open.michigan

Author(s): Don M. Blumenthal, 2010

UNIVERSITY OF MICHIGAN

Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Standards and Best Practices

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 9

Regulations and Security

- Information regulatory compliance requirements protect information assets or are dependent upon protected assets because of:
  - What they are (e.g., sensitive personal data, trade secrets…)
  - What they do (e.g., SOX controls and procedures, EEOC reporting requirements, manufacturing integrity and product safety, transaction processing, products & services delivery)
- Creates dependencies upon effective privacy and security for most, if not all, critical business processes and functions
  - Developing accurate business intelligence and metrics, HR management, product and service delivery and support, quality control, work flow management

Emerging Dependencies

- Effective privacy management and compliance is increasingly dependent upon an evolving conception of reasonable security
  - Recent security-focused laws, regulations and standards International requirements focused on information security (Spain, France, Japan, other)
- “Reasonable security” is no longer just secure architecture
  - Tactical protection of IT architecture (networks, applications, databases) but also strategic protection of business objectives and integrity (information in all forms, business strategy and processes)

Security w/Privacy

- Can't have good privacy without effectively coordinated information security and privacy management
- Can't get effective coordination from just a controls catalogue, or a checklist approach to information privacy governance, risk management, and compliance
- Can't get *reasonable* security from just a controls catalogue or checklist

Reasonable Security

- Focused on all information in any form, and all information assets within the organization
  - Information security, not just IT security
  - More than technology tools or “solutions”
- More than acceptance of a recognized control set
  - Use and implementation of controls should be driven by security strategy and governance tied to business objectives and risk management priorities

Reasonable Security Framework

- Scaleable
  - Defined, prioritized, and manageable domains (accurate scoping of business processes and information assets for ISMS implementation)
- Repeatable
  - Iterative methodologies and processes across defined domains of information processing; consistent, comparable results across enterprise
- Defensible
  - Risk-based, fact-specific, continual improvement process approach utilizing auditable principles and controls, documented processes, and accepted frameworks for risk management and control
- Measurable
  - Metrics, capability maturity; clear picture of program status and performance capabilities, continual improvement is objectively defined and tracks changes in risk or business environments
- Sustainable
  - Business-focused, with defined procedures supporting increasing efficiencies in processes and reducing costs of compliance over information lifecycle and adaptations to change in IT and business environments

Common Approaches

- Focus on technology
  - Only 1 component of complex problem
  - Pen test/vulnerability assessment is snapshot
  - IDS/firewall – Q if configuration reflects policy and are systems monitored
- Ad hoc/reactive – as problems arise
- No systematic risk assessment method
- Difficult to communicate needs and objectives to management
  - “We need it” doesn’t work
  - Oversimplifed ROI demand drives actions
  - Segmented security processes

Standards

- Formalized objective approach for building security
- Technology, processes, and people
- Uniformity and predictability
- More general than BP tends to be
  - BP focused on situation/industry
- May be limited or general
  - NIST 800-53
  - ISOs

Best Practices

- Tend to be less formal or have less formal vetting process, although need certain level of attributes
- University of Dallas definition in Cyber Security Guide –
  - Best [p]ractices are those documented, accessible, effective, appropriate, and widely accepted strategies, plans, tactics, processes, methodologies, activities, and approaches developed by knowledgeable bodies and carried out by adequately trained personnel which are in compliance with existing laws and regulations and that have been shown over time through research, evaluation, and practice to be effective at providing reasonable assurance of desired outcomes, and which are continually reviewed and improved upon as circumstances dictate.

Problems

- Conflict with laws and regulations
- Vary by jurisdiction, especially country
- Number of promulgated BPs
  - What applies, what's legitimate
- Number of certs and bodies
- Fitting BP, standards, regs, etc. together
  - Hierarchy of Security Model (Cyber Security Guide, p. 158)

Government Sources

- Government agencies
  - Regulations
- Security of government systems
  - FISMA
  - OMB
  - NIST; e.g., SP 800-30 (ERM), 800-53 (InfoSec)
    - Q how much apply to government contractors
  - Homeland Security Presidential Directives (HSPDs)
- Security of private sector
  - Pending HITECH EHR certification requirements

