

# **ISO 27001 Implementation A Case Study Panel Discussion**

1

## **ANTARES MANAGEMENT SOLUTIONS**

**Bill Clark, CMQ/OE – ISO Program Manager**

**Kevin McGuirk, PMP – Security Project Manager**

## **JBW GROUP INTERNATIONAL INC**

**Cynthia Kriha, Director – Strategic Programs**

**Patrick F. Sullivan, PhD – Principal Consultant**

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

# Agenda

2

- Introductions
- Antares company overview
- JBW Group company overview
- Brief overview of ISO 27001
- Drivers for certification (Why 27001?)
- Selection process / criteria for selecting a consultant to assist the ISMS implementation
- Overview of implementation approach and timeline
- Lessons Learned
- Challenges and Surprises
- Observations and Benefits
- Questions?

# About Antares

3

- 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

- Full Service Information Security Consultancy founded in 2002
- Specializing in implementation consulting, accredited training and 2<sup>nd</sup> 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

5

- 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

# Drivers for Certification

6

- 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

# Consultant Selection Criteria

7

- 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

- 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

# Challenges and Surprises

9

- ISO 9001 lead to ISO 27001
  - Quality benefits extrapolated to information security
  - Leverage 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

- 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

# Lessons Learned

11

- 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

- **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

Questions?

**Bill Clark – ISO Program Manager**  
**ASQ Certified Manager of Quality / Organizational Excellence,**  
**IRCA-certified ISO 27001 & ISO 9001 Auditor**  
**Antares Management Solutions**  
**Bill.Clark@AntaresSolutions.com**  
216.292.1682

**Kevin McGuirk– Security Project Manager**  
**PMP**  
**Antares Management Solutions**  
**Kevin.McGuirk@AntaresSolutions.com**  
216.595.4759  
www.antaressolutions.com

**John B. Weaver, CISSP, CISA, CISM, CPP**  
**President, Principal Consultant**  
**JBW Group International Inc**  
**jbw@jbwgroup.com**  
877.97.27001  
www.jbwgroup.com