

# Implementing an ISMS: Stories from the Trenches

Peter H. Gregory, CISA, CISSP, DRCE



# About the speaker

- Peter H. Gregory, CISA, CISSP, DRCE
  - Security and risk manager
  - Author of 19 books on security / tech



# About the speaker

- Security and Risk Manager
- \$300MM Public company providing financial services
- ISO27001, ISO 20000 certified. SAS70 Type II, PCI, SOX audits.



- InfraGard – Evergreen State Chapter
- Critical Infrastructure Protection
- Training. Networking. Intelligence.
- Join today.
- [www.infragard.net](http://www.infragard.net)

# Why we run an ISMS

- Foundation of a Trust Platform
- Establish and improve credibility in our top-down security program
- Resist customer audits

# Agenda

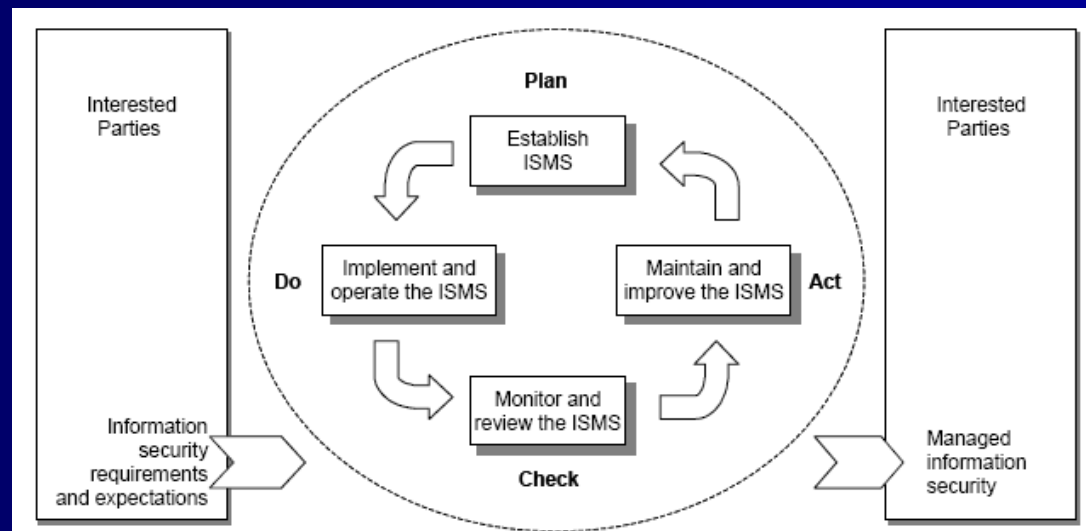
- What is an ISMS
- Background on ISMS & ISO 27001
- How to get audited / certified
- Discussion / questions

# What's an ISMS

- Information Security Management System
  - *Top-down* security management
  - *Organized* security management
  - Policy and risk based
  - Defined in ISO27001:2005

# What is ISO27001

- International standard on information security management
- Management driven, risk-based, life cycle security management



# Brief history of ISO 27001

- BS7799 Part 2 in 1999
- Became ISO27001 in 2005
- Full name: ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements
- Intended to be paired with ISO 27002 (former ISO 17799, formerly BS7799 Part 1)

# 27001 and 27002

- 27001 is the body of ISMS management requirements
- 27002 is the body of controls (the "code of practice")
- You can use them together, or not

# Adoption of ISO27001

- Advantage: established and respected world-wide standard; traction in Europe and Asia
- Disadvantage: document cost; because it is not free, many have not seen it
- Gaining traction in the U.S.