Private Sources

- COSO – financial process controls ERM framework
- CoBIT – IT management built partly on COSO
- ISO – security
- AICPA/SAS 70 – third party audits of financial services
- ANSI X9 – financial industry technical standards and procedures
- ITU, IEEE, IETF
- OWASP
- PCI-DSS – credit cards

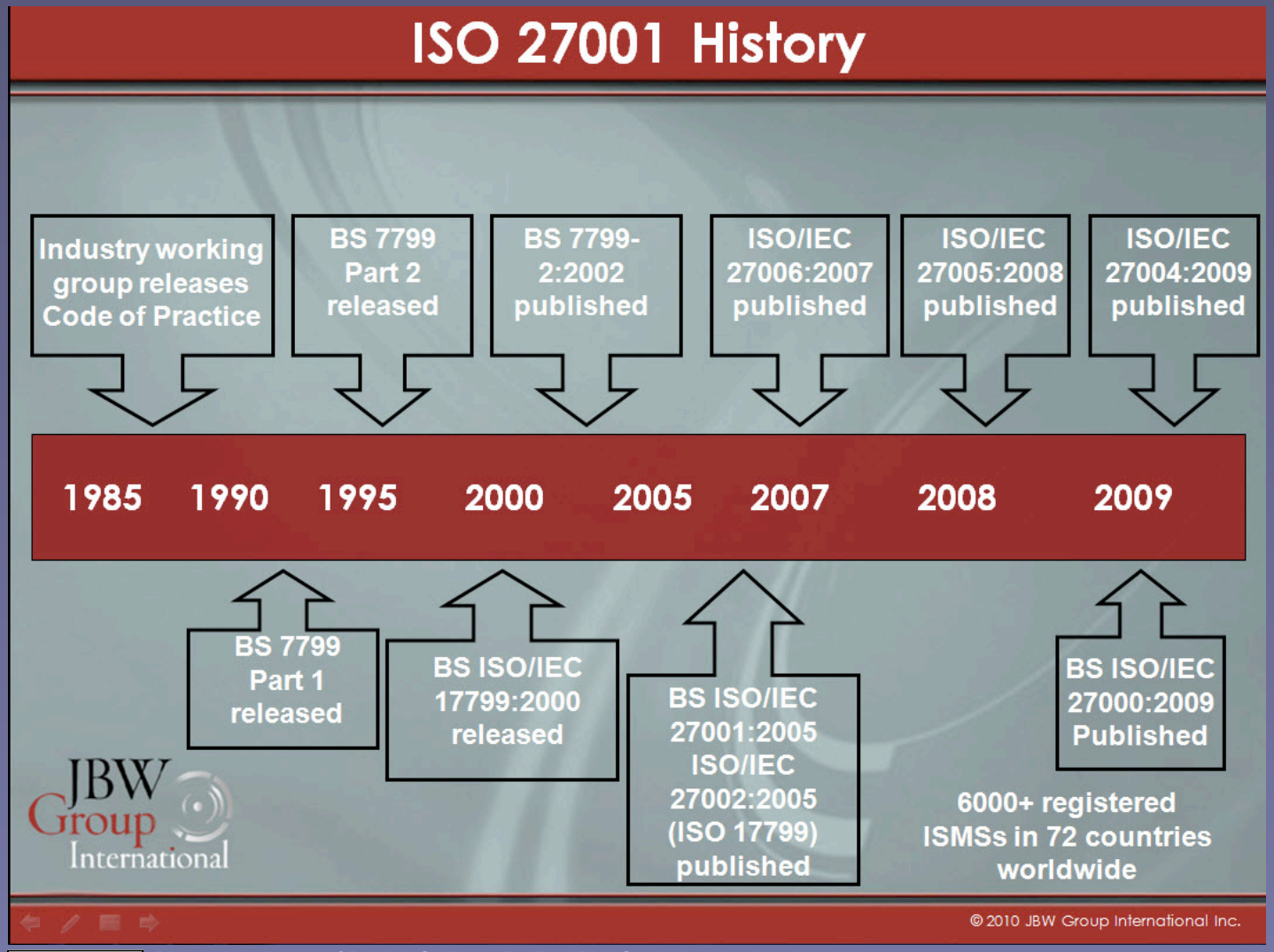
Can Coordinate

- CoBIT – general IT management
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate
- ISO 27000 – security
- PCI – specific to credit cards
- HHS HITECH Act EHR certification

