DLM / ARMA

‘Information management’

‘Using Standards to promote regulatory compliance and effective exploitation’

Alan Shipman

Group 5 Training Limited

13th September 2017

Standards

What is a ‘Standard’

- Specification
  - Contains requirements
- Code of Practice
  - Based on good practice
- Guidance
  - Information

No Standard is mandatory

GROUP 5 training

Standards

Promote compliance

- Sets out a common ground
- Based on expert opinion
- Enables contract clauses
- Certification of compliance
- Cannot replace ‘legal compliance’

GROUP 5 training

Standards

Types of Standards

- British Standards (BS)
  - Produced specifically for a UK market
- European Standards (BS EN)
  - Where a European applicability is important
- International Standards (BS EN ISO)
  - Where it is truly international

Often develops from BS to ISO

GROUP 5 training

Standards

Brexit

- European Standards will still apply
  - CEN is not part of the EU
  - UK will still have a seat at CEN
- European Standards usually overrule National and International Standards
- European initiative:
  - Privacy by design and by default

DIN Secretariat

Standards

Example – GDPR compliance

- Translates EU Regulation into practice
- PII management
- Basis for implementation
- Management of change
- Exploitation
- Evidence of compliance
- Customer confidence

GROUP 5 training

Data Protection

BS 10012

Data protection – Specification for a personal information management system

A British Standard – applicable in the UK only

Under DPA – 2009 edition

Launched in April – 2017 edition

Data Protection

How does it support UK PLC?

Written by experts

Reviewed by everyone?

Based on consensus

Support from the ICO

GROUP 5 training

Management actions

Contents

- Context of the organization
- Leadership, needs and expectations
- Scope of PIMS
- PIMS Policy
- Roles, responsibilities and authorities
- Data inventory and data flows
- Risk assessment / treatment (PIA?)
- Implementation and demonstration
- Improvement

A PIMS?

GROUP 5 training

International

New project in ISO/IEC

ISO/IEC 27552

Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements

Direct link to Information security

GROUP 5 training

Information Security

- BS EN ISO/IEC 27001

Information technology -- Security techniques -- Information security management systems – Requirements

- BS EN ISO/IEC 27002

Information technology -- Security techniques – Code of practice for information security controls

A truly International Standard

Very widely used

GROUP 5 training

ISO/IEC WD2 27552

Fits in with the ISO Management System model

GROUP 5 training

Information Governance?

