



A Standards-based Approach to Information Security and Risk Management

American Society for Quality

Friday, October 19, 2007

John B. Weaver

CISSP, CISA, CISM, CPP

President/CEO

Principal Consultant

A Standards-Based Approach

Agenda

- ❑ Introduction
- ❑ Information Security
- ❑ Current Business Environment
- ❑ Current Practices
- ❑ ISO 27001:2005
- ❑ PDCA and ISMS Implementation
- ❑ Implementation Time and Cost
- ❑ Certification

JBW Group International Inc.

- ❑ Full Service Information Security Consultancy Founded in 2002
- ❑ Focus on Information Security Management System Implementation
- ❑ Fortune 50 companies to small businesses
- ❑ Clients in the United States, Canada, Japan, Mexico and Central America
- ❑ Legal and Regulatory Compliance for Healthcare, Pharmaceutical Clients
- ❑ Energy, Banking and Finance, Telecommunications, Software, Legal
- ❑ Methodology based on Internationally Recognized Information Security Standard
- ❑ Information Security and Corporate Governance
- ❑ Find more information at www.jbwgroup.com



John B. Weaver – CISSP, CISA, CISM, CPP

- ❑ 20 years as a professional paranoid
- ❑ Former director of World-wide & IP network security at Qwest
- ❑ Vice President, Executive Board of InfraGard - FBI/private sector coalition for the protection of the national infrastructure.
- ❑ Taught BS 7799 Audit and Implementation for BSI Americas
- ❑ IRCA-certified ISO 27001 auditor
- ❑ Disaster Preparedness Planning
- ❑ Security program deployment
- ❑ Incident response

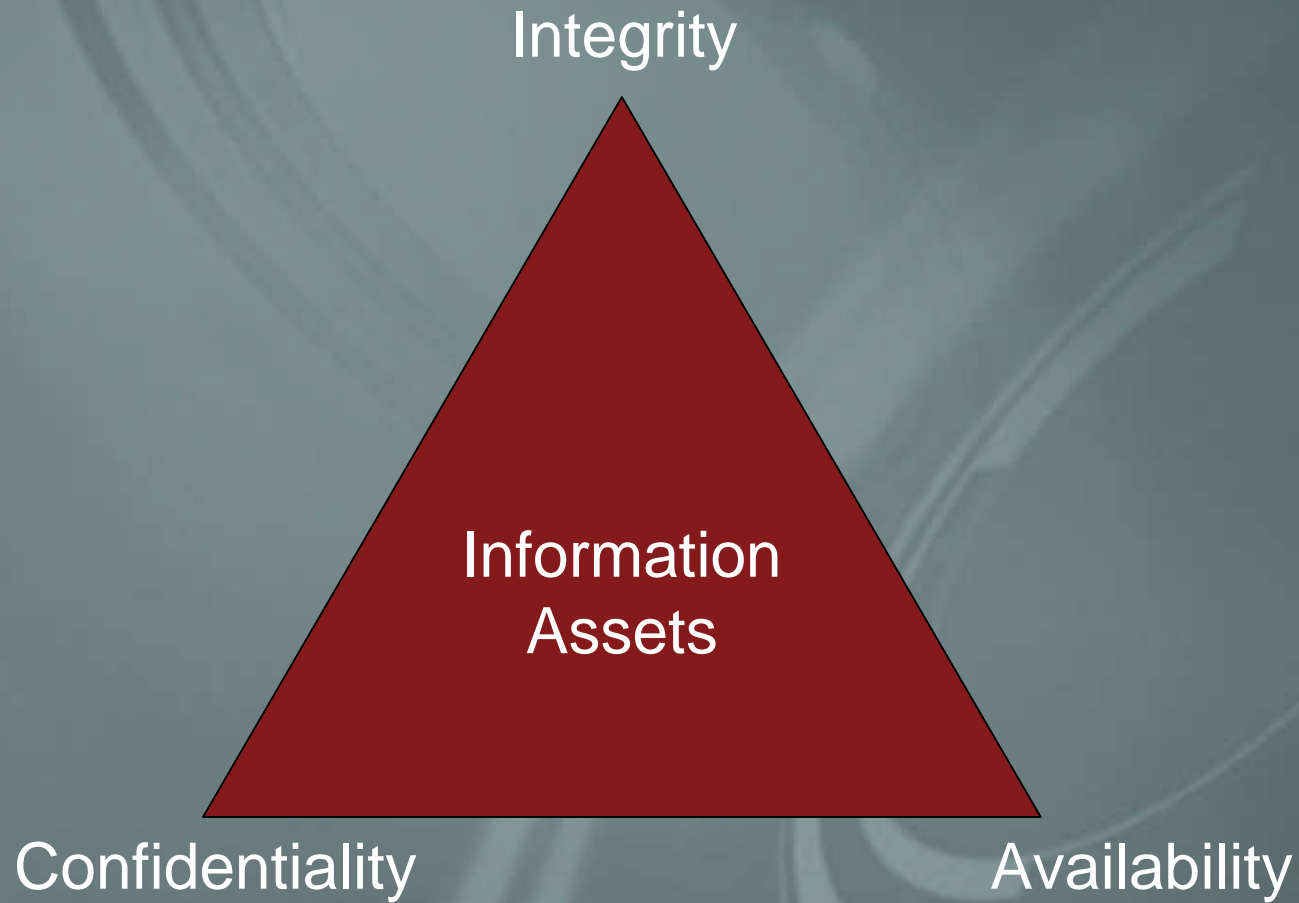


Information Security

“Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.”

