



Eating An Elephant:
Successful
Implementation of
ISO 27001:2005

ASIS International
2nd Asia-Pacific Conference
Wednesday, February 13, 2008

John B. Weaver
CISSP, CISA, CISM, CPP
President/CEO
Principal Consultant

A Standards-Based Approach

Agenda

- ❑ Introduction
- ❑ Information Security
- ❑ Current Business Environment
- ❑ Common Approach to Information Security
- ❑ 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

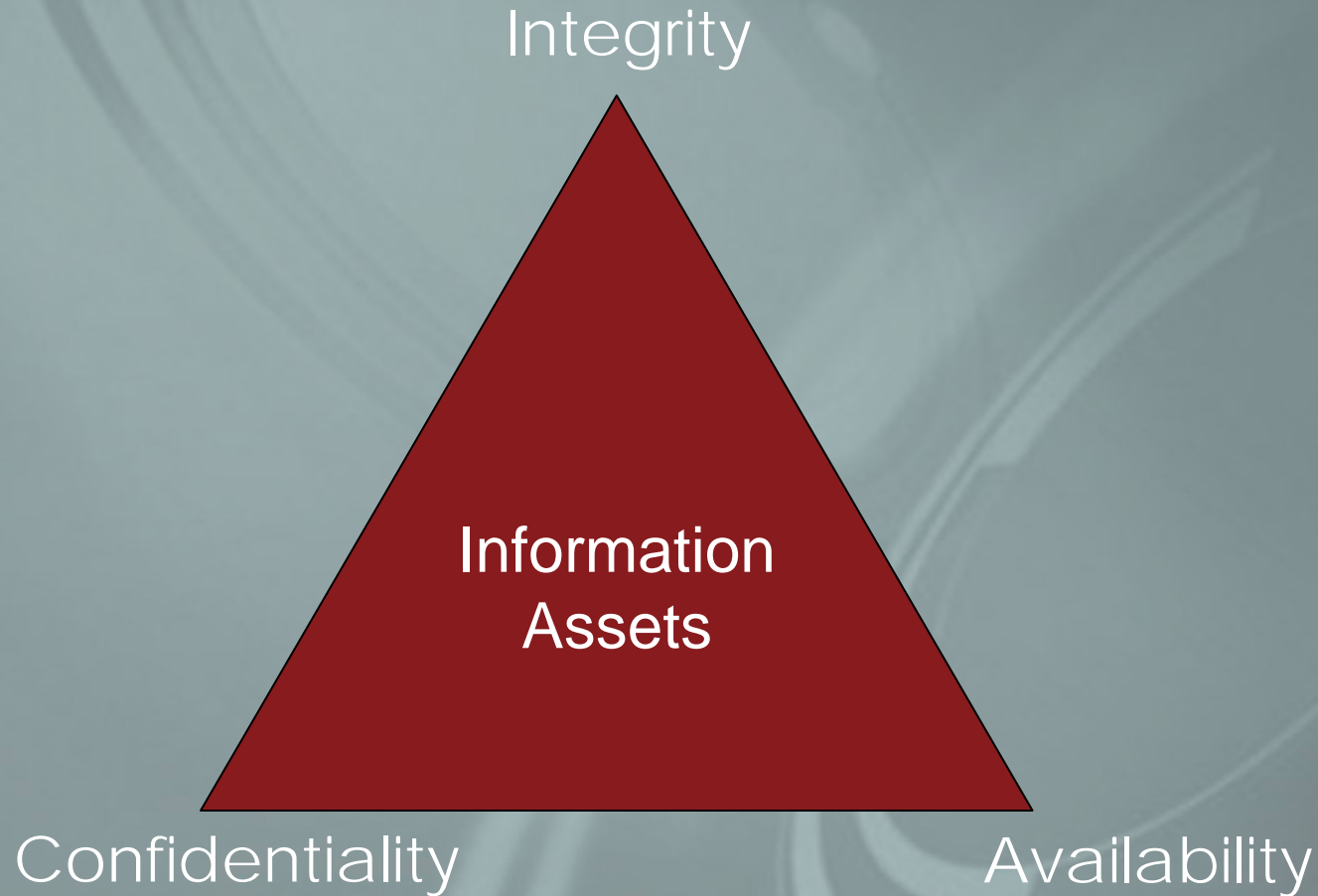
- ❑ 20 years as an information security professional
- ❑ Former director of World-wide & IP network security for an international telecommunications company
- ❑ Taught standard Audit and Implementation for BSI Americas
- ❑ IRCA-certified ISO 27001 auditor
- ❑ Subject matter expert in:
 - ❑ Security program deployment
 - ❑ Disaster Preparedness Planning
 - ❑ Incident response management
- ❑ Guided organizations in multiple verticals to successful certification on the first audit

