



Security Compliance – How do we get there?

Greg Schmidt, Nokia

NOKIA

Nokia for Business

Overview

- The Need for Compliance
- Compliance Standards and Practices Summary
- Common Themes of Compliance
- Approaches to Meeting Compliance Requirements



The Need for Compliance

NOKIA

Compliance Drivers

The Need to Prove a Acceptable Levels of Risk Management

- Not just about Enron, Worldcom, Tyco, and Livedoor
- High Profile scandals were example of poor risk management related to Financial Reporting

Restore and Ensure Confidence in Business

- By ensuring proper Security Controls are in place
- Certification

Evolution of Security Threats and Risks

- The change in how we do business
- Vectors, Vulnerabilities and Threat

Security and Executive Level Relationship

Executive and IT Relationship in the Past

- Many organisations had limited connection between IT Security and Executive Level

Compliance is forcing Integration of Security at Board Level

- Executive Level must be aware and risk and it's management
- IT Security Compliance requiring certification of CEO and CIO
- Compliance Processes require ownership of policy by Executive Level

IT Security Providing Verification of Process and Implementation

- As part of Compliance
- Through ongoing operation

The Long Reach of Security Compliance

Not Limited to Industry Sectors or Countries

Will have a Significant Impact on most every business

IT Security Professionals will be critical to success



Compliance Standards and Practices Summary

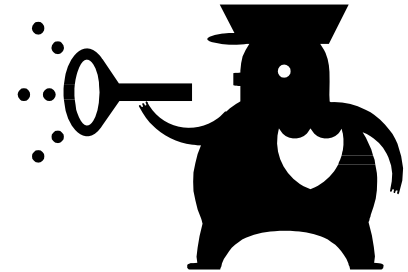
NOKIA

Nokia for Business

Compliance Standards and Practices

■ Sources for Compliance requirements

- Government agencies
- National laws
- Industry Certification bodies
- Internal Corporate Directive or Security Policy



■ Variety of Compliance Guidance

- Regulatory
- Standards
- Best Practices

Sarbanes-Oxley

■ History and Focus

- Response to high profile scandals
- Required for Public Corporations Traded in US

■ Major Provisions

- “C” Level Certification of Financial Reports
- Disclosure of controls that relate to reporting
- Auditor independence
- Section 404
- Specific versus Pervasive Controls

■ COSO\COBIT as recommended Framework for IT Compliance

Also known as SOX and SARBOX

COSO

■ History and Focus

- Sponsored by 5 major accounting groups
- In response to private sector accounting scandals
- Management as Audience

■ Key Concepts

- Internal Controls as Process
- Internal Controls are affected by People
- Controls provide Reasonable not Absolute Assurance

■ Main Provisions

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring



COBIT

■ History and Focus

- Created in 1992 by ISACA and ITGI as Best Practices Framework
- IT as Audience
- Focus on Information needed to support business
- Provides IT Guidance missing from COSO
- Includes IT guidance beyond Security
- Complimentary to ISO 27001/27002

■ Key Concepts

- 4 Key Domains
- 34 High Level Objectives
- 318 Control Objectives

■ Key Domains

- Planning and Organisation
- Acquisition and Implementation
- Delivery and Support
- Monitoring



PCI DSS

■ History and Focus

- Created by Credit Card industry (Visa, MasterCard, Amex)
- Pertains to any company that stores or transmits Personal Account Number (PAN)

■ Key Concepts

- Certification for service providers and merchants
- Protection of storage and transmission of PAN
- 12 Main Requirements in 6 Areas

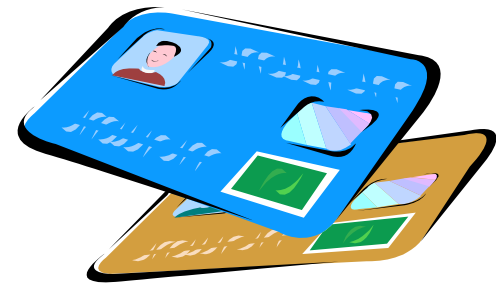
■ Main Provisions

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Vulnerability Management Program
- Strong Access Control
- Monitor and Test Networks
- Maintain Information Security Policy

■ Special Provision

- Compensating Controls
- Network Segmentation

Payment Card Industry
Data Security Standard



ISO 27001/27002

■ History and Focus

- Known by a variety of Names
 - Being renamed as part of ISO 27000 series
- Focus is IT Security

■ Differences in versions

- ISO 27001- Specification of ISMS
- ISO 27002- International Code of Practice for ISMS
- ISO 27002- Suitable controls to meet ISO 270001

