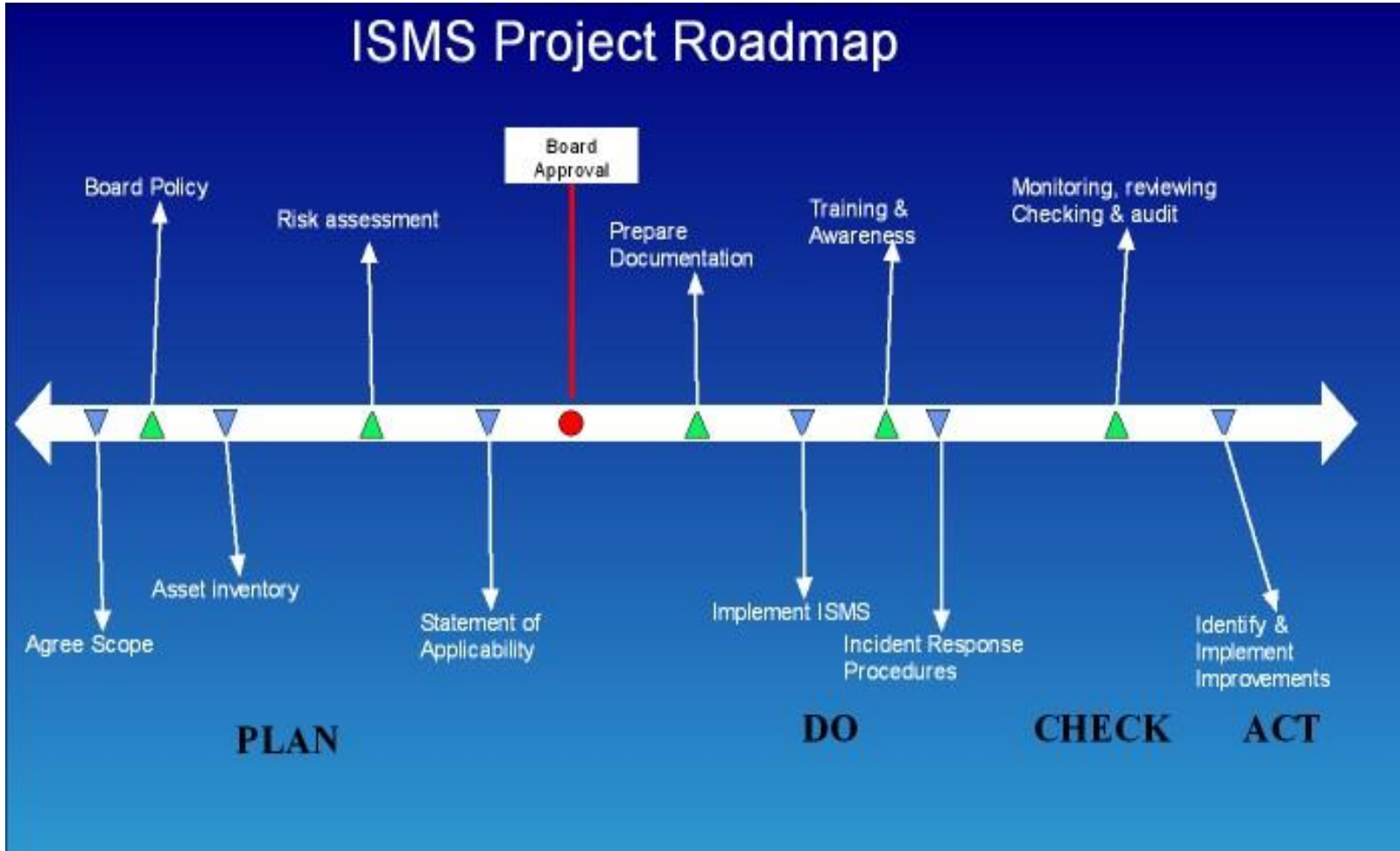
PDCA Cycle: Plan – Do – Check – Act



PDCA at project level and at individual control level

4. Planning:

ISMS Project Roadmap



5. Communication

- Deployment
- Why?
- Regular updates
- Training & awareness:
 - E-Learning
 - Classroom
- Client 1:
 - Head of Marketing on project team
 - eMail Teaser Campaign
 - Fear list
 - Monthly project updates
 - Promised less, delivered more
- Client 2
 - Monthly CEO briefing to all staff