BS ISO/IEC 17799:2005

Information Security



Business Environment

- ❑ Internet connectivity is ubiquitous
- ❑ Businesses and government *require* network inter-connectivity
- ❑ Infrastructure has expanded as technology and business processes have become inseparable
- ❑ Out-sourcing of critical business functions is common
- ❑ Migration of critical business functions off-shore
- ❑ Legal and regulatory compliance

Points to Consider

- ❑ All regulatory compliance requirements that impact business either specify protection of information assets or are dependent upon protected assets
- ❑ Information regulation (any regulation that affects information assets) creates dependencies upon effective privacy and security for most, if not all, critical business processes and functions

US Legal & Regulatory Environment

- ❑ Sarbanes-Oxley Act
- ❑ PCAOB Rel. 2004-001 Audit Section
- ❑ SAS94
- ❑ Fair Credit Reporting Act (FCRA)
- ❑ AICPA Suitability Trust Services Criteria
- ❑ SEC CFR 17: 240.15d-15 Controls and Procedures
- ❑ NASD/NYSE 240.17Ad-7 Transfer Agent Record Retention
- ❑ GLBA (15 USC Sec 6801-6809) 16 CFR 314
- ❑ Appendix: 12 CFR 30, 208, 225, 364 & 570
- ❑ Federal Financial Institutions Examination Council (FFIEC) Information Security
- ❑ FFIEC Business Continuity Planning
- ❑ FFIEC Audit
- ❑ FFIEC Operations
- ❑ Health Insurance Portability and Accountability Act (HIPAA) § 164
- ❑ 21 CFR Part 11 – FDA Regulation of Electronic Records and Electronic Signatures
- ❑ Payment Card Industry Data Security Standard (PCI-DSS)
- ❑ Federal Trade Commission (FTC)
- ❑ CC1798 (SB1386) and similar in 33 states
- ❑ Federal Information Security Management Act (FISMA)
- ❑ USA PATRIOT
- ❑ Community Choice Aggregation (CCA)
- ❑ Federal Information System Controls Audit Manual (FISCAM)
- ❑ General Accounting Office (GAO)
- ❑ FDA 510(k)
- ❑ Federal Energy Regulatory Commission (FERC)
- ❑ Nuclear Regulatory Commission (NRC) 10CFR Part 95
- ❑ Critical Energy Infrastructure Information (CEII)
- ❑ Communications Assistance for Law Enforcement Act (CALEA)
- ❑ Digital Millennium Copyright Act (DMCA)
- ❑ Business Software Alliance (BSA)
- ❑ Customs-Trade Partnership Against Terrorism (C-TPAT)
- ❑ Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002))

Global Legal & Regulatory Environment

- ❑ New Basel Capital Accord (Basel-II)
- ❑ Payment Card Industry Data Security Standard (PCI-DSS)
- ❑ Society for Worldwide Interbank Funds Transfer (SWIFT)
- ❑ Personal Information Protection Act (PIPA) – Canada
- ❑ Personal Information and Electronic Documents Act (PIPEDA) – Canada
- ❑ Personal Information Privacy Act (JPIPA) – Japan
- ❑ SafeSecure ISP – Japan
- ❑ Federal Consumer Protection Code, E-Commerce Act – Mexico
- ❑ Privacy and Electronic Communications (EC Directive) Regulations 2003
- ❑ Directive 95/46/EC Directive on Privacy and Electronic Communications – European Union
- ❑ Central Information System Security Division (DCSSI) Encryption – France
- ❑ Federal Data Protection Act (FDPA - Bundesdatenschutzgesetz - BDSG) of 2001 – Germany
- ❑ Privacy Protection Act (PPA) of Schleswig-Holstein of 2000 – Germany
- ❑ US Department of Commerce “Safe Harbor”

Recent US Security Breaches

- ❑ January, 2007: TJX – 45,700,000 credit and debit card numbers, 455,000 driver's license information compromised
- ❑ February, 2007: Veterans Administration – records of over 600,000 active duty and retired veterans compromised
- ❑ March, 2007: US Navy College Office – 3 laptops containing personal information of current and past active duty sailors reported missing
- ❑ April, 2007: Georgia Department of Community Health – 3rd party vendor reported a disk containing personal records of 2,900,000 missing
- ❑ May, 2007: Transportation Security Administration – disk drive containing payroll information of 100,000 current and former TSA employees was stolen
- ❑ June, 2007: State of Ohio – A backup tape containing information on 500,000 state employees and taxpayers was stolen from an intern's car
- ❑ July, 2007: Fidelity National Information Services – an employee at a subsidiary stole financial information of 8,500,000 individuals

