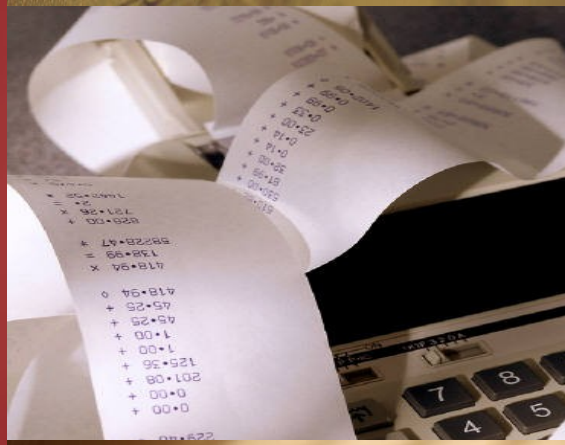
The Pursuit of ISO/IEC 27001:2005 Certification

Joan Ross, CISSP, NSA IEM

Moss Adams LLP

When you think of compliance, what comes to mind?



The Compliance Paradigm Game…

. . .test your knowledge for fun and amusement

Name this Compliance Standard

A.

Application of the "security rule" to protect patient data and electronic transaction interchanges

Name this compliance standard

A.

Evaluation and testing of “design effectiveness” and “operating effectiveness” for accurate reporting of corporate financial information

Name this compliance standard

A.

Provides protections against the selling of your private financial data and the obtainment of your personal information through false pretenses

Name this compliance standard

A.

Data security standards for credit card processing environments, including data storage and encrypted transmissions

Name this Compliance Standard

A.

Independent review of internal controls – could be a Type I or Type II statement on auditing standards

Name this compliance standard

A.3

Issues standards for an environmental management system

Name this compliance standard

A.3

Defines the quality assurance requirements and quality system assessment for companies that design, produce and install service products

Name this compliance standard

A.

Provides the certification model for evaluating, operating and improving an information security management system

What is ISO/IEC?

1. The International Standards Organization and the International Electrotechnical Commission form worldwide standardizations through technical committees and global collaborations

2. Their intent is to align international standards to support consistent and integrated implementations

3. Technology + Management

How did ISO/IEC27001 evolve?

- Iterations date back to the 1980's in U.K.
- U.K. Department of Trade & Industry: A Code of Practice for Information Security Management
- 1995 – BS7799
- 2000 – ISO/IEC17799
- 2005 – ISO/IEC 27001

ISO/IEC 17799 Audit Areas

2. Information Security Policy
3. Organization of Information Security
4. Asset Management
5. Personnel/Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Information Systems Acquisition, Development and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

Scope

- 17799 can provide implementation guidance that can be leveraged when designing 27001 controls
- 27001 uses the word “shall” as opposed to “should”
- “Business” means activities core to the organization’s existence

Approach

- Robust model for the governance and implementation of principles specific to risk assessment, security design & implementation, security management and re-assessment.

The 27001 PDCA Model

- PLAN
- DO
- CHECK
- ACT

Inputs and Outputs

- Interested parties coming in to your ISMS
- Information security requirements and expectations
- Risk assessment and conclusions
- Interested parties receiving data communications
- Managed information security

PLAN

Establish the ISMS

- Policy
- Objectives
- Processes
- Owners
- Procedures
- Key controls
- Risk management
- Delivery of results
- Continuous monitoring
- Auditing of effectiveness
- Information security improvements

Discussion regarding PLAN

DO

Implement and Operate the ISMS

- Demonstrate how the organization effectively implements and continually operates specific to established policy, identified controls, practical processes and defined procedures

Discussion regarding DO

CHECK

Monitor & review the ISMS

- Perform assessments
- Evaluate process
- Measure performance
- Review objectives
- Assess expertise
- Test controls
- Reporting to management

Discussion regarding CHECK

ACT

Maintain & Improve the ISMS

- Internal audits
- Preventative decisions
- Corrective actions
- Review by management
- Improvements

Discussion regarding ACT

Statement of Applicability

- Derived from an organization's risk assessment
- Contains the specific controls, control objectives and reasoning for controls
- Details the precise implementation of the controls for fulfilling objectives
- Justifies the exclusion of other controls and control objectives

Obtain the International Standard Specification

- www.iso.org – search 27001
- www.anab.org – ANSI National Accreditation Board for U.S. companies accredited to certify
- www.ukas.com – U.K. Accreditation Service

Scenarios

- The pursuit of ISO/IEC 27001 certification will be important for global businesses
- Other organizations will view certification as a valuable benchmark
- Companies may apply the framework but not obtain certification

Questions?

Joan Ross
206.605.3100 phone

Joan.ross@mossadams.com