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 drive information security requirements

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 drives requirements & implementation
 - ❑ Segmented security processes across operational or functional divisions

Emerging Standard

- ❑ Process Approach
 - ❑ Foundations in regulatory guidance for implementing security requirements (GLBA, HIPAA, FISMA, BASIL-2, 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

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

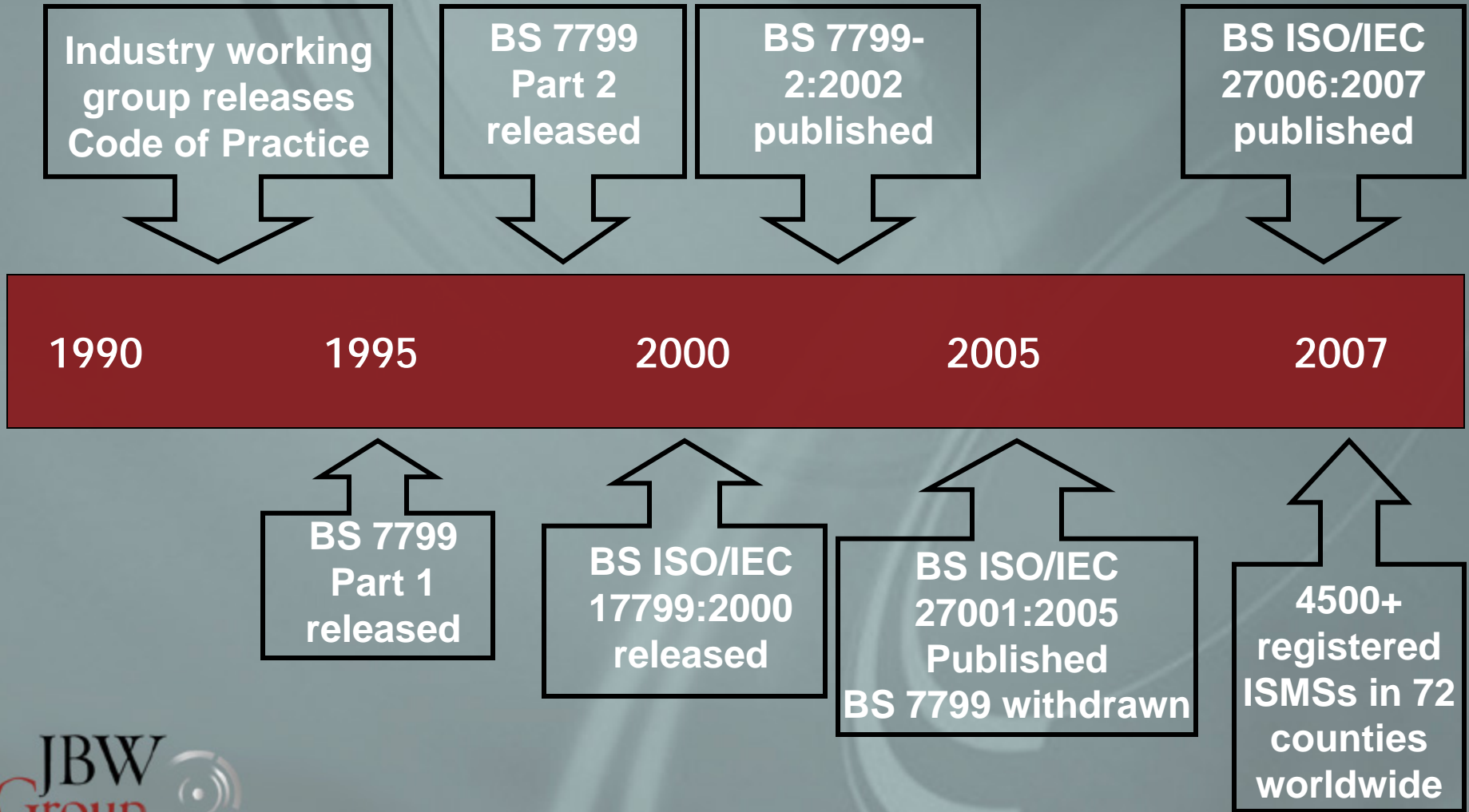
Why ISO/IEC 27001:2005?