Common Security Approach

- ❑ **Technology-focused**
 - ❑ Only one component of a complex problem
 - ❑ Penetration testing, vulnerability assessment
 - Snapshot in time
 - ❑ IDS and Firewall deployment
 - Does configuration reflect policy?
 - Are these systems monitored?
- ❑ **Ad hoc and reactive**
 - ❑ Solutions implemented as problems arise
- ❑ **No systematic method of assessing Risk or Performance**
 - ❑ What information assets are being protected?
 - ❑ Is it the correct solution?
- ❑ **Difficult to communicate needs and objectives to management**
 - ❑ “We need it” usually doesn’t fly
 - ❑ Oversimplified ROI demand, rather than defined risk tolerances and accurate metrics drives requirements & implementation.
 - ❑ Typically results in segmented security processes across operational or functional divisions, duplication of efforts/resources in some areas, critical gaps in others, and inconsistencies across the organization

Common Roadblocks

- ❑ **Process silos within organizations- privacy, security, compliance, IT management, risk management, etc.**
 - ❑ **Increases segregation of core information security competencies**
- ❑ **Multiple compliance initiatives with different ownership for regulations & standards**
 - ❑ **More points of accountability, more decision layers to manage**
- ❑ **Communication gaps**
 - ❑ **Various initiatives duplicate effort, reporting channels aren't effectively coordinated, reporting content isn't appropriately defined or analyzed**

Common Roadblocks

- ❑ **Compartmentalization of strategies, solution sets**
 - ❑ Security is a technology problem, privacy is a legal problem; risk management is driven by compliance, compliance is driven by regulatory detail and deadlines- coordination and comprehensiveness are sacrificed to expedience
- ❑ **Comforting Assumptions**
 - ❑ Absence of incidents = compliance; compliance = security; security = technology tools; technology tools = enterprise solutions; and more
- ❑ **Capability-maturity gaps**
 - ❑ Assurance, compliance outcomes appear to be met but the processes, procedures and corresponding records that support them aren't systematic, fully defined, consistent or documented

Emerging Standard

- ❑ **Process Approach**
 - ❑ Foundations in regulatory guidance for implementing security requirements (GLBA, HIPAA, FISMA, etc.), reflected in recent enforcement trends
- ❑ **Fact-Specific, Risk-Based, Continual Improvement**
 - ❑ Security controls must adapt/respond to existing threats and to changes in the business and information environments
- ❑ **Core components**
 - ❑ Asset inventory; periodic risk assessment; controls appropriate to risks; management of third parties; education and training, monitoring and testing; review and revise



See Thomas Smedinghoff, "The New Law of Information Security: What Companies Need to do Now", *The Computer and Internet Lawyer Journal*, November 2005.

Corporate Governance

Corporate Governance and Information Security Management are Inseparable in the Modern Organization

The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital

-Peter Drucker, "Management Challenges for the 21st Century", *Harpers Business*, 1993

The road to information security goes through corporate governance...The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Board and CEO's

