



ISO 27001 for Chief Privacy Officers:  
Using the Standard to Develop  
Integrated Information Privacy and  
Security Management

**Secure 360<sup>o</sup>™**

May 13-14, 2008  
St. Paul, MN

**Patrick F. Sullivan, Ph.D**

Principal Consultant

# Agenda

- ❑ Privacy, Security and the Emerging Legal Standard for Reasonable Security
- ❑ What is ISO 27001
- ❑ Implementing an Information Security Management System
- ❑ Using an ISMS to Achieve Integrated Information Privacy and Security Management

# JBW Group International Inc.

- ❑ **Information Security Consultancy Founded in 2002**
- ❑ **Clients in the United States, Canada, Japan, Mexico and Central America**
- ❑ **Information Security Governance, Risk Management and Compliance for clients in**
  - **Financial Services (Retail Banking, Insurance, Credit Card Issuers)**
  - **Healthcare, Pharmaceuticals**
  - **Energy, Telecommunications, Software, Legal**
  - **Retail**
- ❑ **Methodology based on Internationally Recognized Information Security Standard**



# Points to Consider

- ❑ All regulatory compliance requirements that impact business either specifically protect information assets or are dependent upon protected assets
  - Information assets must be protected either because of what they are (e.g., sensitive personal data, trade secrets, etc.) or what they do (e.g., SOX disclosure controls and procedures, EEOC reporting requirements, manufacturing integrity and product safety, transaction processing, delivery of products & services)
- ❑ 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
  - Developing accurate business intelligence and metrics, HR management, product and service delivery and support, quality control, work flow management

# Problem- Emerging Dependencies

- ❑ Effective privacy management and compliance is increasingly dependent upon an evolving conception of reasonable security
  - Recent security-focused laws, regulations and standards (security breach notification, “reasonable security” requirements, PCI-DSS); recent enforcement (Lilly, BJ’s Wholesale Club, other)
  - International requirements focused on information security (Spain, France, Japan, other)
- ❑ “Reasonable security” is no longer just secure architecture (firewalls, intrusion detection, etc)
  - Information security management has evolved far beyond its earlier scope and constructs- from tactical protection of IT architecture (networks, applications, databases) to strategic protection of business objectives and integrity (information in all forms, business strategy and processes)

# Privacy Development

- Legal and regulatory drivers have shaped emergence of the privacy management domain focused on business use of personal information and data subject's rights and protections
  - Regulations typically focus on data subject rights and protections (notice, choice, access/correction, redress), and appropriate policies to ensure these
  - Legal compliance has been the obvious near-term priority
  - Privacy was seen as having a strategic focus (appropriate policies around information use and protection of data subjects, assuring legal collection and use of personal information)
  - Security typically addressed tactical protection of assets (confidentiality, integrity, availability of networks, systems, applications, proprietary data)
    - Security usually addressed as a segregated process within privacy models, generally in non-specific “safeguards” principles
    - Or, as in GLB, HIPAA, segregated in the statute and in the implementing regulations themselves

# 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



# Result

- ❑ Functional segregation was typical and remains the case in many organizations...
- ❑ ...Leading to greater or lesser degrees of effective coordination, based on the skills, awareness and defined competencies of CPO/CISO roles, level of industry regulation, other factors
- ❑ But under the emerging legal standard of reasonable security:
  - Information security management has evolved far beyond its earlier scope and constructs- from tactical protection of IT architecture to strategic protection of business objectives and integrity (information and processes)
  - Privacy management and compliance have become less dependent on the construction of policies and increasingly dependent upon information security management

# Emerging Legal Standard

- Reasonable security is a risk-based, fact-specific process characterized by:
  - Defined governance structures & processes
  - Identification, inventory and valuation of information assets
  - Periodic risk assessment (threats, vulnerabilities, impacts)
  - Controls appropriate to identified risks and adaptable to changes in the business/technical/threat environments
  - Management of risks associated with third parties
  - Training and awareness
  - Monitoring of controls performance and effectiveness
  - Appropriate management review of processes, policies and controls
  - Continual improvement
- And should be business-driven, scaleable, defensible, sustainable



See: "Where We're Headed: New Trends in the Law of Information Security," Thomas J. Smedinghoff, *Privacy and Data Security Law Journal*, January 2007

# 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

# What is ISO 27001?

- ❑ Internationally recognized standard for information security management
  - Published and governed by International Organization for Standardization (ISO)
- ❑ 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