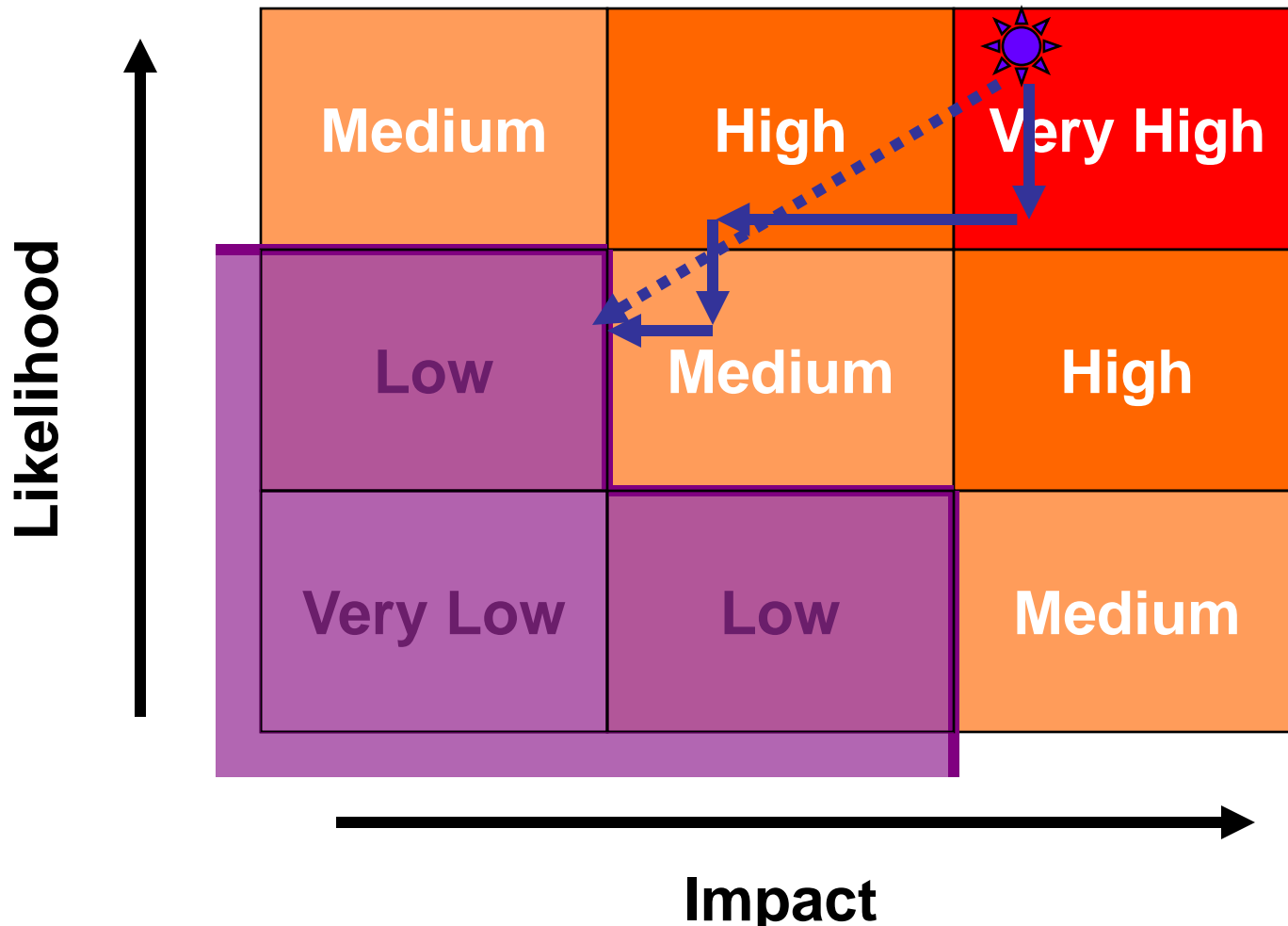


6. Risk Assessment

- ISMS founded on a risk assessment
- Risk assessment methodology must be defined
- Risk assessments must give 'reproducible and comparable results'
- Impossible without a risk assessment tool and a team committed to the task, with a specific time frame for success
- Client 1:
 - PDCA applied to risk assessment process
 - Agreed risk assessment methodology and selected tool
 - Selected and trained a risk assessment team
 - Grouped assets at a high level
 - Completed exercise on time!
- Client 3: had completed control selection before considering risk assessment methodology

6. Risk Assessment

Qualitative approach simplifies project



7. Controls

The Risk Treatment Plan



- **A control is a countermeasure for a risk**
- Must select controls from ISO 27001 Annex A
- You can also import from other standards or invent your own if control objective requires it
- Controls are to be selected **by objective**
 - **Client 3 selected controls the IT manager thought were necessary**
- **Guidance:**
 - Some controls are more effective at reducing risk than others
 - Over a third of fixes are comparatively ineffective.
 - An avoidance strategy of fixing every vulnerability, although guaranteed to minimise risk, is potentially expensive and time wasting
 - **Don't select two controls where one will do**
 - **Client 3 selected controls from the SoA, which meant that they removed some controls they had previously applied.**