ISO 27000 Series

- **ISO 27000 –** Information Security techniques, fundamentals and vocabulary
- **ISO 27001–** Information Security Management System Requirements (the *standard* to which an organization can certify)
- **ISO 27002–** *Code of Practice* (ISO 17799:2005, guidance for interpretation and implementation of controls)
- **ISO 27003–** ISMS Implementation (proposed)
- **ISO 27004–** Guide for Information Security Metrics and Measures (proposed)
- **ISO 27005–** Guide for Risk Management (currently BS 7799-3:2006)
- **ISO 27006–** International Accreditation Guidelines (Effective October 2007)

27001 Series History



PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

ISO 27001

- Internationally recognized standard for information security management
- Stringent guidelines to evaluate, implement, maintain, and manage security of information assets
- Requires use of comprehensive security controls developed from industry best practices
  - Organizes appropriate implementation of controls to manage risk
- Successful implementation of the ISO 27001 guidelines allows formal accreditation of the information security management system by a governing body

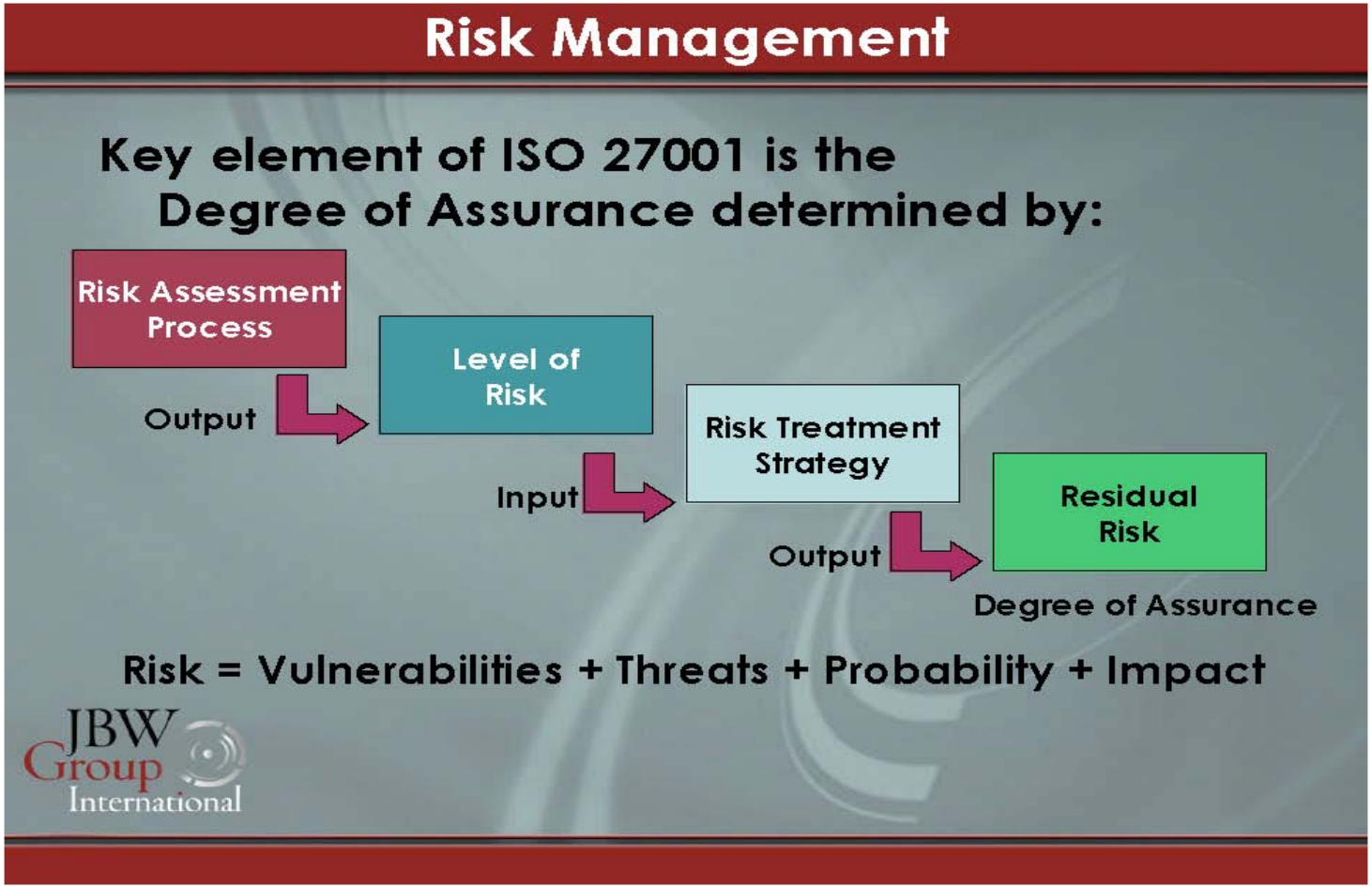
Need for 27001

- Business oriented, process driven
- Comprehensive and holistic framework –Information
- Security Management as a complete system
- Measurable –Valuation of assets and scaling of risk
- Repeatable –Formal approach, structured processes
- Scalable –Facilitates prototyping, adaptable
- Defensible –Articulates level of assurance
- Recognizes information in all forms
- Requires governance (management buy-in and oversight)
- Uses best practices by reference
- Promotes security awareness throughout organization
- Continuous improvement requirement implicit

ISO/IEC 27001:2005

- ISO/IEC 27001:2005 *Information technology – Security techniques –Information security management –Requirements*
  - Is the auditable quality management standard specifying requirements for an Information Security Management System (ISMS)
  - Eight clauses specify the mandatory organization and process requirements for implementing an ISMS in conformance with the standard
  - Annex A enumerates 39 control objectives and 133 controls across eleven categories of information security management to be implemented according to the organization's risk treatment plan for a defined scope of operations and assets

27001 Risk Management



PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

27001 Components

- 1-8 – Basic requirements for quality management system
- Appendix A – List of control objectives and controls
