



ISO 27005:2008 A Standard-Based Approach to IT Risk Management

Presented to:

Secure 360

Updated October 22, 2008

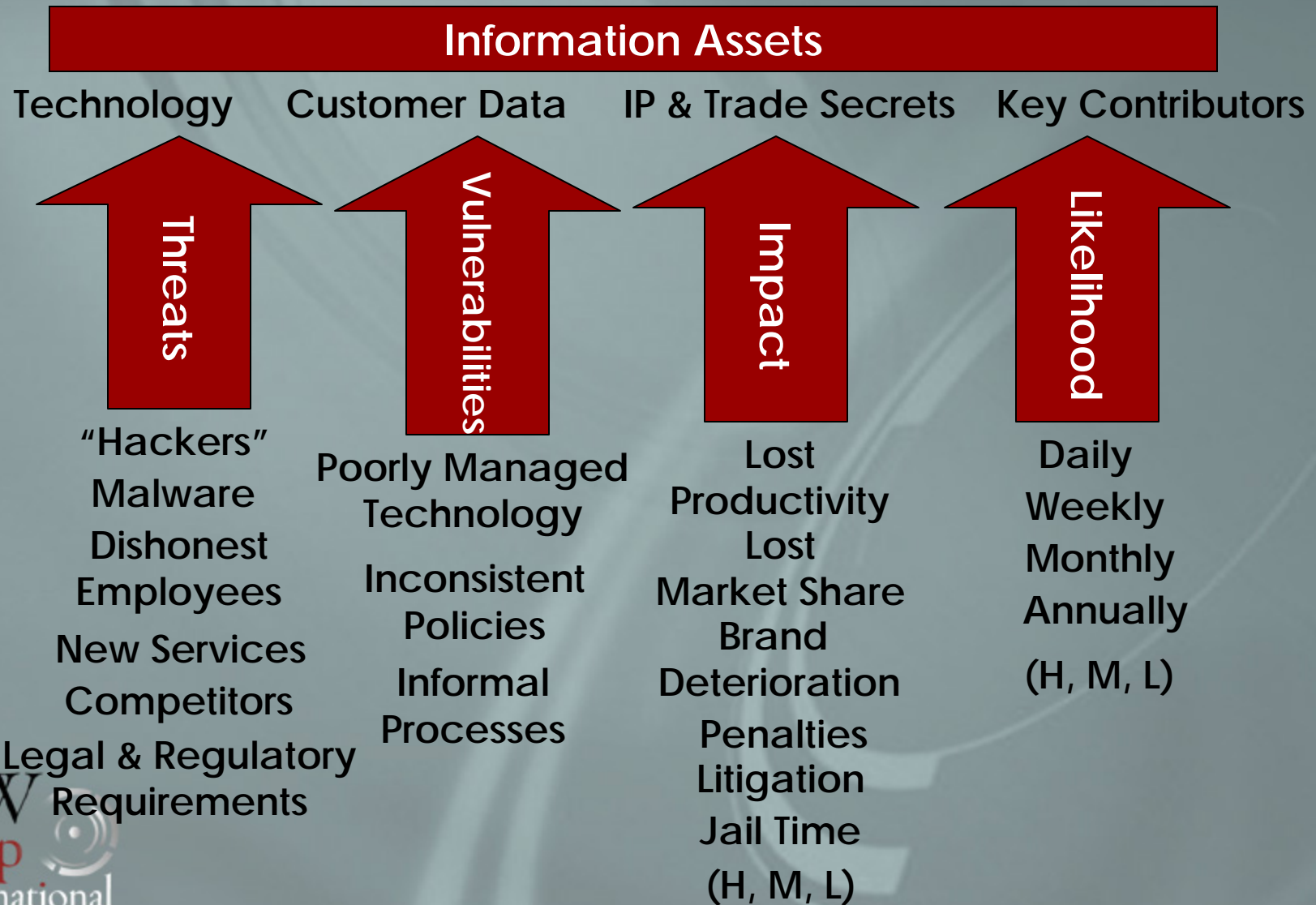
John B. Weaver

CISSP, CISA, CISM, CPP

President/CEO

Principal Consultant

What is Risk?



What is Risk Assessment?



What is Risk Management?