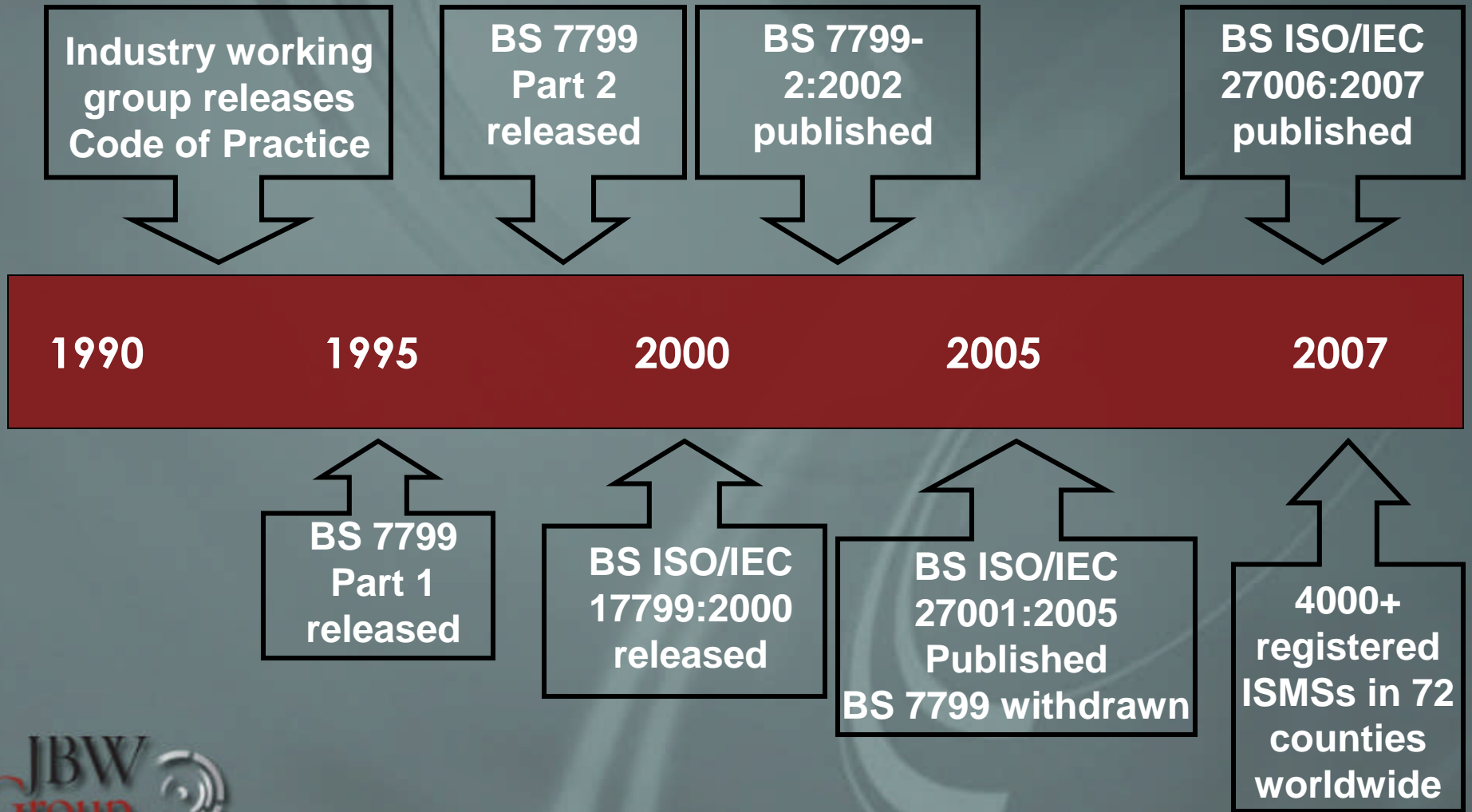
-National Cyber Security Summit Task Force, *Corporate Governance Report*, "Information Security Governance: A Call to Action", 2004



Why ISO/IEC 27001:2005?

- ❑ 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)
- ❑ Utilizes “best practices”
- ❑ Promotes security awareness throughout organization
- ❑ Incorporates Total Quality Management (continuous improvement)

ISO 27001 History



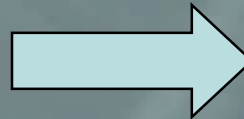
ISO/IEC 27001:2005

Code of Practice and Specification for Use

ISO/IEC 27002:2007
(formerly ISO/IEC 17799:2005)