- Appendix C – standards for security, quality management, environment
- Compare to PCI, which doesn't have governance elements beyond basics
- Can use ISO as PCI starting point
  - Core controls
  - Effective mitigation

ISO/IEC 27001: 2005 Structure

Clauses 1-8	1. Scope 2. Normative references 3. Terms and definitions 4. Information security management system (Plan-Do-Check-Act) 9. Management responsibility 10. Internal ISMS audits 11. Management review of the ISMS 12. ISMS improvement	▪ Defines management structure and processes for organizing and conducting appropriate, effective implementation of control objectives and controls ▪ Drives performance and improvement ▪ Criteria for audit, certification of an organization to the standard
Annex A	A.5 Security policy A.6 Organizing 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	▪ Eleven security categories, 39 control objectives, 133 controls ▪ *Code of practice* provides guidance for adapting implementation to risk management objectives and business environments (scope) ▪ Viewed as a starting point for identifying best practices- business objectives, regulatory environment, scope of implementation, risk assessment may indicate more (or fewer)

PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

General Requirements

- Clauses 4-8
- Information Security Management System (ISMS)
- Establish, Manage, Implement, Operate,
- Monitor, Review, Maintain, and Improve the ISMS
- Documentation Requirements
- Control of Documents and Records
- Management Responsibility
- Internal ISMS audits
- Management Review of the ISMS
- ISMS Improvement

ISMS Implementation

- Determine the Scope of the ISMS
- Identify core and support processes
- Identify information assets associated with processes (asset inventory)
- Assess risks to information assets
- Determine an acceptable level of risk (Degree of Assurance)
- Select control objectives and controls
- Implement and remediate controls
- Perform internal audits, reviews and gap analysis
- Identify and treat non-conformities

ISMIS Implementation Timetable

- Depends on several variables -
- Scope of the ISMS
- Complexity of the environment
- Maturity of the existing Information
- Security Program
- Resources available for implementation
- Skill sets of the available resources

ISMS Implementation Costs

- Also depends on several variables
  - Required speed of implementation
  - Protracted implementation doesn't *necessarily* mean lesser cost
- ISMS implementation often provides greater visibility and control of spending for security
- Direct ROI for certification