7. Control Selection

Deploy all aspects of a control, and use controls that have more than one application

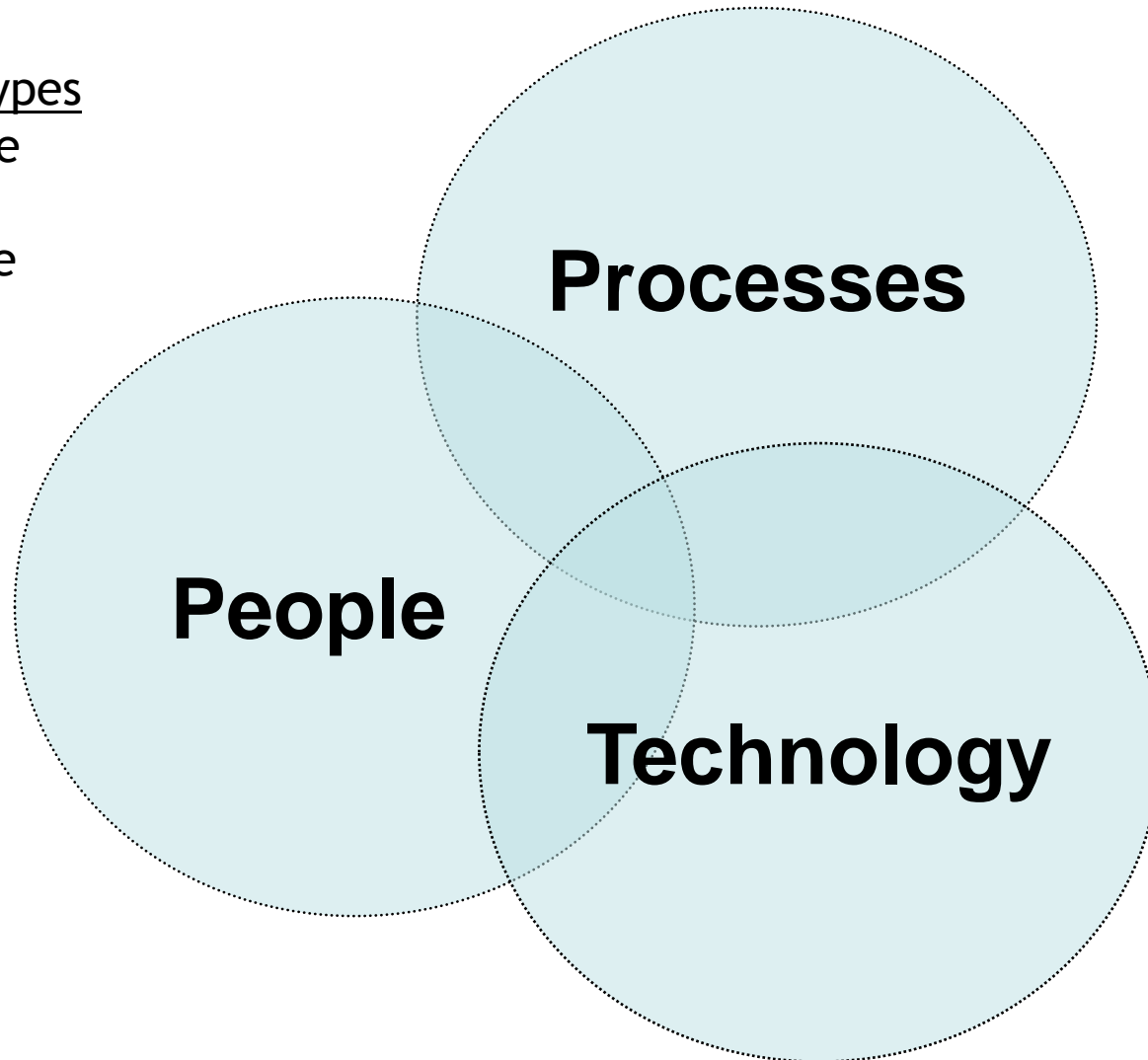


Control Types

Preventive

Detective

Corrective



7. Control Selection

ISO27001 Annex A: 11 Control Categories

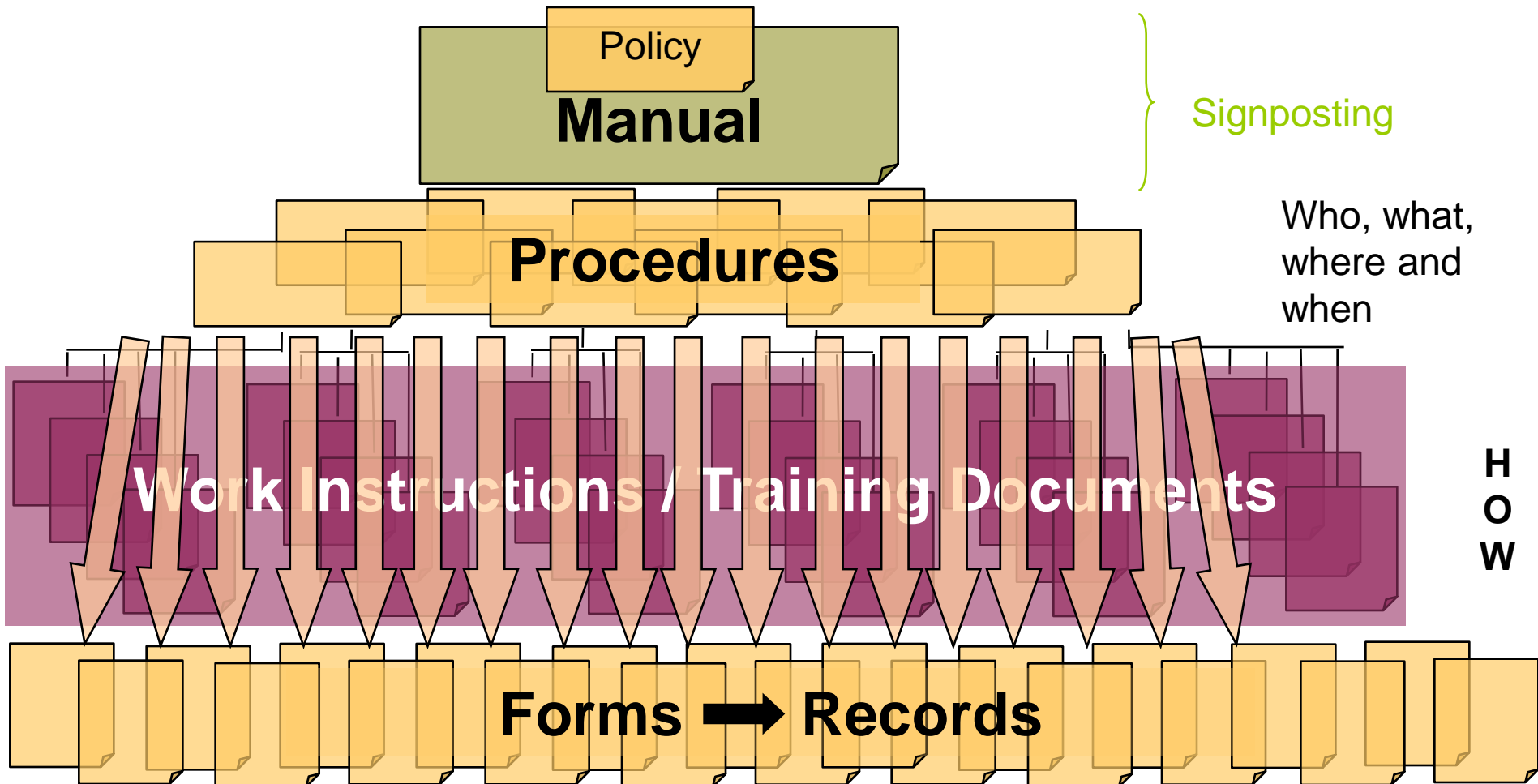


8. Documentation: document life cycle management



- ***"It's good sense to avoid re-inventing existing wheels. Encourage cooperation by taking the guesswork out of...infosecurity and use template-based processes."*** Jay G Heiser, VP and research director at Gartner Research
- Integrate with any existing internal management frameworks (eg ISO9001, CobiT, ITIL, etc)
- Enforce PCI DSS integration
 - PCI controls are mandatory, not voluntary
- Consider DLM tools to keep documentation controlled and current
- Policies and procedures need to be accepted by users – may need to be linked to training
- Client 1 deployed a commercial DLM tool from the outset and used it to support process creation and procedure drafting

8. Documentation



9. Testing

- Internal audit
- External specialist (technical) audit support
- Paper test (control orientated)
- Simulation
 - Particularly important for business continuity aspects
- Complete cycle of audits usually required
 - Can be prioritized by risk profile
 - Well begun can argue for future completion
 - Clients 1, 2 & 3 were all successful at audit
 - Client 4 failed at audit and had to call for help!



Securing Information Assets with ISO 27001

Alan Calder
IT Governance Ltd