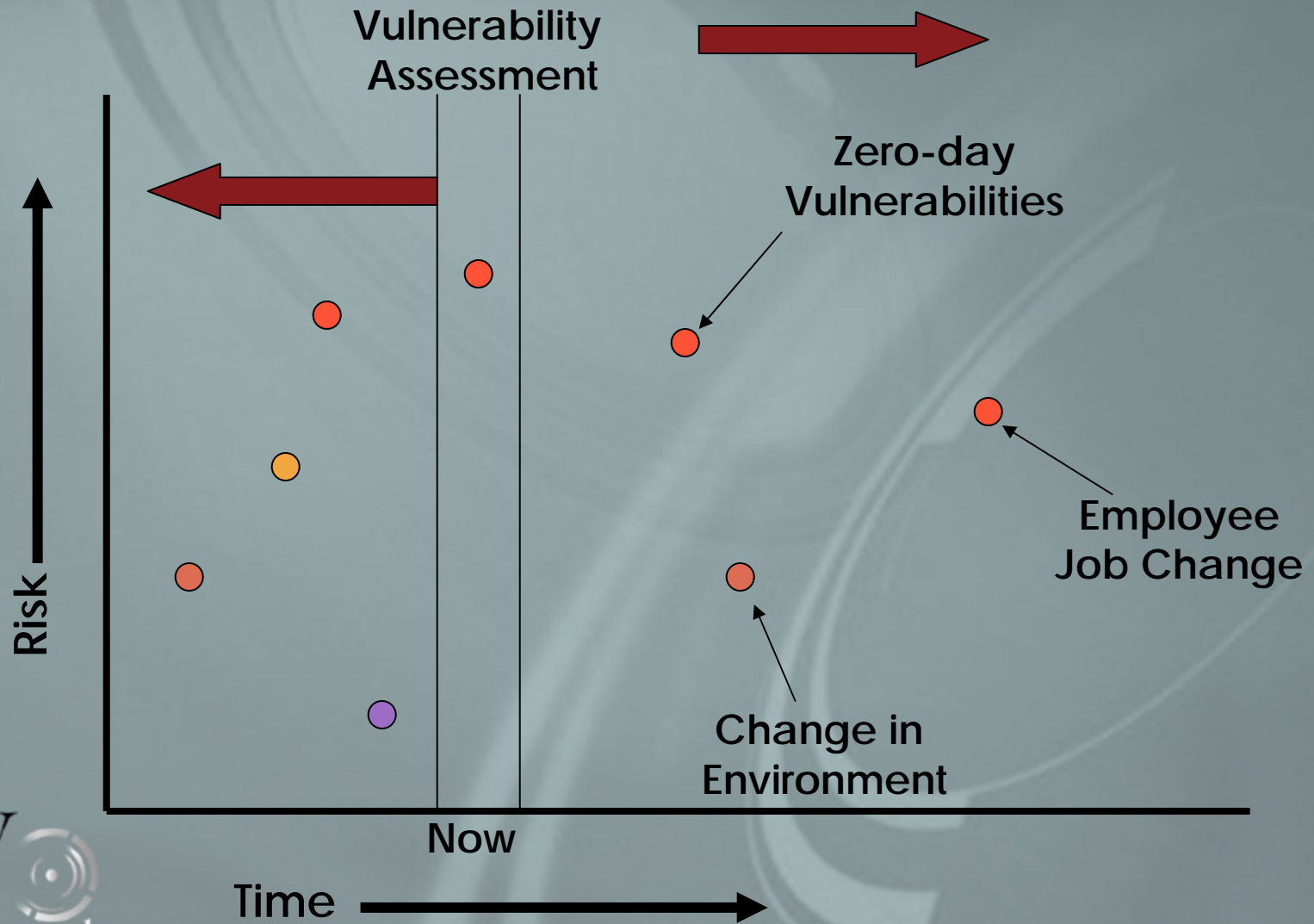
Risk Management is a system for:

- ❑ Identifying information assets
- ❑ Identifying relevant legal and business requirements
- ❑ Determining valuation of assets
- ❑ Determining vulnerabilities associated with the identified assets
- ❑ Anticipating threats that may exploit asset vulnerabilities
- ❑ Assessing the likelihood of occurrence
- ❑ Calculating the level of risk

What is Risk Management?