- ❑ 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)

Reasonable Security

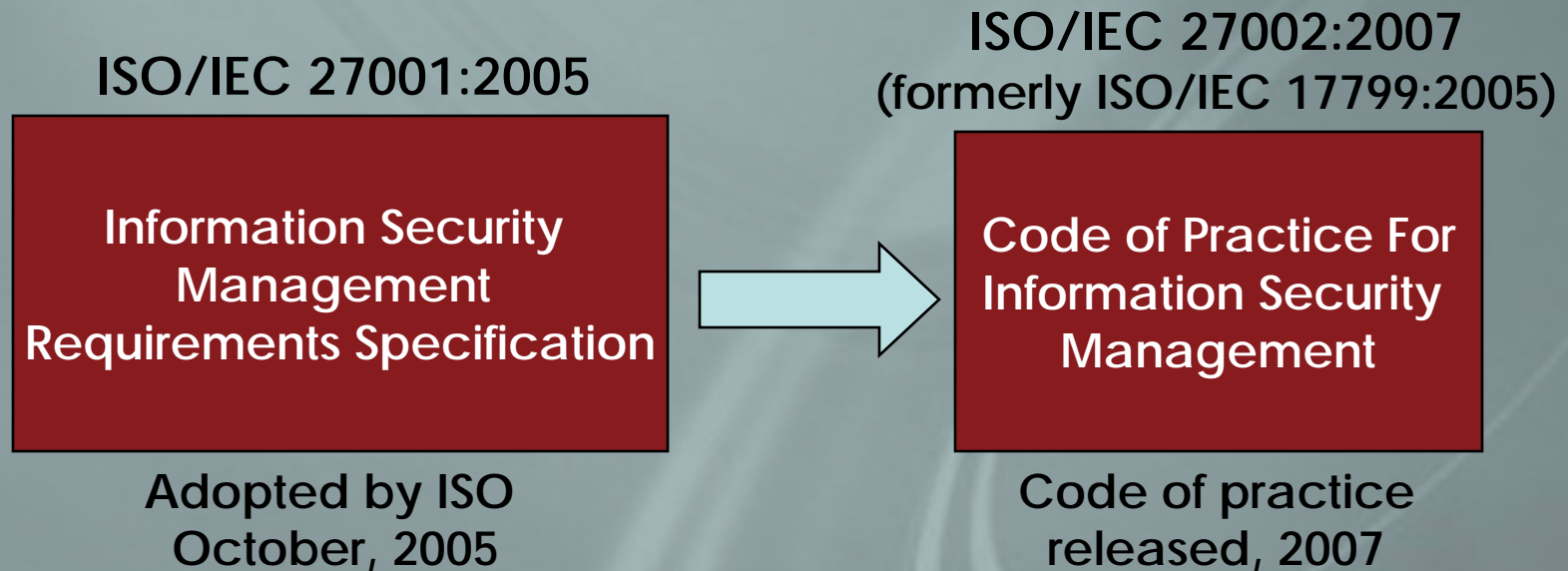
- ❑ Focused on all information in any form, and all information assets within the organization
 - ❑ Information security, not just IT security (the architecture-networks, applications, databases, hardware)
- ❑ More than technology tools or “solutions”
 - ❑ Purchase orders for vendor products (firewalls, monitoring tools, encryption, content filters, other) aren’t the same thing as an information security strategy
- ❑ 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

