



ISO 27001
Implementation:
A Case Study Panel
Discussion

Northeast Ohio ISSA

A Chapter of the Information Systems Security Association

**September Chapter Meeting
September 9, 2010**

Panel

ANTARES MANAGEMENT SOLUTIONS

Bill Clark, CMQ/OE – ISO Program Manager

Kevin McGuirk, PMP – Security Project Manager

JBW GROUP INTERNATIONAL INC

Patrick F. Sullivan, PhD – Principal Consultant

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



Agenda

- ❑ **Introductions**
- ❑ **Antares Company Overview**
- ❑ **JBW Group Company Overview**
- ❑ **ISO 27001 and Related Standards**
- ❑ **Drivers for Certification (Why 27001?)**
- ❑ **Benefits and Specific Examples**
- ❑ **Consultant Selection Criteria**
- ❑ **Overview of Implementation Approach**
- ❑ **Overview of Implementation Timeline**
- ❑ **Unique Aspects of Antares Implementation**
- ❑ **Observations and Importance of Scope**
- ❑ **Lessons Learned**
- ❑ **Questions**

About Antares

- ❑ **Medical Mutual of Ohio founded 1934 in Cleveland, Ohio**
 - \$2B, 2700 employees, serving over 3 million customers
- ❑ **Antares Management Solutions founded in 1997 as a business division of MMO**
 - Mission: to provide information technology and business processing services through delivery of solution with exceptional value
 - \$272 million, 650 employees, in several location to provide DR/BCP
- ❑ **IT solutions for Healthcare Vertical**
 - Information Technology Services
 - Health Business Processing
 - IT Outsourcing expanding to other segments
- ❑ **Beachwood Data Center Operations**
 - ISO 27001:2005 Certified in October 2009
 - One of 2 Insurance Companies in US with 27001 Certification
 - Over 100 Employees within the scope of ISMS
 - Active governance with MMO and AMS top executives
 - ISO 9001:2008 Re-Certified in February 2010

About JBW Group International Inc.

- ❑ Full Service Information Security Consultancy founded in 2002
- ❑ Specializing in implementation consulting, accredited training and 2nd party audit for
 - ISO 27001 – Information Security Management Systems
 - ISO 28000 – Physical Security Management Systems
 - ISO 20000 – IT Service Management Systems
 - ISO 31000 – Enterprise Risk Management Systems
 - BS 25999 – Business Continuity Management Systems
- ❑ Fortune 1000 clients in United States, Canada, Japan, China, Mexico, Central and South America