- ❑ Evaluating the risk and determine an acceptable level of risk
- ❑ Identifying a risk treatment strategy
- ❑ Implementing the risk treatment strategy
- ❑ Assessing the implementation of controls
- ❑ Monitoring and reporting effectiveness
- ❑ Reviewing and re-assessing risks to the organization
- ❑ Improving the ongoing Risk Management activities

Risk Management



Standards-based Approach

- ❑ Process Approach
 - ❑ Foundations in regulatory guidance
 - ❑ Identification of relevant components
 - ❑ Plan development and maintenance
- ❑ Fact-Specific, Risk-Based, Continual Improvement
 - ❑ Process as applied to 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; pre-determined acceptance criteria; monitoring and testing; review and revise, responsibility and authority assigned organizationally, risk assessor competency

ISO 27005:2008

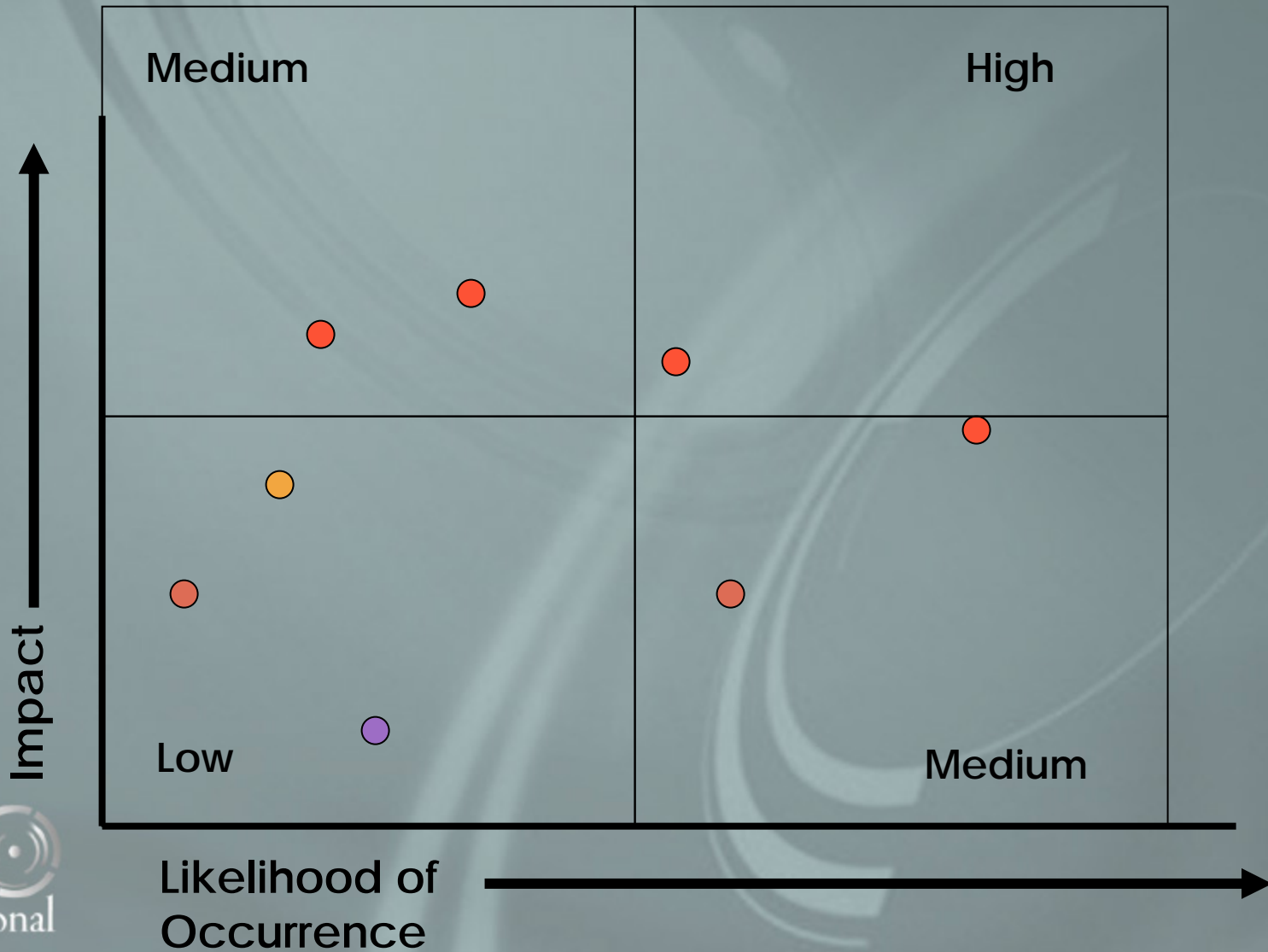
Risk management guidelines designed for use as a companion to ISO 27001:2005 and requires:

- ❑ Business case for Information Security
- ❑ Clearly defined scope of the security program (ISMS)
- ❑ Policy in clear support for information security
- ❑ Risk management methodology
- ❑ Information security risks in the organizational context

ISO 27005 Risk Assessment

- ❑ Risk assessment process
 - ❑ Identification of assets
 - ❑ Identification of legal and business requirements
 - ❑ Valuation of assets
 - ❑ Identification and assessment of threats and vulnerabilities
 - ❑ Assess the likelihood of occurrence
- ❑ Evaluation of risk
 - ❑ Calculation of risk
 - ❑ Assessment against a pre-determined scale