**Code of Practice For
Information Security
Management**

Code of practice
released, 2007



ISO/IEC 27001:2005

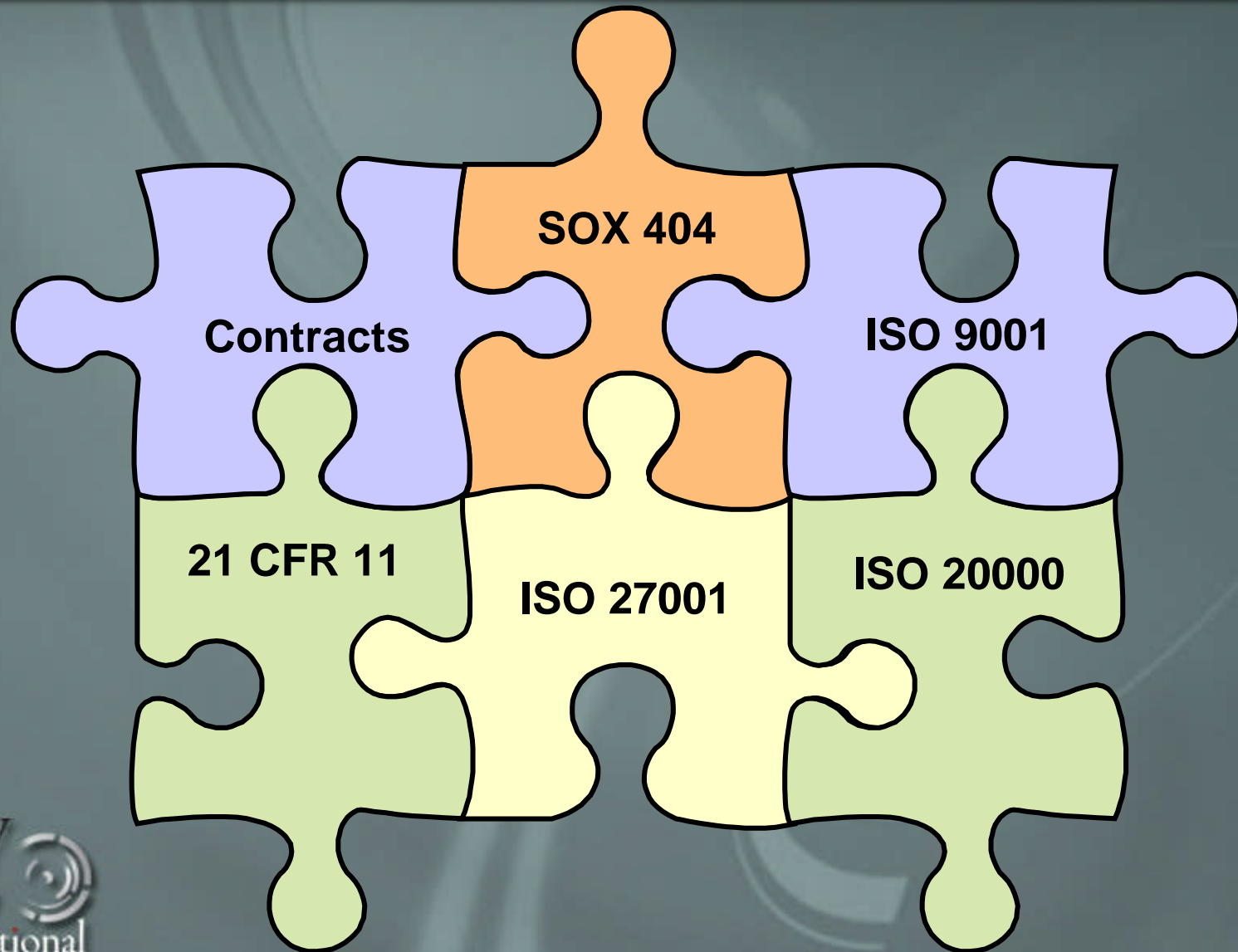
**Information Security
Management
Requirements Specification**

Adopted by ISO
October, 2005

ISO 27000 Series

- ❑ ISO 27000 – Information Security techniques, fundamentals and vocabulary
- ❑ ISO 27001 – Information Security Management System Requirements
- ❑ ISO 27002 – Code of Practice (ISO 17799:2005)
- ❑ 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 (10/2007 implementation deadline)

