



# Professional Services Information Security Practice

Regulatory Compliance Readiness



# Introductions

Andrew Riley, CISSP, CIPP/G, C|EH

Senior Information Security Analyst

[andrew.riley@ncanet.com](mailto:andrew.riley@ncanet.com)

# Agenda

- **What is compliance?**
- **Overview of Compliance Frameworks**
- **What does Regulatory Compliance mean for IT Security?**
- **Limiting Scope**
- **Standards that Drive Security and Compliance**
- **Proactive Approach**

# What is Compliance?

- **A set of standards, enforcement bodies and penalties**
- **Provide a uniformed approach to securing sensitive information for a given jurisdiction (governmental, industry, business partner)**
- **Provide broad coverage of security practices and ensure layered defense**
- **Most allow for flexibility based on the size and complexity of the organization**

# Security Compliance Framework Overview

- HIPAA/HITECH –Healthcare Industry
- SoX 404 –Publicly Traded Corporations
- PCI-DSS –Credit Card Merchants
- GLBA –Financial Services
- CIP –Utilities (Critical Infrastructure)
- 43 states have data breach notification laws

# Health Information Portability and Accountability Act of 1996 (HIPAA)

- Applies to the Healthcare Industry
- Covered Entities
- Defines Electronic Protected Health Information (ePHI)
  - An individual and:
    - The individual's past, present or future physical or mental health; OR
    - The provision of health care to the individual; OR
    - The past, present or future payment for health care.



Continuous Improvement  
for *your* business.

# HIPAA and HITECH

- Security and Privacy Rules
- Enforced by HHS OCR
- Administrative, Physical and Technical Safeguards
- HITECH expands coverage to non-covered entities and adds breach reporting
- Part of the ARRA of 2009
- FTC enforcement for non-covered entities

# Sarbanes-Oxley Act (SOX)

- SOX 404 –Publicly Traded Corporations
- Enforced by SEC
- Ensure internal control over financial reporting
- Management assessment of effective controls
- Disclose Material Weaknesses
- Based on a defined framework –often COBIT

# Sarbanes-Oxley Act (SOX)

- Hosts which process or store financial data that may cause a misstatement
- Auditors attest to and report on management's assessment
- Evaluating Design Effectiveness of Controls
- Testing Operating Effectiveness of Controls

# Payment Card Industry Data Security Standard (PCI-DSS) v1.2

- PCI-DSS –Credit Card Transaction Processors
- ID theft and fraud prevention
- Enforced by the Acquirer (bank or card processor)
- Cardholder Data –Name, PAN, Service Code, Expiration
  - Safeguard
- Sensitive Authentication Data –Magnetic Stripe Data, PIN, Verification Code
  - Can not be stored

# PCI-DSS

- 4 levels
- Self Assessment (Levels 2-4)
- Outside Assessment by QSA for level 1
  - 6 million + transactions/year
- Quarterly scans by ASV for e-commerce sites
- Level 2 Merchants with MasterCard must comply with level 1 rules by 12/31/2010

# Gramm-Leach-Bliley Act of 1999 (GLBA)

- GLBA –Financial Services
- Enforced by FTC
- Safeguards Rule
  - Designate an employee to manage safeguards
  - Develop risk management process
  - Develop, monitor, and test a program to secure the information
  - Evaluate and adjust safeguards as needed with the changes in how information is collected, stored, and used

# GLBA

- Names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers
- FFIEC Sets standards for FDIC, NCUA, OCC, OTS
- FFIEC Guidance –Examination Handbook
- Booklet on Information Security



Continuous Improvement  
for *your* business.

# Indian Gaming Regulations

- National Indian Gaming Commission (NIGC)
- Minimum Internal Controls Standard (MICS)
- Audit and enforcement by NIGC
  - Issuance of violation
  - Assessment of civil fines
  - Issuance of closure orders
- MICS IT Audit Checklist

# State Data Breach Laws

## ■ 43 states have data breach notification laws

Washington Law -Notice of Security Breaches RCW 19.255.010, RCW 42.56.590

- Social security number
- Driver's license number or Washington identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

# What does it mean for IT Security?

- Audit involvement
- Prove that a security control is effective
- Prove a negative statement
- Documentation, logs, change control, authorization
- Segregation of duties
- Business driver for information security
- Security improvements
- Operational efficiency is possible

# Limiting Scope

## Some steps for limiting Compliance Scope

- Don't store unnecessary data
- Compliance Farm - consolidation
- Data Retention Policy
- Network Segmentation
- Encryption
- DLP

# Applicable Standards

## Regulations have their origins in standards

- ISO/IEC 27001:2005 and ISO/IEC 27002
- COBIT – ISACA/ITGI
- NIST 800 Series
- GASSP –I2SF
- Standard of Good Practice –ISF
- Regulating bodies pick and choose requirements; many of which are removed through a public comment process

# Proactive Approach

- Align Security Program with an accepted standard
  - Recommend ISO 27001
- Develop a compliance mapping matrix
  - From standard to applicable compliance framework
- Reference applicable standard and compliance objective in policy works
- Look for ways to further reduce scope
- Monitor legislative activity and industry trends for compliance
- Network within an industry to identify good practices

# NCA has the Vision and the Expertise

**Network Computing Architects, Inc. (NCA), founded in 1992, is a West Coast provider of Information Security, Enterprise Networking, Unified Communications, Wireless, Carrier and IP Product, service and training solutions.**

- Headquartered in Bellevue, WA with regional offices in E.WA, OR & CA
- 50 + Employees

**NCA achieved ISO 27001:2005 ISMS Certification in December 2007.**

NCA is two of sixteen BSI Americas ISO 27001:2005 Associate Consultant Partners and *the first ACP to obtain their own ISO 27001 Certification.*



ISO/IEC 27001:2005 Certified  
# IS 506700



ISO 27001- 012 1207





**Reasonable assurance for *your* information.**