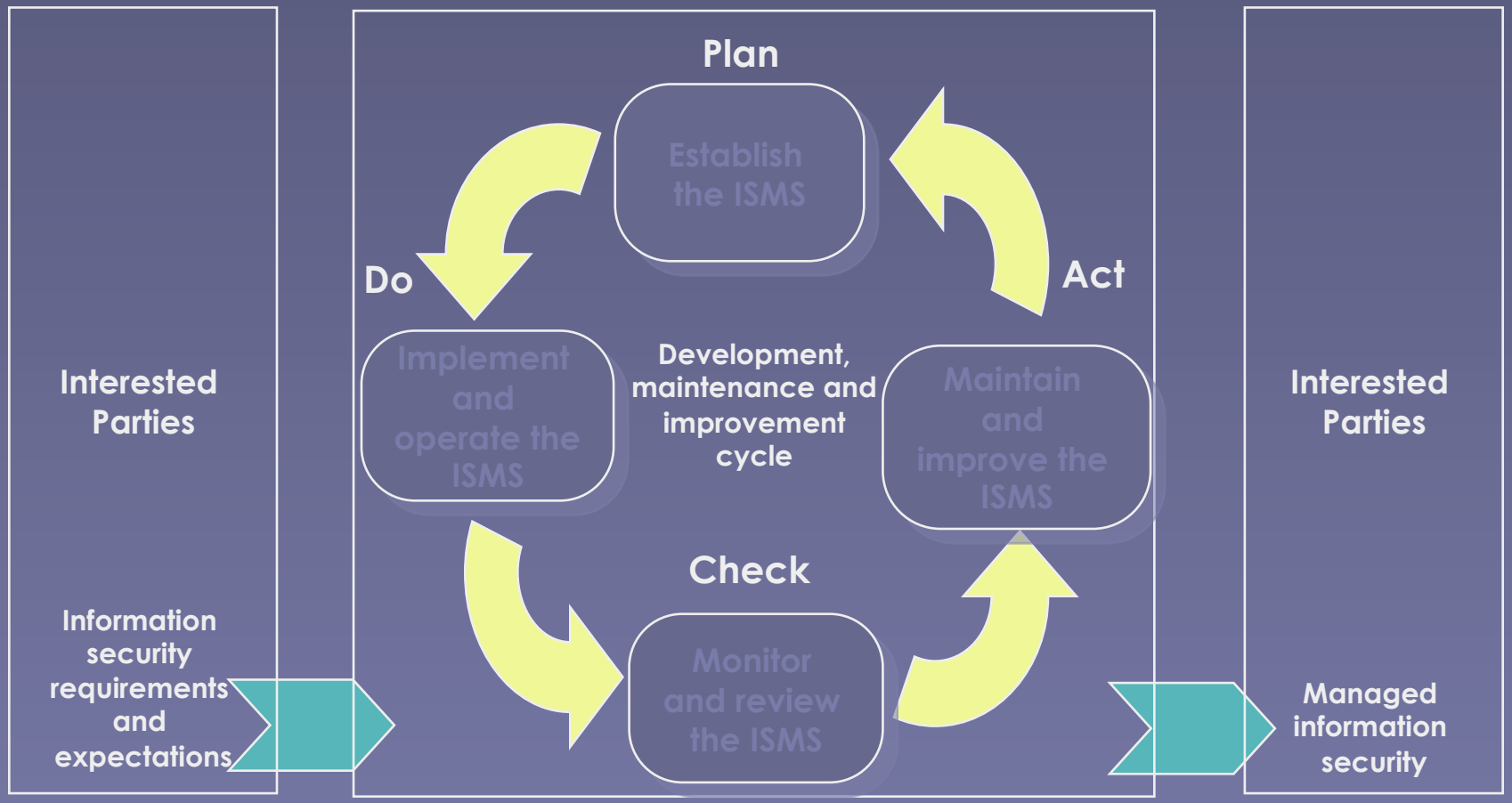
Key ISMS Requirements

- 4.2.1c- organizations must define and document their risk approach (risk management methodology)
  - Methodology must allow risk assessment to generate comparable and reproducible results
  - Risk assessment and risk treatment plans must be reviewed and updated at least annually
  - Assessors will look for clear relationships from control selection to risk assessment and treatment plan, to ISMS policy and objectives
- 4.2.2d- organizations must measure the effectiveness of controls
  - Iterated in 4.2.3c; effectiveness measurement is essential to determining performance of the ISMS in managing risk; ties performance, risk management objectives to business objectives
  - Effectiveness measurement is essential to continual improvement of the ISMS