Standards Complement Regulations



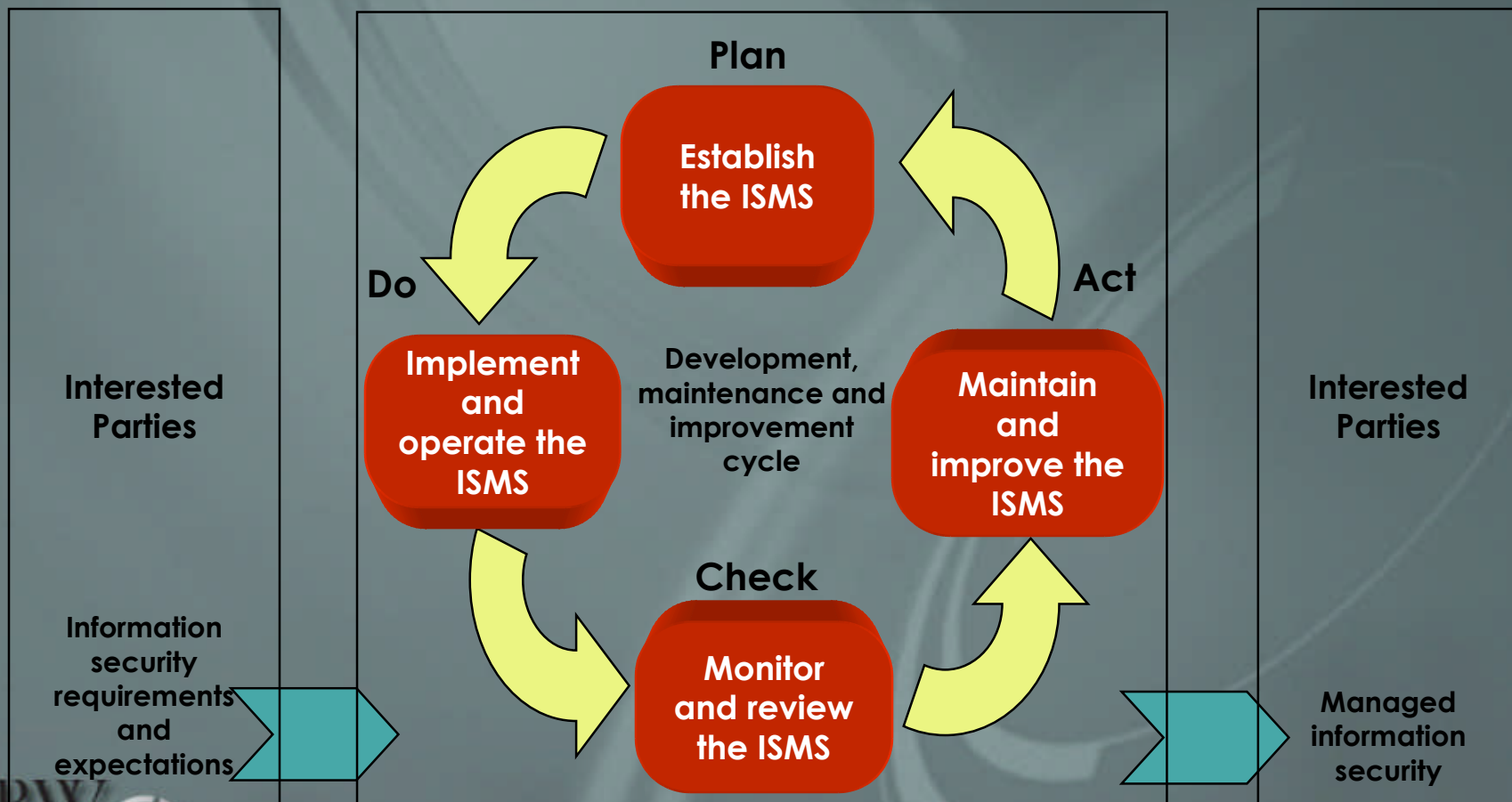
ISO 27001:2005

General Requirements (Clauses 4-8)

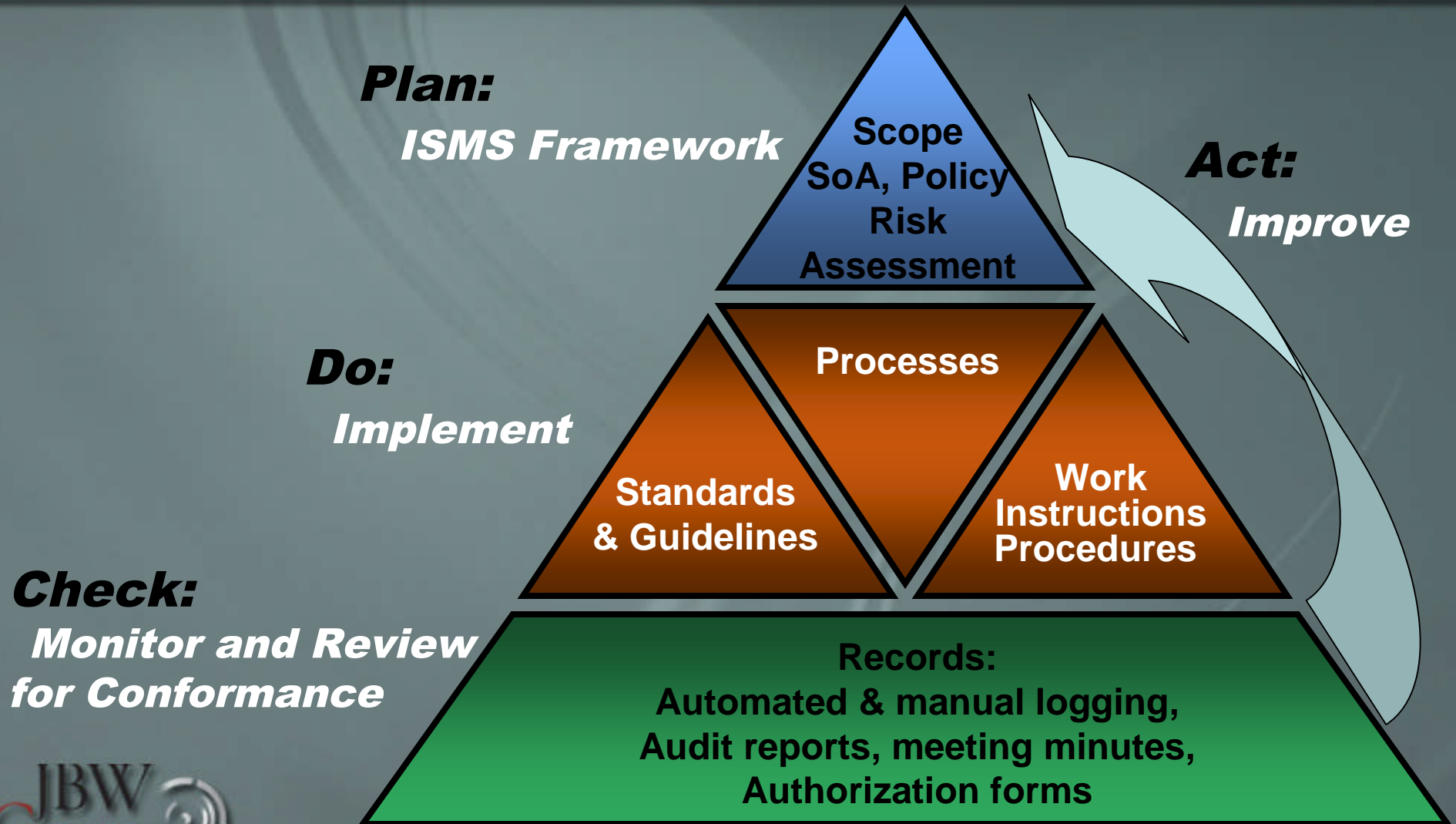
Control Objectives and Controls (Annex A)