■ Key Concepts

- Confidentiality, Integrity Availability
- Specific Security Controls are not recommended
- Integration with Cobit

Also known as

BS7799

BS7799-2

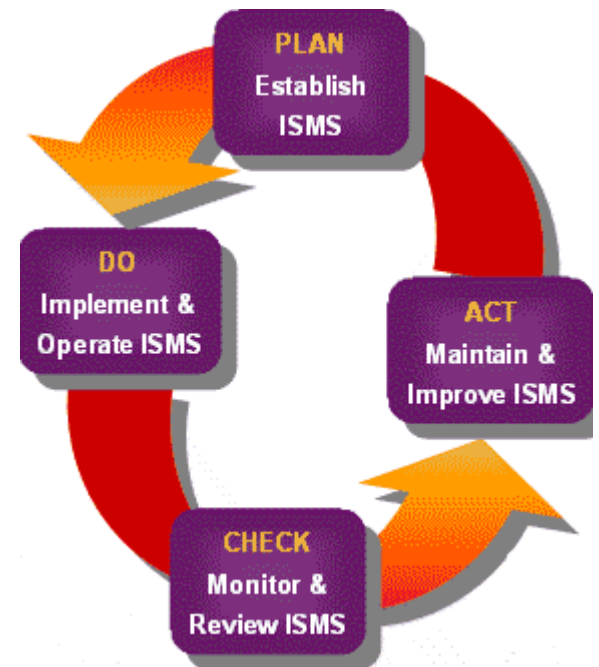
ISO 17799

ISO 27001/27002

■ Main Provisions

- 12 Main Sections
- 39 Control Objectives
- Specific Security Controls not Required
 - More flexible across organisation
 - Provides flexibility for technology change
 - Difficult for external certification
- Integration with COBIT

■ Plan, Do, Check, Act





Common Themes of Compliance

NOKIA

Nokia for Business

Common Compliance Themes

- Knowledge of and control your assets
- Centralised Control and Management
- Apply Controls in response to Risk
- Granular control of access and authentication
- Integration of Security and Business
- Follows existing Best Practice guidance





Approaches to Meeting Compliance Requirements

NOKIA

Nokia for Business

Don't Wait for Compliance to find You

■ Choose reliable providers and products

- Avoid Point Solutions
- Avoid Second Tier Vendors

■ Ensure you suppliers can support their products

- Software update
- Bug Fix
- Signature

■ Take a Wider View of Compliance

- Implement solutions that address core areas
 - Access and authorisation controls
 - Private networks and segmentation
 - Intrusion Detection
 - Centralised Management



Remember what Drives the Business

- **Consider solutions with Business in mind**
- **Improve Fundamental Business Value**
- **Create Differentiators**
- **Keep focus on User experience**
- **Use Compliance to help raise efficiency**



Implement Solutions for the Future

- Be aware of changing threats
- Review what is not working *and* what is working
- Plan Do Check Act



NOKIA

Nokia

Your Partner in Compliance

Nokia for Business

Nokia Firewall Security Solutions

■ Nokia/Check Point Firewall Solution

- Appliance based firewall solution
- 10 year Partnership with Check Point
- Over 600,000 installations globally

■ Strong and Flexible features

- Centralised Management and logging
- Role based authentication
- Global Policy Management/Deployment
- Complete access and audit trails

■ Provides compliance controls across Standards and Practices

- SOX (404)
- COSO (Control Activities)
- COBIT (DS5)
- PCI (Network Segmentation, Access Control, Secure Network)
- ISO (Communications & Ops Mgmt, Access Control)



Nokia IPS Threat Management Solutions

■ Nokia/SourceFire IPS Solution

- Appliance based firewall solution
- Best of Breed Nokia and SourceFire IPS

■ Strong and Flexible features

- IDS/IPS Option
- RNA for Network and host compliance
- Centralised Management
- Built-in Incident Management tools

■ Provides compliance controls across Standards and Practices

- SOX (404)
- COSO (Control Activities)
- COBIT (DS5)
- PCI (Network Segmentation, Secure Network)
- ISO (Communications & Ops Mgmt, Access Control, Incident Management)



What Next?

- **The Future is Compliance**
- **Leverage Compliance to Improve Security and Business**
- **ISO2700x and COBIT**
- **Make Decisions now with Compliance in Mind**



Helpful Links

Sarbanes Oxley

thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm

COSO

www.coso.org

PCI

www.pcisecuritystandards.org

COBIT

www.isca.com/cobit

ISO 27001/27002

www.iso27001security.com

ISF

www.isfsecuritystandard.com

ITIL

www.itil.co.uk

Thank You

NOKIA

Nokia for Business