



Research Sites Restoration Ltd

ISO 27001 Information Security Challenges in Implementing Standard

Richard Hibbert

RSRL Head of Quality and Management systems

16/10/2012

About RSRL

- Research Sites Restoration Limited (RSRL) is the site licence company responsible for the closure programme at Harwell and Winfrith.
- RSRL operates under contract to the Nuclear Decommissioning Authority (NDA).
- RSRL employs around 430 people.

Presentation Content

- Importance of Information Security
- Quick look at ISO 27001
- RSRL approach to implementing ISO 27001
- Challenges faced and lessons learned

Importance of Information Security

- Key Areas
 - Nuclear security
 - Legal compliance (e.g. Data Protection Act)
 - Commercial security
 - Protection of reputation
 - Process effectiveness and efficiency
 - Business Continuity

Information and Efficiency

- “On average, up to 10% of staff time is spent looking for records and information”
- (Elizabeth Parker, “Managing Your Organization’s Records”)

ISO 27001

BRITISH STANDARD

BS ISO/IEC
27001:2005
BS 7799-2:2005

**Information
technology — Security
techniques —**

**Information security
management
systems —**

Requirements

ISO 27001 Overview

- The standard provides a model for an Information Security Management System (ISMS)
 - Can be used as audit standard both internally and externally
 - Aligned with ISO 9001 and ISO 14001
- Information Security includes confidentiality, integrity and availability of information
 - Information can in any form (physical or electronic)
- The standard is primarily about identifying and managing information security risks
 - Information is viewed and treated as a valuable asset

Summary of Requirements of ISO 27001 (1)

- Management Commitment
 - Policy and objectives
 - Scope statement
 - Resources
- Identification of legal, regulatory and contractual requirements
- Roles and Responsibilities
- Risk Management
 - Risk assessment to defined method
 - Risk treatment plan including control objectives and controls
 - Management approval of residual risks
 - Statement of Applicability (Summary of decisions concerning risk treatment)

Summary of Requirements of ISO 27001 (2)

- ISMS procedures
 - Including document and records management
- Training, awareness and competence
- Monitoring
- Audits
- Management Review
- Continual Improvement
 - Corrective action
 - Preventive Action

Annex A – Control objectives and controls

- Section 4.2.1 of ISO 27001 requires selection of control objectives and controls from Annex A although others may also be required.
 - Requires specialist technical understanding to be able to interpret some sections

RSRL Key Driver for ISMS Development

- Meet Customer (NDA) Requirements
 - NDA has very onerous information security obligations
 - NDA is required to carry out annual self-assessment using CESG Information Assurance Maturity Model (IAMM) and demonstrate improvement

RSRL Approach to ISMS Development

- Run as a small project over two years
 - Relaxed timescale to avoid conflicts with other system developments and work priorities
- Support Services Director acted as Sponsor
 - Has role of Information Governance Officer and acts as the Senior Information Risk Owner
- Development of System led by IT Manager and Head of Quality
 - Consultancy support to help with project management, system development, training delivery and carrying out risk assessments
- Appointed Information Asset Owners for key assets
- Self-assessment not third party certification

Key Development Steps

- Intensive ISO 27001 familiarisation training for IT Manager and Head of Quality
- Initial gap analysis carried out by IT Manager and Head of Quality
 - Key task list developed
- Paper presented to Executive to gain approval
- Task list developed into project plan
- Legal, regulatory and contractual obligations identified
- Risk assessment methodology developed and risk assessments carried out
- ISMS documentation developed within framework of integrated management system
- Training identified and delivered

Impact on RSRL Processes



Research Sites
Restoration Ltd

Management
System
Manual

PROCESSES

Asset Care & Maintenance	Asset Management	Business Improvement	Commissioning	Dangerous Goods (inc. RAM) Transport	Decommissioning
Design	Document Control	Emergency Planning	Environmental Management	Governance	Independent Assessment
Knowledge Management	Maintain Management System	Manage People	Non-Conformance Management	Nuclear Material Management	Organisational Change Control
Plant Management	Procurement	Programme Management	Project Management	Property Management	Radiological Protection
Safety Case Management	Safety Management (Operational)	Security	Self-Monitoring	SHE Risk Assessing	Stakeholder Engagement
Strategic Direction	Support Service Delivery	Tenant Control	Waste Management	Work Control	Workforce & Skills Management



New ISMS Documentation

- POL 0001 - Security and Information Security Policy
- MAN 0035 - Information Security Manual
- PRC 0169 - Identifying Information Security Obligations
- PRC 0157 - Information Security Risk Assessment
- RUL 0002 - Information Technology Security Rules
- STD 0108 - Control of Removable Media
- PRC 0209 - Contract Security and Security Aspect Letters

Current Status

- Information security obligations identified
- Information risk assessments carried out for most important set of information assets
- Risk treatment plan and statement of applicability produced
- Key controls defined in management system
 - Security requirements clarified
 - Records management requirements and practices strengthened
 - Some new documentation produced
- Awareness training delivered

Benefits

- Increased awareness of Information Security Obligations
 - For example, a review of requirements of records agreement with NDA has required improvements to records management practices
- Increased awareness of Information Security risks and controls
- Highlighted where existing security requirements were not well presented or understood
 - Now properly formalised in management system
- Improved monitoring of network now allows rapid detection of any use of unauthorised USB devices
 - Highlighted need for more awareness training

Future Developments

- Extend scope of risk assessments to ensure comprehensive coverage of information assets
- Deliver further awareness training
- Fully establish monitoring and reporting arrangements
- Carry out independent assessments to confirm effective implementation of system
- Carry out self-assessment using IAMM
- Report status to 2013 Annual Management Review

Summary - Challenges in Implementing ISO27001

- Securing Sponsorship
 - Risk ownership and acceptance is vital
- Getting the right people involved
 - IT, Management Systems, Security, etc.
- Raising awareness of information security issues
- Avoiding conflicts with what already exists
 - RSRL already had many security controls in place
 - System integration opportunities were identified early
- Keeping the momentum going
 - Use of part-time resource can cause loss of focus

Questions ?