Control Objectives & Controls

- Appendix A
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Key to Implementation: Plan-Do-Check-Act Methodology



PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

BS ISO/IEC 27001:2005

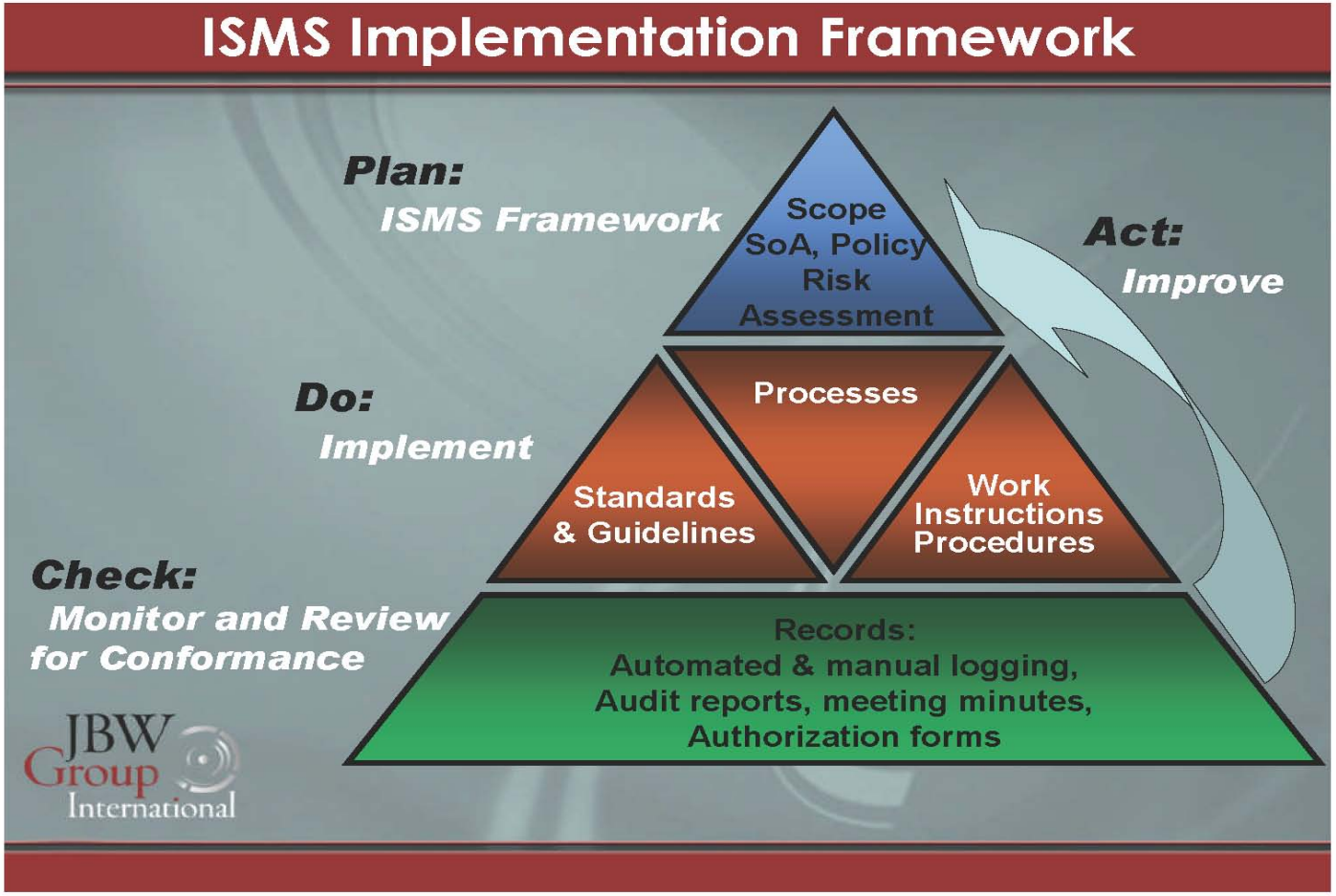
Plan-Do

- **Plan**
  - Define scope of implementation & corresponding business objectives for information security management
  - Establish ISMS policy, define risk assessment approach, identify & analyze risks, develop options for managing risks, select control objectives & controls
  - Obtain management approval for ISMS implementation and residual risk
- **Do**
  - Develop and implement the risk treatment plan, define effectiveness metrics, deliver training, manage resources & operations

Check-Act

- **Check**
  - Monitoring & review procedures (records, automated & manual logging, incident detection & prevention, audits)
  - Review of effectiveness of ISMS policy, objectives, controls to ensure that security objectives have been met and continue to support business
  - Review effectiveness of controls to ensure that security objectives have been met
  - Review risk assessment, risk acceptance criteria and residual risk
- **Act**
  - Identify and implement improvements to the ISMS
  - Take appropriate preventative and corrective actions
  - Ensure improvements and actions achieve intended objectives