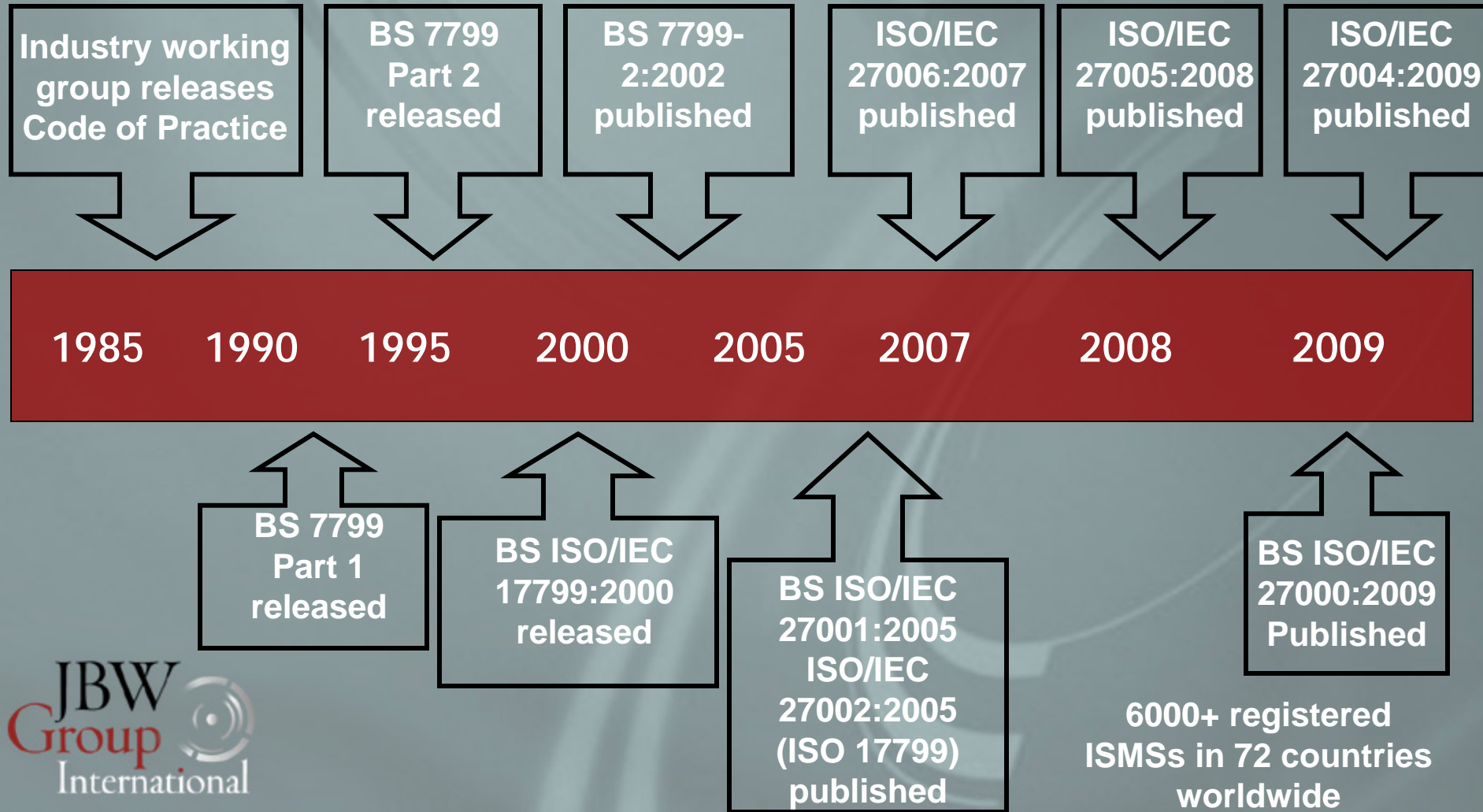
About ISO 27001:2005

- ❑ Risk based, business focused and process oriented
- ❑ Framework for information security that is scalable, repeatable, measurable, sustainable, defensible and continually improving
- ❑ Specifies requirements for management oversight, governance, risk management and controls in areas of:
 - Security Policy
 - Organizational Security
 - Asset Management
 - Human Resources
 - Physical and Environmental
 - Communications & Operations
 - Access Control
 - Acquisition, Development & Maintenance
 - Incident Management
 - Business Continuity
 - Compliance

ISO 27001 Structure

- ❑ **Clauses 1-8 (requirements specification- the auditable standard)**
 - Define the Plan-Do-Check-Act methodology and specify requirements for applying P-D-C-A to information security management
 - Specifications include required processes, organization, management actions, and ISMS documentation
 - Formal risk management methodology
 - Measures of effectiveness of controls
- ❑ **Annex A (ISO 17799 => ISO 27002)**
 - 133 controls organized under 39 control objectives across 11 security categories

ISO 27001 History



ISO/IEC 27001:2005

Specification for Use and Code of Practice

ISO/IEC 27001:2005

Information Security
Management
Requirements Specification
(Auditable Standard)

Adopted by ISO
October, 2005



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

Code of Practice For
Information Security
Management
(Controls Guidance)

Code of practice
released, 2007

ISO 27000 Series

- ❑ ISO 27000:2009 – *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 27003:2010 – *ISMS Implementation Guidance*
- ❑ ISO 27004:2009 – *Guide for Information Security Metrics and Measures*
- ❑ ISO 27005:2008 – *Guide for Risk Management*
- ❑ ISO 27006:2007 – *International Accreditation Guidelines*

ISO 27000 Series

- ❑ ISO 27007 – *Guidance for information security management systems auditing (proposed)*
- ❑ ISO 27011:2008 – *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2005*
- ❑ ISO 27799:2008 – *Health Informatics - Information security management in health using ISO/IEC 27002:2005*
- ❑ *ISO/IEC 27XXX – Future publications for Financial, Energy, other verticals*

Drivers for Certification

- ❑ Customer Driven
 - Competitive advantage
 - Market differentiation
- ❑ Greater Visibility into Information Security program
 - Demonstrate Information Security competence
 - Transfer institutional knowledge
 - Developed engineering from alchemy
 - Develop metrics and measures
- ❑ Legal and regulatory compliance
 - HIPAA/HITECH
 - GLBA Security Rule
 - Ohio Department of Insurance Model Audit Rule

Benefits

- ❑ Executive Awareness
 - Better informed risk-based decisions
 - Support internal audit program
 - Facilitate/support training
- ❑ Cohesive, consistent audit results
 - Always audit ready
 - Minimize resource impact for 60+ annual audits
- ❑ Collaboration with all areas of the organization
 - Developed working collaboration with corporate audit
 - Department contributes to the ISMS internal audit teams

Benefits – Specific Examples

❑ IT Governance

- Information Security Advisory Committee
 - Security
 - Human Resources
 - Corporate Controller
 - President, Antares Management Solutions
 - Chief Managed Care Officer
 - Medical Mutual Statewide Operations
 - Medical Mutual Financial Administration
 - General Counsel & Chief Privacy Officer
- Documented Security – Legal Staff Interaction Cycle (Compliance, Risk, Contracts)

❑ Defensible IT Risk Management System

- Built on COSO, NIST 800-39, ISO 27005
- Reviewed by: IBM, Ohio Department of Insurance, US Office of Personnel Management (FEHBP)

❑ Institutionalizing Information Security Best Practices

- Documenting the Mature Security Program
- Instituting Knowledge Transfer through the ISMS Internal Auditor Program