# What is ISO 27001?

- ❑ **Not just a catalogue of accepted control objectives and controls!**
- ❑ The most common misconception of ISO 27001 is to confuse the standard with the *Code of practice*
  - Key management requirements (governance, risk management, continual improvement) are excluded
    - 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

# ISO/IEC 27001:2005

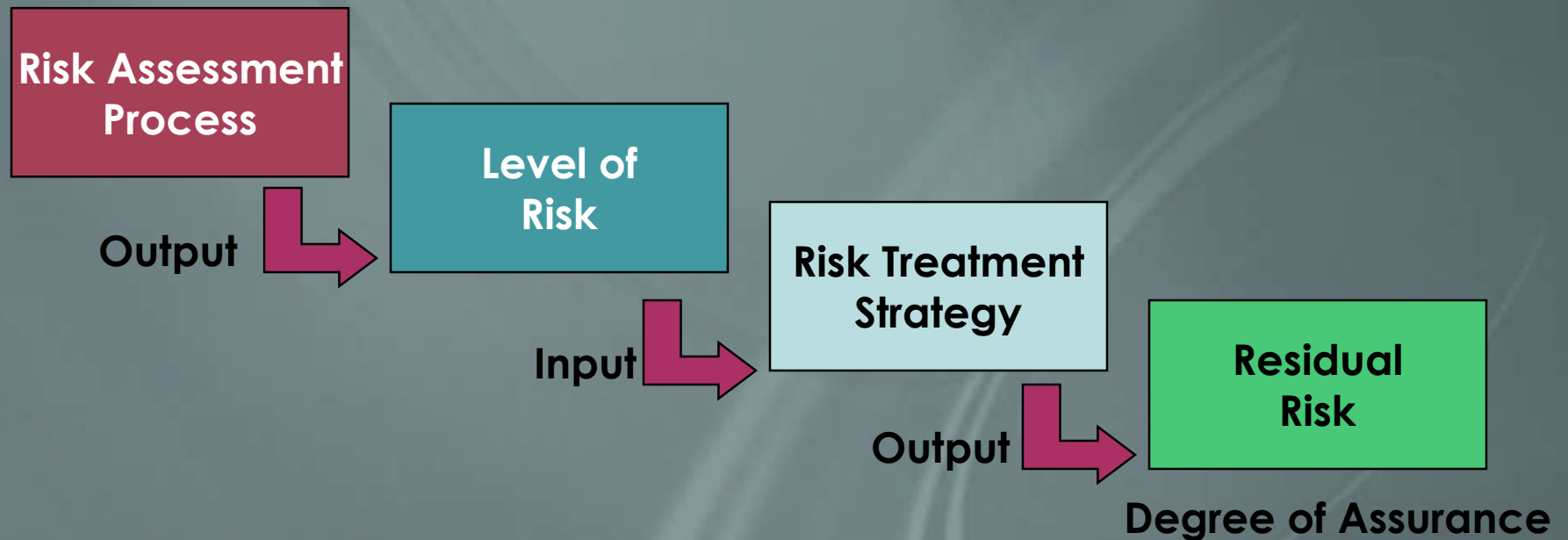
- ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management – Requirements*
  - Is the auditable quality management standard specifying requirements for an Information Security Management System (ISMS)
  - Eight clauses specify the mandatory organization and process 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