ISO 27001 History



ISO/IEC 27001:2005

Specification for Use and Code of Practice



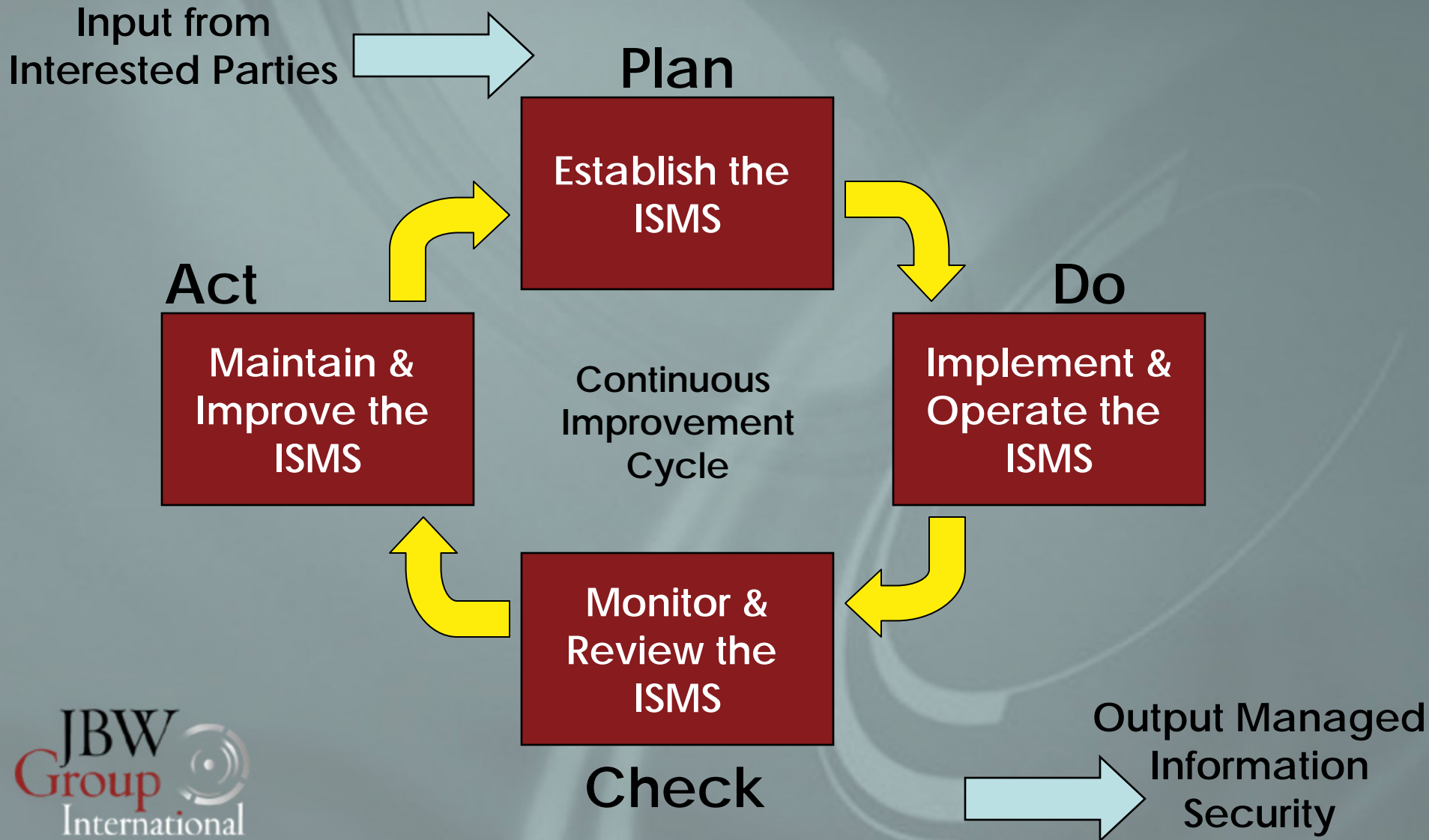
ISO 27000 Series

- ❑ ISO 27000 – *Information Security techniques, fundamentals and vocabulary*
- ❑ ISO 27001:2005 – *Information Security Management System Requirements*
- ❑ ISO 27002:2005 – *Code of Practice (formerly 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 27006:2007 – *International Accreditation Guidelines (10/2007 implementation deadline)*