- ❑ 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

PDCA Applied to ISMS

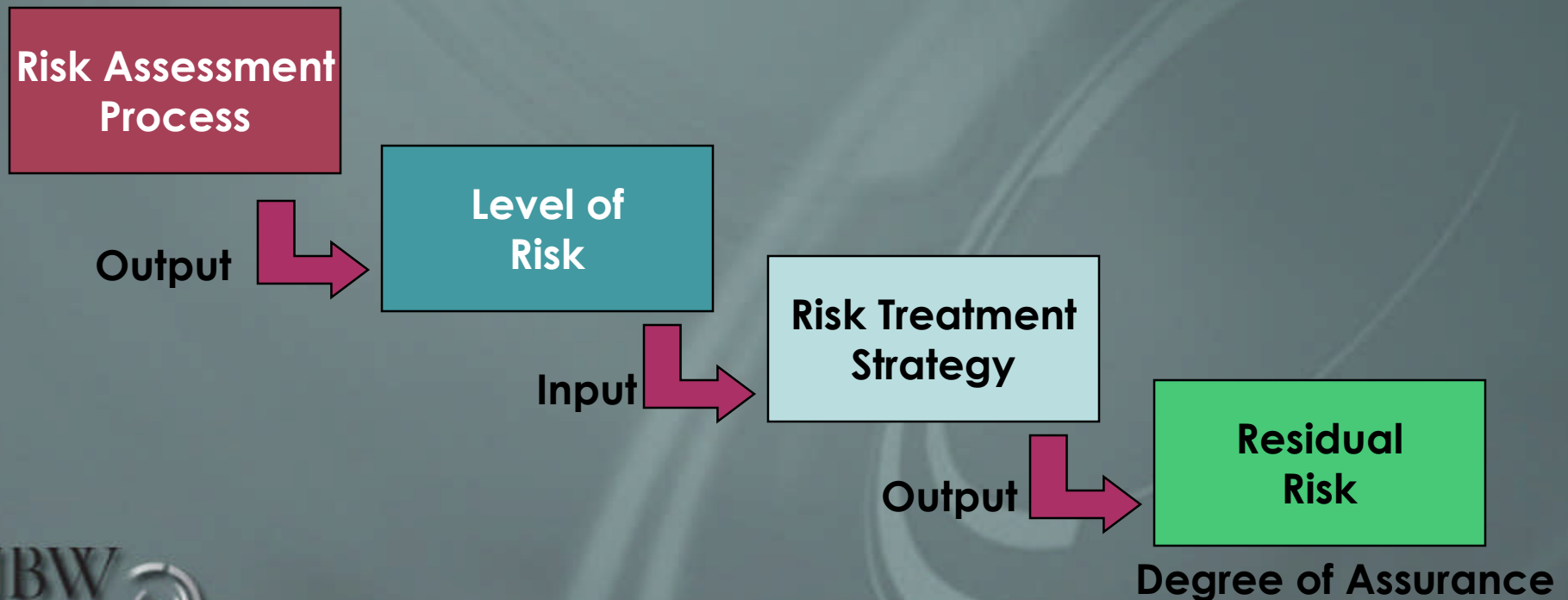


ISMS Implementation Framework



Risk Management

Key element of ISO27001 is the
Degree of Assurance determined by:



10-Step Implementation Strategy

Determine customer needs and business requirements



Scope

Identify core and support processes

Identify and value assets (within the context of their use)

Assess and analyze assets (Vulnerabilities → Threats → Probabilities → Impacts → Risks → Degree of Assurance)

Validate acceptable risk

Select control objectives and controls



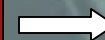
Perform gap analysis

Define method of implementation for each control

Produce Statement of Applicability (SoA) and summary of controls

Implement and remediate controls

Perform internal audits and reviews



Identify non-conformities,
Potential non-conformities and
opportunities for improvement

ISMS Implementation Timetable

Time to implement an ISMS 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

Cost to implement an ISMS 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

Certification

Certification Bodies Accredited by:

- ❑ ANSI-ASQ National Accreditation Board (ANAB) – www.anab.org
- ❑ United Kingdom Accreditation Service (UKAS) – www.ukas.org

