

# Planning for Security

*Presentation for:*

PMI – Northern Utah Professional Development Day 2008

Kevin D. Spease, CISSP-ISSEP



ISSE SERVICES

# Overview

- Security and Compliance
- In the beginning - Initiating
- Before you get started – Planning
- Wrap Up
- Questions



# Security and Compliance

- The goal of Security:
  - Operate with an acceptable level of risk
- The goal of Compliance:
  - Demonstrate due diligence
- Compliance is *not necessarily* secure
- The Challenge:
  - Develop secure systems with compliant designs

*And it starts with Initiating...*



# Initiating

- Consider organizational process assets
  - Security policies, procedures and guidelines
- Include security within project scope
  - Document high-level security requirement
- Project and deliverable requirements
  - Requirements, design and testing artifacts
  - Compliance documentation may be required



# Planning

- System Security Management Plan
- Consider:
  - Security policies, procedures and guidelines
  - Historical data and lessons-learned
  - Configuration management process
  - Expert judgment
    - Professional groups and forums (ISSA & ISACA)
    - Stakeholders (CFO, CIO, CISO, CMO)
    - Consultants



# Planning

- System Security Management Plan
- At a minimum include:
  - Security scope
  - Security-related deliverables
  - Stakeholders
  - Schedule and Milestones
  - *Security Requirements*



# Planning

- Security requirements critical to success
  - *But often ignored, forgotten or skirted*
- Whenever possible, use NIST guidelines
- Good requirements are:
  - Necessary
  - Concise
  - Implementation-free
  - Attainable
  - Complete
  - Consistent
  - Unambiguous



# Wrapping up

- Secure systems begin with good planning
- Understand your compliance environment
- Include security in your project plan
- Solid security requirements are critical



# Questions



ISSE SERVICES

# Resources

- Information Systems Security Association (ISSA) – Utah Chapter
  - [www.issa-utah.org](http://www.issa-utah.org)
- Information Systems Audit and Control Association (ISACA) – Utah
  - [www.isaca-ut.org](http://www.isaca-ut.org)
- National Institute for Standards and Technology (NIST)
  - <http://csrc.nist.gov/publications/PubsSPs.html>



# Contact Information

Kevin Spease

1-866-334-ISSE

[kevin.spease@isse-services.com](mailto:kevin.spease@isse-services.com)

[www.isse-services.com](http://www.isse-services.com)



ISSE SERVICES