ISMS PDCA



PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

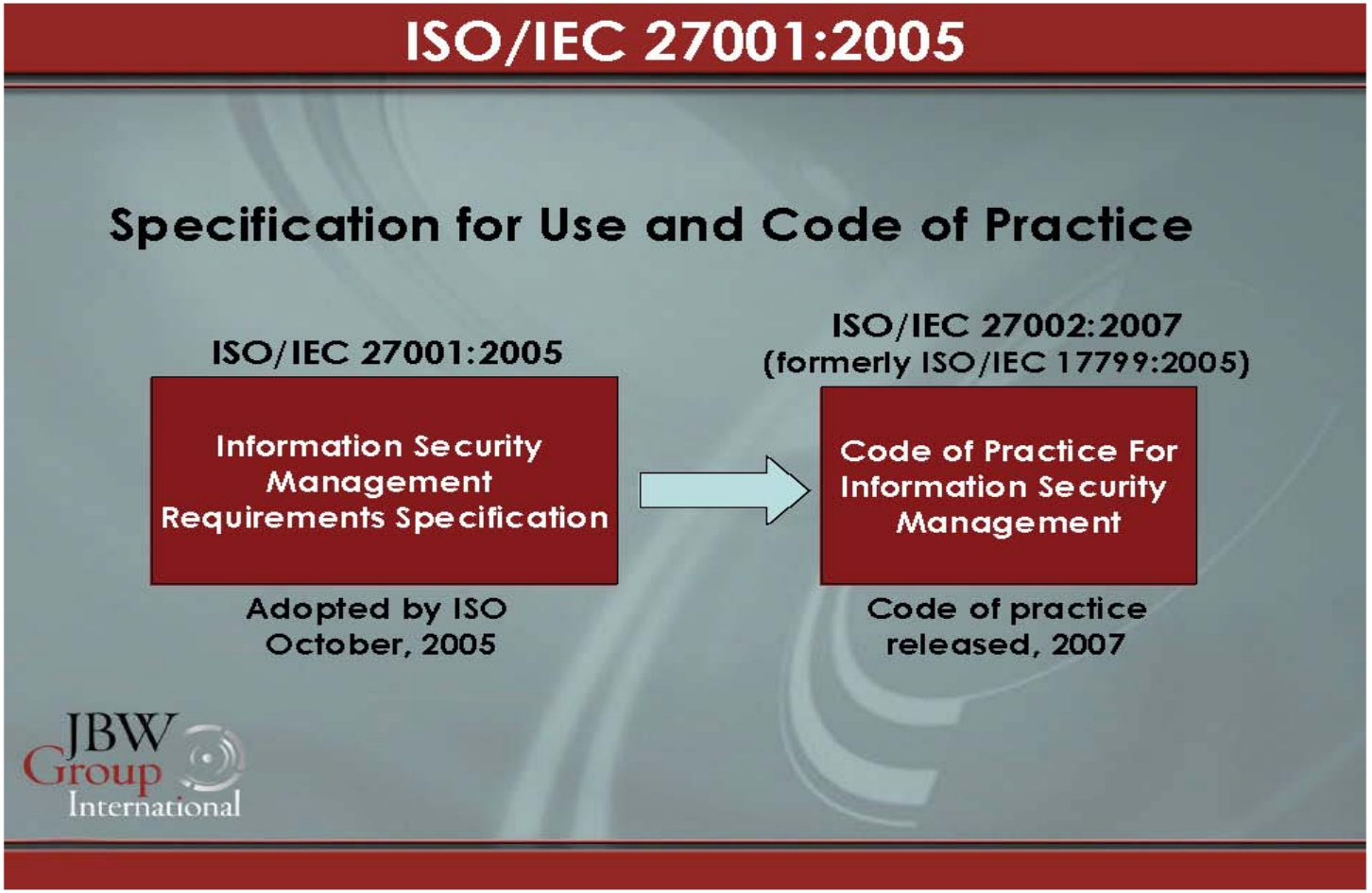
Governance vs Control Objectives

- 27001 not just a catalogue of accepted control objectives and controls
- Governance is critical
- Often confused with 27002 C*ode of Practice*

ISO/IEC 27002

- *Information technology –Security techniques – Code of practice for information security management*
- Provides high-level guidance for relating risk assessment to implementation of Annex A control objectives and controls
- Provides guidance on implementing Annex A controls per the risk assessment and risk treatment plan required in Clause 4 of the standard- guides method of implementing controls relative to scope requirements and risk management objectives

27001-27002



PD-INEL Diagram courtesy of Patrick Sullivan, Ph.D., JBW Group International.

Code of Practice

- Excludes key management requirements (governance, risk management, continual improvement)
  - Does not appropriately consider business objectives and strategies
  - Leads to under-utilization of the control objectives and controls- "one-size-fits-all" adoption of Annex A or *Code of Practice*
  - Potential under-determination of risk; robust risk analysis methodology (BS7799-3, OCTAVE) may not be utilized
  - No metrics for process maturity, control effectiveness
  - Significantly impedes effective coordination of information security across organization, and effective coordination of privacy and security management
- Benefits are diminished, costs look big, requirements look monolithic

Typical Problem

- Most organizations focus on most of Do and some of Check
- Wholesale implementation of controls (almost exclusive focus on *Code of practice*); not strategically shaped to scope requirements or business objectives
  - Emphasis on control checklists, monitoring, audit
- Separates information security from business objectives at the management process level
  - Information security becomes less strategic, more tactical; less comprehensive and more initiative/deadline-driven