Risk Calculation and Evaluation



ISO 27005 Risk Treatment

Risk treatment occurs through:

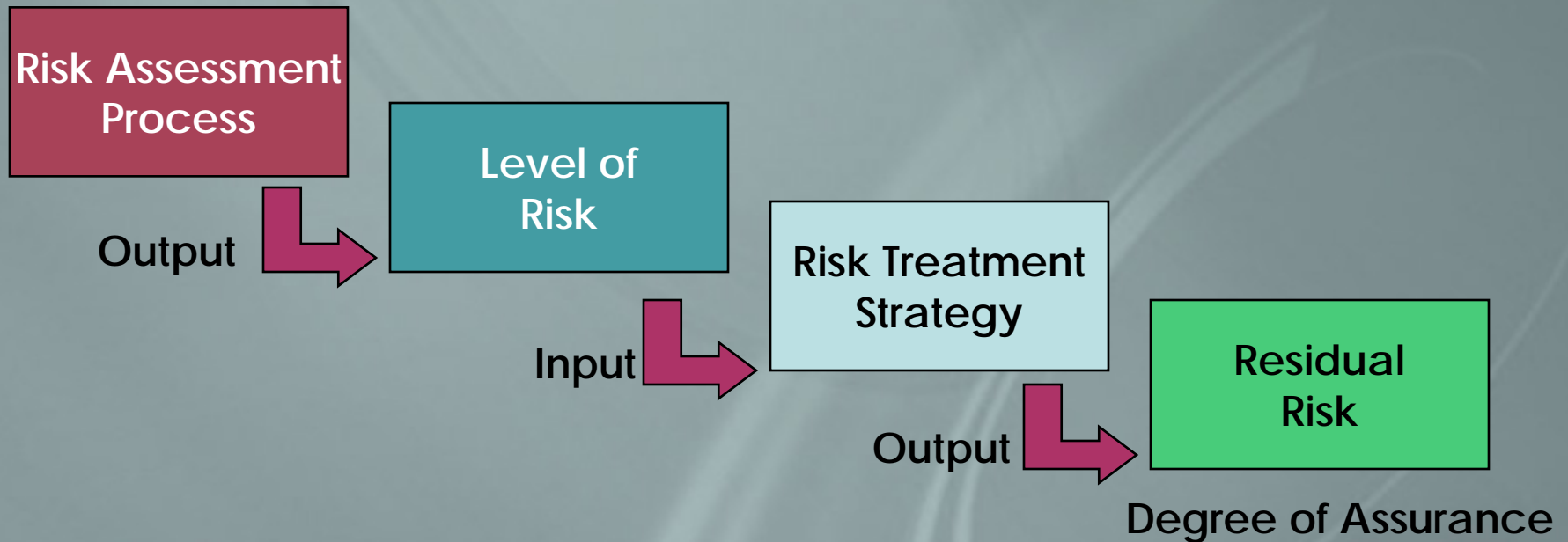
- ❑ Prevention and detection controls
- ❑ Avoidance of risk
- ❑ Acceptance of risk
- ❑ Transfer risk to another entity
- ❑ Some combination

Management decision-making criteria

- ❑ What is the impact?
- ❑ How frequently is it expected to occur?
- ❑ What is the cost to manage the risk?
 - ❑ Green dollars
 - ❑ Resources
- ❑ Current business priorities

Organizational Risk Tolerance

Degree of Assurance determined by:



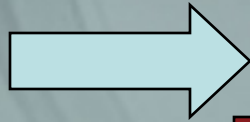
Risk = Vulnerabilities + Threats + Probability + Impact

Ongoing Risk Management

- ❑ Monitoring and maintenance
- ❑ Management review
- ❑ Risk reviews and re-assessment
- ❑ Audits
- ❑ Control of documentation
- ❑ Corrective actions
- ❑ Preventative actions
- ❑ Reporting and communications
- ❑ Risk management role

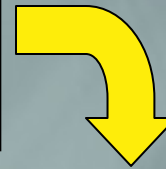
Plan-Do-Check-Act

Risk Tolerance



Plan

Assess and Evaluate Risks



Do

Select & Implement Controls



Monitor & Review Risks

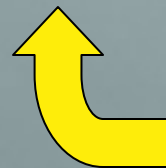
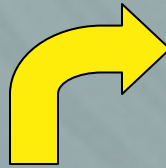
Check