General Requirements (Clauses 4-8) Information Security Management System (ISMS)

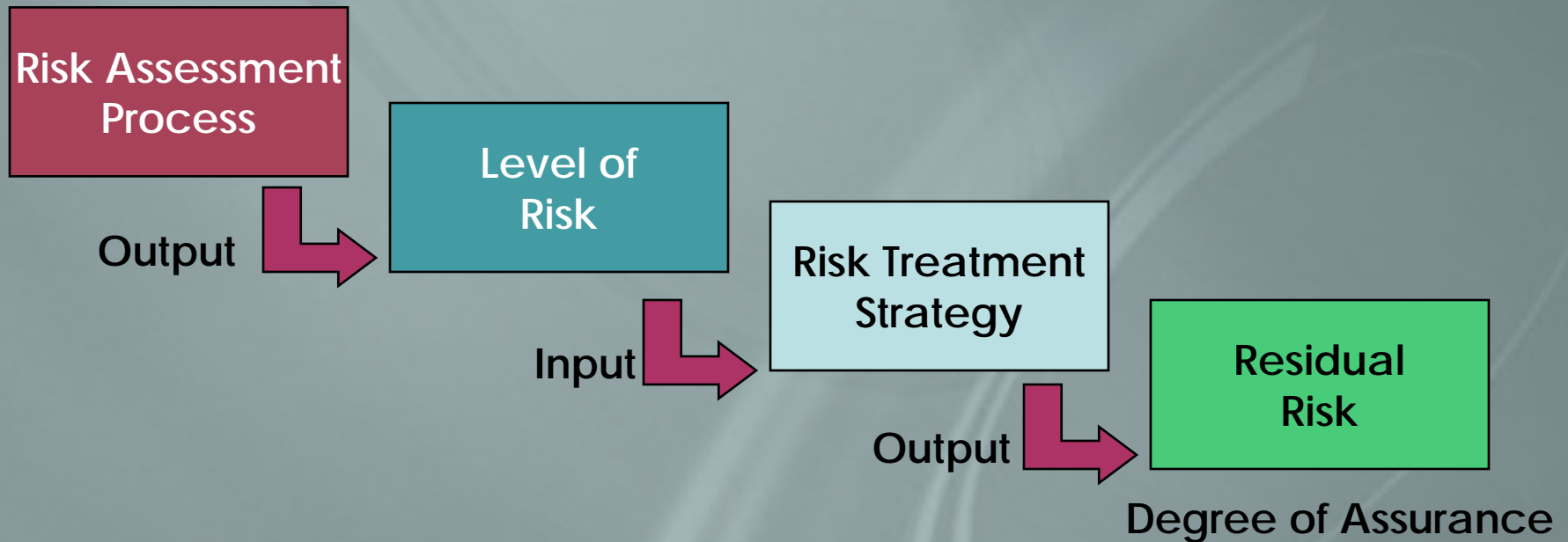
- ❑ Establish, Manage, Implement, Operate, Monitor, Review, Maintain, and Improve the ISMS
- ❑ Documentation Requirements
- ❑ Control of Documents and Records
- ❑ Management Responsibility
- ❑ Internal ISMS audits
- ❑ Management Review of the ISMS
- ❑ ISMS Improvement

Plan-Do-Check-Act



Risk Management

Key element of ISO 27001 is the Degree of Assurance determined by:

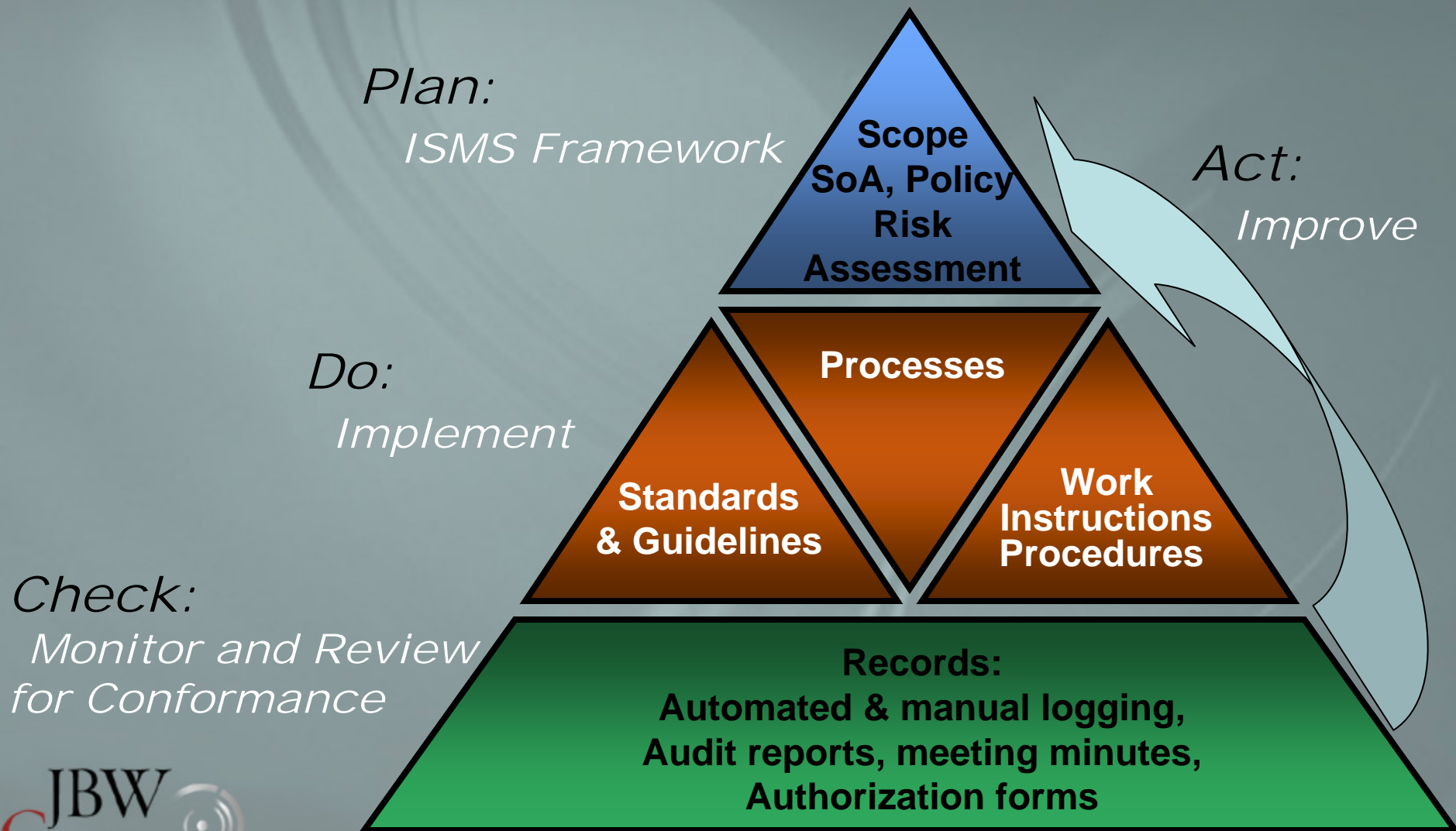


Risk = Vulnerabilities + Threats + Probability + Impact

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

ISMS Implementation Framework



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

Common Implementation Errors

- ❑ 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
- ❑ Separates information security from business objectives at the management process level
- ❑ Heavy emphasis on presence/absence of controls, utilization of the audit checklists, passing the assessment
- ❑ Little apparent effort to relate implementation to wider organizational information security needs, objectives, processes

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

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 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
- ❑ Periodic surveillance audits (every six months or annually)
- ❑ 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 USA

+1.877.97.27001

www.JBWGroup.com