# 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

# Risk Management

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



**Risk = Vulnerabilities + Threats + Probability + Impact**

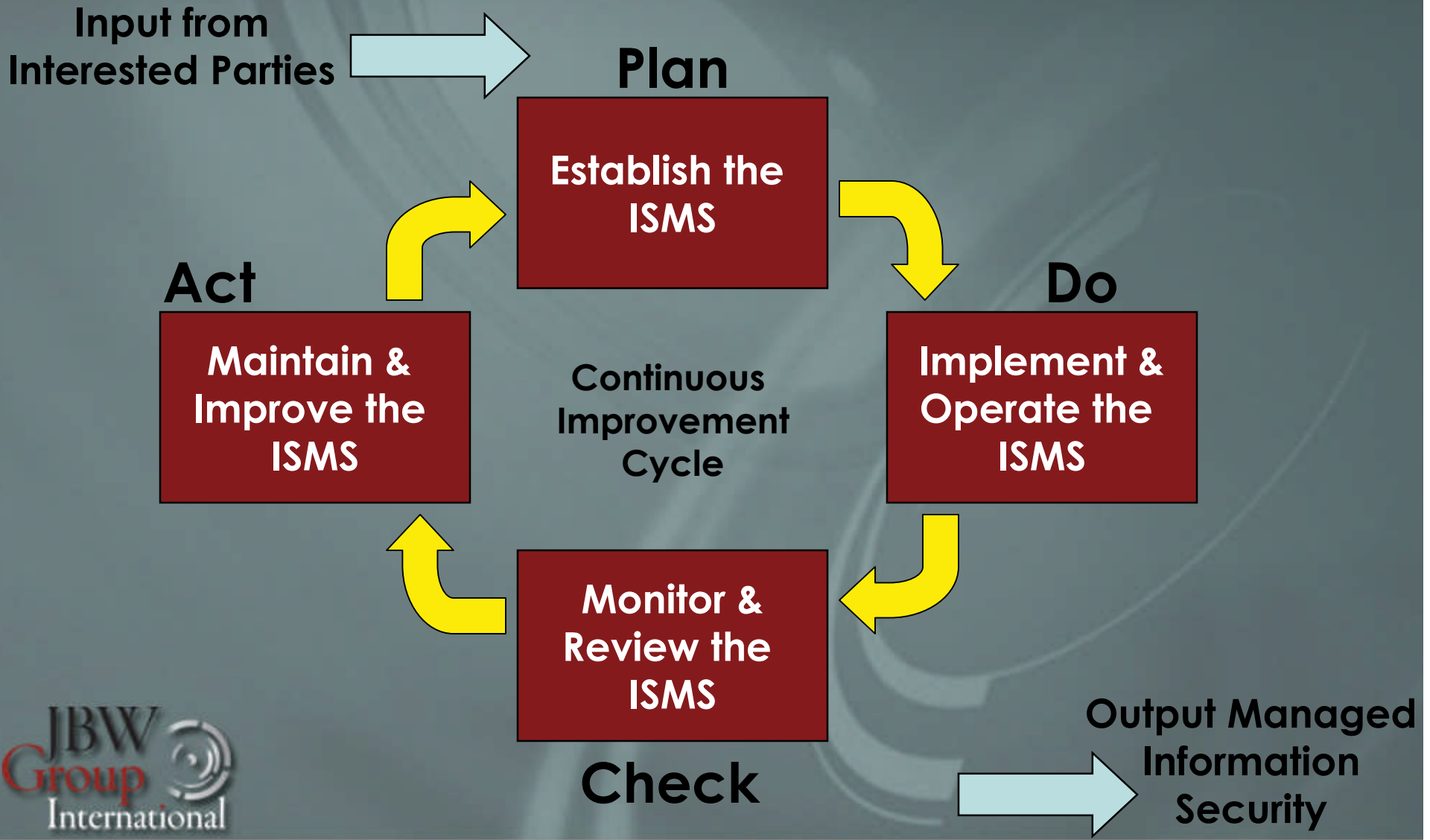
# ISO/IEC 27002

- ❑ ISO/IEC 27002:2007 *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
  - Replaces BS ISO/IEC 17799:2005