Registrars:

- ❑ SRI Quality Registrar (SRI) – www.sriregistrar.com
- ❑ Bureau Veritas Quality Institute (BVQi) – www.bvqi.com
- ❑ British Standards Institute (BSI) – www.bsiamericas.com
- ❑ Over 70 accredited registrars

Certification

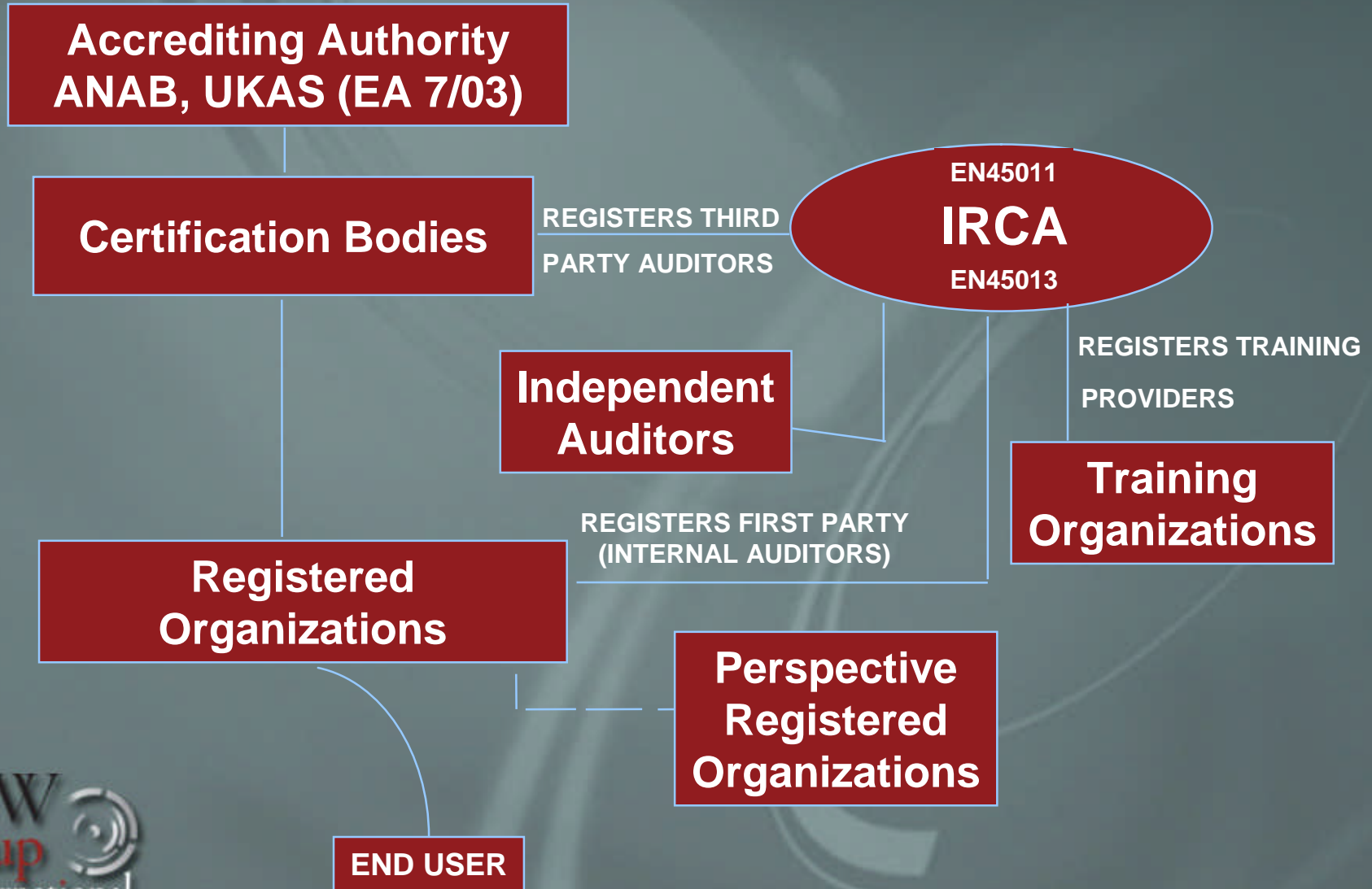
Auditor Competency

- ❑ 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



Certification

Certification Audit process

- ❑ An organization's Information Security Management System (ISMS) is registered
- ❑ Pre-assessment audit (optional)
- ❑ Stage 1 Audit – Documentation review
- ❑ Stage 2 Audit – Implementation audit
- ❑ Surveillance audits every six months
- ❑ Re-certification audit every three years
- ❑ Publicly available Statement of Applicability



John B. Weaver

CISSP, CISA, CISM, CPP

President/CEO – Principal Consultant

JBW Group International

PO Box 19393

Minneapolis, MN 55419

877.97.27001

www.JBWGroup.com