ISO 14001
Environmental

BS ISO 27001
Information
Security

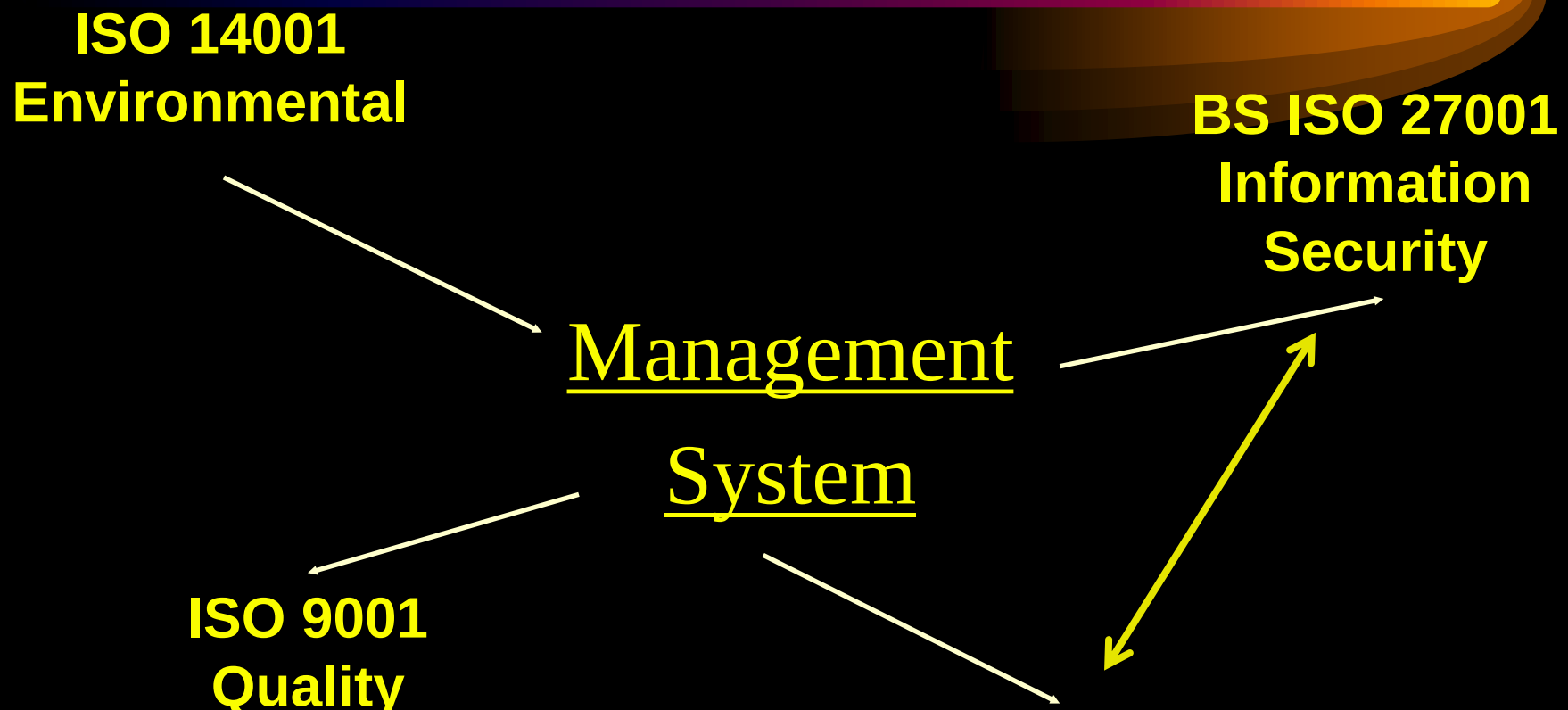
Management System

ISO 9001
Quality

BS 10012
Data protection

GROUP 5 training

Information Governance?



GROUP 5 training

ISO/IEC WD2 27552

International support

- 27 countries supported proposal
- 4 countries against (but have now joined)
- 15 countries agreed to participate
- Includes guidance to SME's
- Enables confidence

ISO/IEC WD2 27552

Scope

- International
- Data controllers
- Data processors
- Joint controller / processor

ISO/IEC WD2 27552

Structure

- 0 Introduction
- 1 Scope
- 2 Normative references
- 3 Terms, definitions and abbreviations
- 4 PIMS -> ISO/IEC 27001
- 5 PIMS -> ISO/IEC 27002
- 6 Guidance for PII controllers
- 7 Guidance for PII processors
- Annex A – Controls for PII controllers
- Annex B – Controls for PII processors

GROUP 5 training

ISO/IEC WD2 27552

Application

- Understand scope of applicability
- Implement privacy risk assessment (PIA)
- Determine privacy risk treatment
- Identify controls
- Use Annex A or B to check for omissions
- Add controls where appropriate

NOTE: Not all controls in Annex A / B are required in every implementation

ISO/IEC WD2 27552

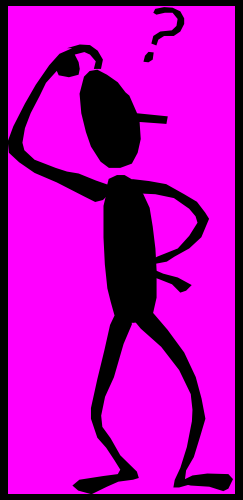
Future

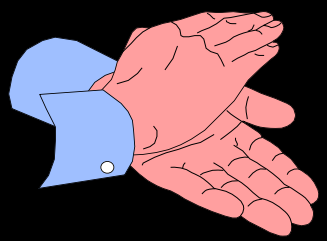
- Certification
- Compliance scheme
- Trust marks
- Worldwide adoption

Who knows????

Thank You

Any Questions?





GROUP 5 training

Contacts

Alan Shipman

Phone: 01923-450527

a.shipman@group5.co.uk

www.group5.co.uk

GROUP 5 training