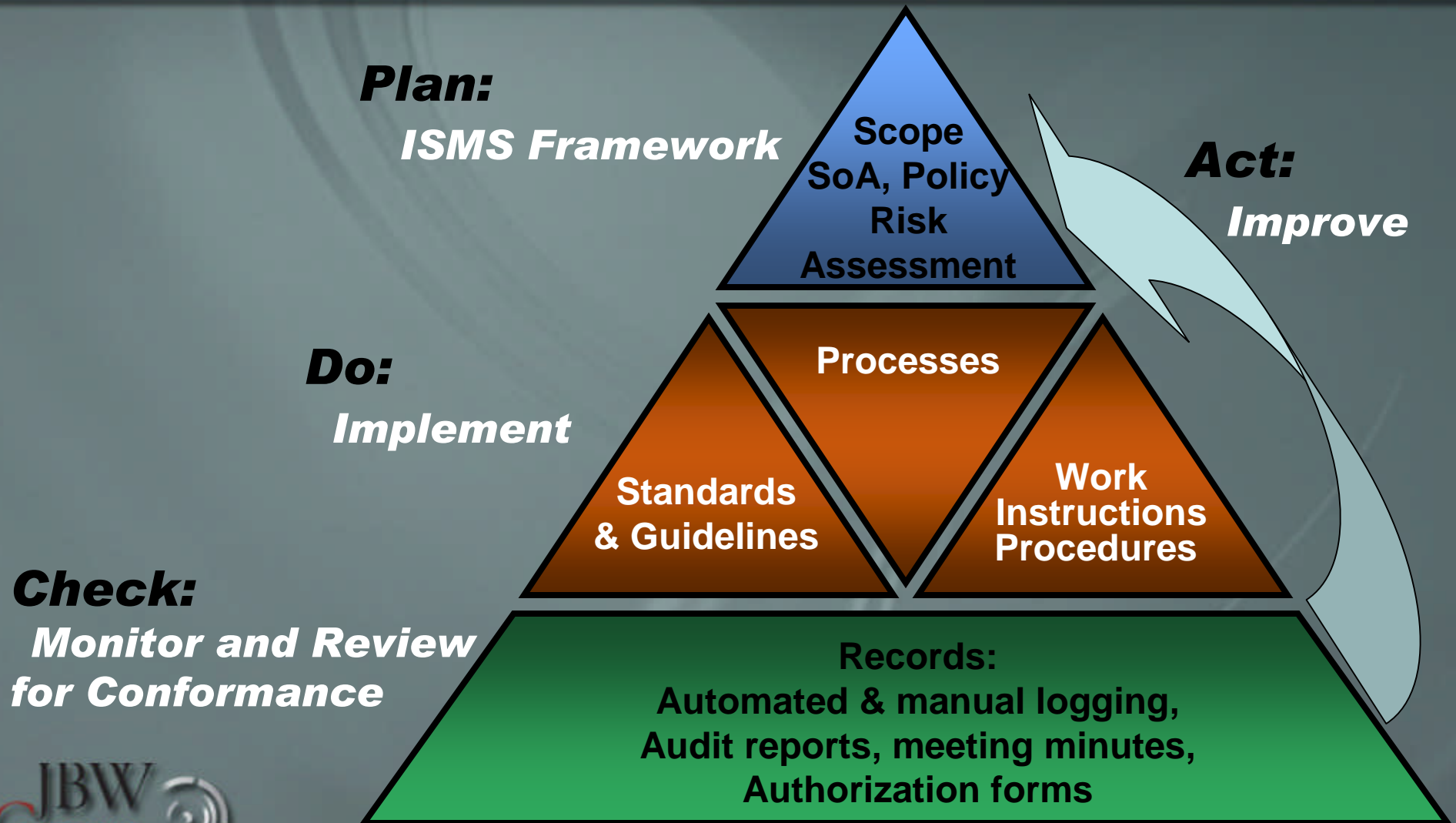
# ISO 27000 Series

- ❑ **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)

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



# 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

# 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, utilization of the audit checklists, passing the assessment
  - Little apparent effort to relate PCI implementation to wider organizational information security needs, objectives, processes

# Integrating Privacy & Security Management

- 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

# Moving Towards Effective Integration

- ❑ Steering committees, working groups, joint projects and work streams, and common control frameworks are a start, but more needs to be identified and documented-
- ❑ What are the shared management elements?
  - In looking at the following list, consider that these items do not suggest duplicative effort, although that may be found along the way)
- ❑ For any of the shared elements, what are the specific or unique contributions from each management domain?

# Common Management Elements

- ❑ Business strategies and objectives supported by security & privacy management
- ❑ Regulations, laws, standards
- ❑ Compliance objectives
- ❑ Corporate governance objectives and stakeholders/stakeholder expectations
- ❑ Risks, risk management strategy, objectives, priorities
- ❑ Methodologies (including key concepts/constructs, tools, etc)
- ❑ Processes and operations
- ❑ Internal business/organizational touchpoints (other processes/process flows, work flows, management structures, stakeholders, clients)
- ❑ External touchpoints (vendors, business partners, regulatory authorities, stakeholders, clients)

# Common Management Elements

- ❑ Reporting and review
- ❑ Shared competencies and subject matter expertise
- ❑ Common conceptions of scope hierarchies for information compliance management within the organization
- ❑ Mutual and asymmetric dependencies
- ❑ Documentation requirements

# What Does Implementation Accomplish?

## A framework for achieving reasonable security that is:

- Scalable
  - 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

Thanks!





Information Assurance

**Patrick F. Sullivan, Ph.D.**

Principal Consultant

[patrick.sullivan@jbwgrop.com](mailto:patrick.sullivan@jbwgrop.com)

+1.317.752.5316

**JBW Group International**

PO Box 19393

Minneapolis, MN 55419 USA

**+1.877.97.27001**

[www.JBWGroup.com](http://www.JBWGroup.com)