  - Re-inventing the wheel replaces continual improvement
- Retail approach to PCI-DSS is a classic example
  - Heavy emphasis on presence/absence of controls, use of the audit checklists, passing the assessment
  - Little apparent effort to relate PCI implementation to wider organizational information security needs, objectives, processes

Specific Benefits to CPO's

- Plan-Do-Check-Act methodology detailed in the requirements specification is the key to effective coordination, integration of privacy and security management
  - Establishes management structures & processes for identification of common business, compliance objectives
  - Establishes a framework for integrated risk management approach
  - Establishes a framework for meaningful selection, interpretation, implementation and management of control objectives and controls
  - Ensures comprehensive support/coverage of privacy requirements by information security processes and controls
  - Basis for coordinated metrics for performance, criteria and objectives for improvement

ISO Certification

- Auditor Competency
  - International Register of Certificated Auditors (IRCA) www.irca.org
- ISO 27006:2007 - auditor competency
- Certification
  - Self-certification (internal audit)
  - Second party audit (business and vendor partners)
  - Third party audit (independent and registration audits)

Certification Audit Process

- Register organization's ISMS is registered
- Pre-assessment audit (optional)
- Stage 1 Audit –Documentation review
- Stage 2 Audit –Implementation audit
- Periodic surveillance audits (every six months or annually)
- Re-certification audit every three years
- Publicly available Statement of Applicability

ISO 27006

- International Accreditation Guidelines
- Accredits individuals/companies using ISOs in analyses
- Very important
- Very difficult, more than British standard that it replaced
- Verisign and BSI offering accreditation program
  - End run around ISO?