The Road to ISO 27001 Certification
Are there any shortcuts?

Sallie Newton, CISSP, PCI-P, GISP, ITIL v3, GISF, former CCSFP & QSA

About Me - Personal

- One daughter, two dogs, love to travel, and mentor women in tech.

About Me – Professional (33 years)

- 1986 on Wall Street working for Bear Stearns, one of the largest brokerage firms on Wall Street. Quickly learned the rules and regulations of the New York Stock Exchange (NYSE)
- After 10 years on Wall Street, I went back to school (Parsons School of Design), where I learned graphic design and how to build websites as ecommerce was exploding.
- NY MTA Property Protection Agent – NY State Licensed Security Guard
- Worked for Macys-by-mail which became Macys.com
- NC Bioterrorism Unit Business Continuity and Disaster Recovery
- NC Department of Revenue – Auditing tax returns
- NC State University – IT Security and Compliance
- Consulting – Serve as vCISO for some of the largest global leading brands
- Currently serve as Application Security Professional

So, what is ISO?

ISO Internal Organization of Standardization

- www.iso.org
- Protect IT and non-IT assets and data
- Published jointly by the ISO and IEC
- Originally published 1995 BS 7799
- Written by UK government
- 2005 incorporated into ISO 27000 series
- 2013 is the most current version
- Does not formally mandate specific controls

Management

- Makes the decision to achieve ISO 27001 Certification
- Commitment and unwavering support is critical
- Sets the expectation for everyone in the organization

Certifying Body

- http://anabdirectory.remoteauditor.com/

- ABS Quality Evaluations, Inc.
- A-LIGN Compliance and Security, Inc. dba A-LIGN
- Aprio, LLP
- BSI Assurance UK Limited
- Coalfire ISO Inc.
- DEKRA Certification, Inc.
- DQS Inc.
-

What is ISO 27001?

International standard for the governance of information assets, creating an effective and sustainable Information Security Management System (ISMS).

ISMS?

ISMS Board

- Use the organizations mission, objectives and activities to prioritize risk management decisions.
  Identify all personnel, systems and infrastructure dependencies for all critical organizational functions
- Use critical functions and their dependencies to inform risk management decisions including BCP/DRP
  Define resilience requirement/maximum tolerable downtime to support delivery of critical services
- Governance
  Risk Assessment
  Risk Management

ISMS: Scope

- The organization shall determine the boundaries and applicability of the information security management system.

ISO Stage 1 Audit

- Remote telephone audit to determine organizations ISO cert readiness requires the following documents:

  - Scope
  - Statement of Applicability
  - Proof of ISMS Board including Meeting Minutes
  - Security Policies
  - Risk Assessment
  - Audit

ISMS: Policies

Policies include:

- HR Policies
  - Background checks
  - Onboarding and Termination
- Network Security
- Mobile Device Policy
- Asset Management Policy
- Data Classification
- Business Continuity
- Disaster Recover
- Incident Response
- Physical Security
- Backup
- Logging and Monitoring
- System acquisition, development and maintenance
- Third-party management
- Note, list not exhaustive

Information Security Policies

- The foundation of an Information Security Program. These are the laws of the land that dictate, control and manage what people should and should not be doing. .
- ➔ **Concise**
  Short 5 or less pages focused on risk mitigation
- ➔ **Readability**
  Written in layman's terms for all to understand
- ➔ **Enforceable**
  Enforced on a regular basis

Policy

To protect people, critical data, critical processes and organization

- Focused on the unique requirements and culture of the organization
- Updated on a regular basis
- Published for all to access
- Communicated at regular intervals
- Separate from procedures, standards and baselines
- Strict versioning control with effective and expiration dates Ex. 3.1.5, 3.1.6

Policy

- **Focused on People**
- Policy - high level strategic document
- “You must change your password every 90 days.”
- Procedure - details the specific steps to be followed to accomplish a specific task.

- **Focused on Technology**
- Standard - high level document focused on uniform use of a specific technology
- Baseline - details the specific implementation of a standard

Guidelines - optional tips and tricks to help user follow policies, procedures, standards and baselines.


SPEED
LIMIT
45
PEED
IMIT
45

Important Triad

- Policy - tells users what to do
- Training - gives users the skills to do it
- Awareness - changes users behavior
- Example: Users must lock their computers prior to walking away from their computer.
- Why: To Protect Yourself
- Background Statement: If you walk away from your desk without locking your computer, you are liable for actions taken under your credentials. (Increase compliance)

ISMS: Training and Awareness

Effective Training & Awareness Program

- Policy focused
  - Focus on the policy statements that have the lowest compliance

  - Frequent intervals
  - Monthly security messages in a variety of delivery
    - In-person training
    - Emails
    - Newsletters
    - Cybersecurity Month Activities (Oct.)

    - Relevant to the users –
      - End-user – strong passwords
      - Developers – OWASP training

Document, document, document!

Because if it is not documented, it didn't happen. Tales from a former auditor.

- Document your training and awareness program including content, attendees, and delivery dates

ISO Stage 2 Audit

- Onsite audit
- In-depth interviews with key stakeholders, HR, end-users
- Submit remaining policies, process, standards and procedures

Decisions, decisions?

- Certifying body will review final documentation and make a decision to move grant the organization the ISO 27001 certification

Or

- Request more documentation – although, not ideal, this does not mean the organization has failed, the road to certification may just be a longer trip.

Certification Achieved, now what?

- ISO 27001 Certification comes with the responsibility to continuously improvement your security posture to maintain your certification status.

- Annual Audits

- Recertification


Questions?