Consultant Selection Criteria

❑ Expertise

- Knowledgeable on subject matter
- Knowledge of Legal and Regulatory impacts facing our industry
- Competent and capable staff

❑ Ability to Execute

- Consulting globally on ISMS Implementation
- Successfully guided clients through implementation and certification
- Track Record of transferring knowledge

❑ Reputation

- Integrity
- Commitment to Client Success
- Recognized Information Security Leader and ISO 27001 Advocate

Implementation Overview

- ❑ Readiness assessment
 - Identified mature areas and gaps
 - Developed an implementation roadmap
- ❑ Staffing the implementation team
 - Core team as part of the planning process
 - Identified champions
 - Identified challengers
- ❑ Training
 - Knowledge of the standard
 - Implementation training
 - Staff training
 - Technology training
 - Executive training
- ❑ Project Management
 - Day-to-day tactical oversight
 - Strategic program management

Implementation Timeline

1. Draft Business Case
2. Gain Management Authorization
3. Form Team
4. Evaluate and Select Consultant
5. Consultant – Team Gap Analysis
6. Train Staff on Implementation and 27001 Lead Auditor
7. Draft Scope
8. Develop Project Plan from Gap Findings
9. ID and Classify Assets
10. Complete Risk Assessment and Treatment Processes
 - Management Acceptance or Residual Risk
 - Management Authorizes Risk Treatment

Implementation Timeline

12. Select Applicable Controls
13. Statement of Applicability Drafted
14. Management Authorizes Implementation and operation of ISMS
15. Complete ISMS Internal Audit
16. Request Registrar Pre-Cert Audit
17. Corrective Actions
18. Stage 1
19. Corrective Actions
20. Stage 2
- 21. Certification**

Unique Aspects of Antares Implementation

- ❑ ISO 9001 led to ISO 27001
 - Quality benefits extrapolated to information security
 - Leveraged quality culture
- ❑ Ramp up of individual knowledge transfer
 - (Re)Learning curve for veterans
 - Learning curve for new employees
- ❑ Organizational change over time
- ❑ Rapid adoption by Legal and General Audit
 - Quickly recognized value

Observations

- ❑ ISMS implementation benefited from the AMS Quality culture
 - Multi-year operating Quality Management System
 - Process oriented
 - Understanding of the registration/certification process
 - Understanding of the value of metrics and measures
- ❑ Mature Information Security Program
 - High-performance Security Team
 - Exceptional security awareness training program
- ❑ Established and Productive Linkage with Legal
 - Regular weekly meetings between the Security Manager and General Counsel
 - One attorney dedicated to Compliance

The Importance of Scope

- ❑ Meaningful scope key to certification
 - Meaningful Scope = Meaningful Certification
 - Key to Manageable Implementation
 - Avoids Potential for “Deceitful” Scope
- ❑ Relevant scope important to customers
 - ISMS is Appropriate to Business-Critical Assets
 - Management of Security Risk Relevant to Services
 - Addresses Customer Requirements and Due Diligence
- ❑ Relevant scope important internally
 - Major Success Factor
 - Scope Size and Complexity
 - Time to Implement
 - Maturity of Information Security Program
 - Enterprise Risk Management
 - Management Support and Commitment

AMS input: The Importance of Scope

- ❑ **Meaningful scope key to certification**
 - Investing time, money and effort...Get what your paying for.
 - Dividends in Risk Mitigation
 - Audits
 - Strategic Planning
 - Enterprise Architecture
- ❑ **Relevant scope important to customers**
 - 27001 Certification means something on first review.
 - Seal of approval on key Security, Risk and Continuity Processes
 - Your customers' data is in GOOD HANDS
- ❑ **Relevant scope important internally**
 - Facilitates training
 - Consistent application of Security Program
 - Management Decisions based on Metrics not Magic

Lessons Learned

- ❑ **Begin with Governance in Mind**
- ❑ **Train before you begin implementation**
 - Learn the standard and what auditors look for (ISO 27001 Lead Auditor)
- ❑ **Benefits of iterative audits**
 - Multiple cycles honed the ISMS
 - Developed auditor pool with expertise
 - Created security awareness throughout the organization
- ❑ **Understand Scope**
 - Needs to be well defined early
- ❑ **Communications versus Training**

Questions?

Contact Information



An ISO 27001/ISO 9000 Certified Company

www.antaressolutions.com

Bill Clark

ISO Program Manager, ASQ Certified Manager of Quality / Organizational Excellence, IRCA-certified ISO 27001 & ISO 9001 Auditor

Bill.Clark@AntaresSolutions.com

216.292.1682

Kevin McGuirk

Security Project Manager, PMP

Kevin.McGuirk@AntaresSolutions.com

216.595.4759





John B. Weaver

CISSP, CISA, CISM, CPP

President/CEO

Principal Consultant

JBW Group International

PO Box 19373

Minneapolis, MN 55419 USA

+1.877.97.27001

www.JBWGroup.com