Output
Managed
Risk

Act

Maintain & Improve the Risk Controls

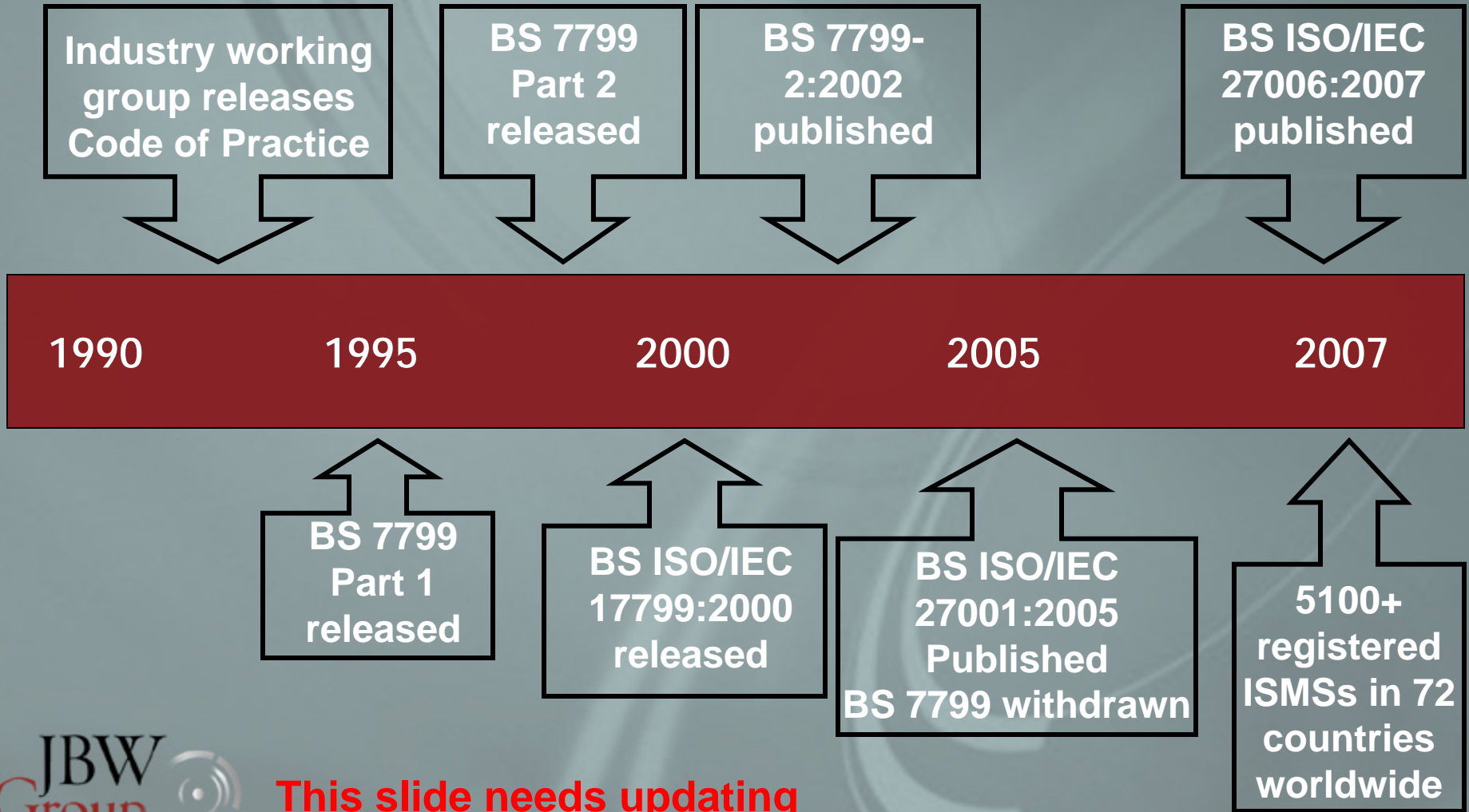


Continuous
Improvement
Cycle

ISO 27005 Annexes

- ❑ Annex A – Defining the scope and boundaries of the information security risk management process
- ❑ Annex B – Identification and valuation of assets and impact assessment
- ❑ Annex C – Examples of typical threats
- ❑ Annex D – Vulnerabilities and methods for vulnerability assessment
- ❑ Annex E – Information security risk assessment approaches
- ❑ Annex F – Constraints for risk reduction

ISO 27001 History



This slide needs updating

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 (formerly BS 7799-3:2006)***
- ❑ ISO 27006:2007 – *International Accreditation Guidelines (10/2007 implementation deadline)*

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
- ❑ Applicable risk management methodology



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