# Why ISO 27001

- International standard
- International recognition
- Vetted
- If you follow it faithfully, you'll get your security right

# Framework / Structure

- Required activities / processes
- Required documents
- Required records
  
- Do all that and you can be certified

# Required processes

- Risk Assessment
- Risk Treatment Plan
- Incident Management
- Monitoring and Review
- Corrective Action
- Preventive Action

# Required documents

- ISMS Scope Description
- ISMS Policy (High-Level)
- Asset Inventory
- Operational Procedures and Controls
- Internal Audit Plan, Procedure, and Schedule

# Required records

- Evidence of Management Risk Decisions
- Evidence of Legal and Regulatory Review
- Evidence of Management Review

# How to be *audited*

- Pick any security consulting firm with competent auditors who are familiar with 27001 / 27002
  - Give preference to certified ISMS auditors

# How to get *registered*

- Be audited by a registrar
  - BSI Americas ([bsiamericas.com](http://bsiamericas.com))
  - Bureau Veritas Certification Holding SAS ([www.bureauveritas.com](http://www.bureauveritas.com) )
  - KPMG ([kpmg.com](http://kpmg.com))
  - Perry Johnson Registrars ([pjr.com](http://pjr.com))
- How to find a registrar
  - [ukas.com](http://ukas.com)

# Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

Redmond  
Washington  
98052  
USA

Holds Certificate No:

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

Management of the Information Security Management System for Hosting Operations, including

Centers, using the Statement of Applicability dated , 2008.

For and on behalf of BSI:

  
President, BSI Management Systems America, Inc.

Originally Registered: 2004

Latest Issue: 2008

Expiry Date: 2010



Page: 1 of 2

**BSI**  
Management  
Systems

This certificate remains the property of BSI and shall be returned immediately upon request.  
An electronic certificate can be authenticated [online](#). Printed copies can be validated at [www.bsigroup.com/ClientDirectory](http://www.bsigroup.com/ClientDirectory).  
To be read in conjunction with the scope above or the attached appendix.  
Americas Headquarters: 12110 Sunset Hills Road, Suite 200, Reston, VA 20190, USA.

# How to get registered

1. Management commitment
2. Define security policy
3. Define ISMS scope
4. Perform risk assessment
5. Risk treatment
6. Select objectives and controls
7. Implement controls
8. Undergo audit by registered audit firm
9. If pass, receive certificate

# Security Policy

- Use what you have or develop one
- Nothing sacred or special here
- Advice: use ISO 27002 as a guide

# ISMS Scope

- Formal statement that describes the activities that are in scope for ISO 27001 registration

# Risk Assessment

- Identify in-scope assets
- Identify threats, vulnerabilities
- Identify impact of threat realization
- Analyze risks

# Risk Treatment

- Treat risks from the risk assessment
  - Mitigate, avoid, transfer, accept
- Identify / create controls to mitigate
- Obtain approval for residual risk

# Create / Select Controls

- Use 27002 (17799) as a guide
  - Omit those you don't need
  - Add others

# Implement Controls

- Processes
- Procedures
- Records

# Get your audit

Get your certificate, hopefully!

# Recap: Required processes

- Risk Assessment
- Risk Treatment Plan
- Incident Management
- Monitoring and Review
- Corrective Action
- Preventive Action

# Recap: Required documents

- ISMS Scope Description
- ISMS Policy (High-Level)
- Asset Inventory
- Operational Procedures and Controls
- Internal Audit Plan, Procedure, and Schedule

# Recap: Required records

- Evidence of Management Risk Decisions
- Evidence of Legal and Regulatory Review
- Evidence of Management Review

# And now for those stories...

...what would you like to know?

# More information

- [iso.org](http://iso.org) or [ansi.org](http://ansi.org) – purchase
  - CHF 126.00 = US\$ 108.72 on 10/27/08
- [bsiamericas.com](http://bsiamericas.com), [kpmg.com](http://kpmg.com), [pjr.com](http://pjr.com)
- [iso-17799.safemode.org](http://iso-17799.safemode.org)
- [iso27001.org](http://iso27001.org) - information

[petergregory@yahoo.com](mailto:petergregory@yahoo.com)  
[www.peterhgregory.com](http://www.peterhgregory.com)