Agenda

• ISO 27001 Overview
• ISO 27002 Overview
• Certification Process
ISO 27001 - Overview

- International Standards Organization
- Information Security Management System (“ISMS”)
- Based on British Standard 7799
- Management system – Process
- Conform not comply – Voluntary
- Framework for established scope
ISO 27001 - Overview

- “Plan-Do-Check-Act” (“PDCA”)
- Plan - Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.
- Do - Implement and exploit the ISMS policy, controls, processes and procedures.
ISO 27001 - Overview

• Check - Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.

• Act - Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system.
ISO 27001 - Overview

• Why implement
  – Benchmark information security
  – International operations
  – Competitive advantage
  – Contractual obligations
ISO 27001 - Clauses

• Based on Clauses 4 - 8
• 4 Information security management system
  – Establish the plan
  – Implement the plan
  – Monitor the plan
  – Improve the plan
ISO 27001 - Clauses

• 5 Management responsibility
  – Management commitment
  – Training and awareness
• 6 Internal ISMS audits
• 7 Management review
• 8 Continual improvement
ISO 27001 – Key Concepts

- Asset Registry
- Risk assessment – ISO 27005
- Statement of Applicability
- Major Non-Conformities
- Minor Non-Conformities
- Corrective Action Plan
ISO 27002 - Overview

- Appendix of ISO 27001
- ~133 controls
- Basis for Statement of Applicability
- Selected by the organization based on risk
- Not a certification
ISO 27002 - Clauses

• Based on Clauses 5 - 15
  – 5 Security policy
  – 6 Organization of information security
  – 7 Asset management
  – 8 Human resources
  – 9 Physical and environmental security
  – 10 Communication and operations management
ISO 27002 - Clauses

• Based on Clauses 5 - 15
  – 11 Access controls
  – 12 Information systems acquisition, development, and maintenance
  – 13 Information security incident management
  – 14 Business continuity management
  – 15 Compliance
Certification Process

- Performed by a Certification Body
- ANSI National Accreditation Board ("ANAB")
- 3 year certification
  - Year 1 – full scope audit
  - Years 2 & 3 – surveillance audit
- Certification letter & seal
Certification Process

- **Year 1**
  - Stage 1 – Policy and procedure review
  - Stage 2 – Detailed tests
  - Address major non-conformities
  - Issue report

- **Years 2 and 3**
  - High level policy review
  - 33% of Statement of Applicability
Questions

Gene.Geiger@alignsecurity.com
Neil.Gonsalves@aligncpa.com