Balancing Between Risk and Compliance

Dave Mann, Ph.D.
Senior Security Strategist
BindView Development

Business is risky!

- Want low risk?
  - Get a savings account
- Risk Appetite = Organizational need for risk
  - Different for NSA, Local State College and You
- Risk Posture = Actual status of risk
  - Assumed
  - Mitigated
  - Transferred
- Objective: Balance risk posture against risk appetite

Risk Management supports business goals

Business Goals

Serve Customer, Share Holder Value, Reduce Costs, Regulatory Compliance, Increase Revenues…

Corporate Governance (Risk Appetite)

Policies and Procedures including: Financial, Human Resources, Security/IT…

Practices and Implementation (Risk Posture)

Accounts, Customers, Personnel, Manufacturing, Physical Plant, IT Infrastructure…

IT Risk Management: Subset of corporate risk management

Business Goals

Serve Customer, Share Holder Value, Reduce Costs, Regulatory Compliance, Increase Revenues…

IT Governance (Risk Appetite)

IT and Security Policies and Procedures including: Acceptable Use, Monitoring, Vulnerability Management, Perimeter Security, 3rd-Party Access, Outsourcing, Access Control, Information Classification…

IT Practices and Implementation (Risk Posture)

User Management, Desk Tops, Servers, Mail, Security Audit, Intrusion Detection, NOC, Back-up and Recovery, Asset Management…

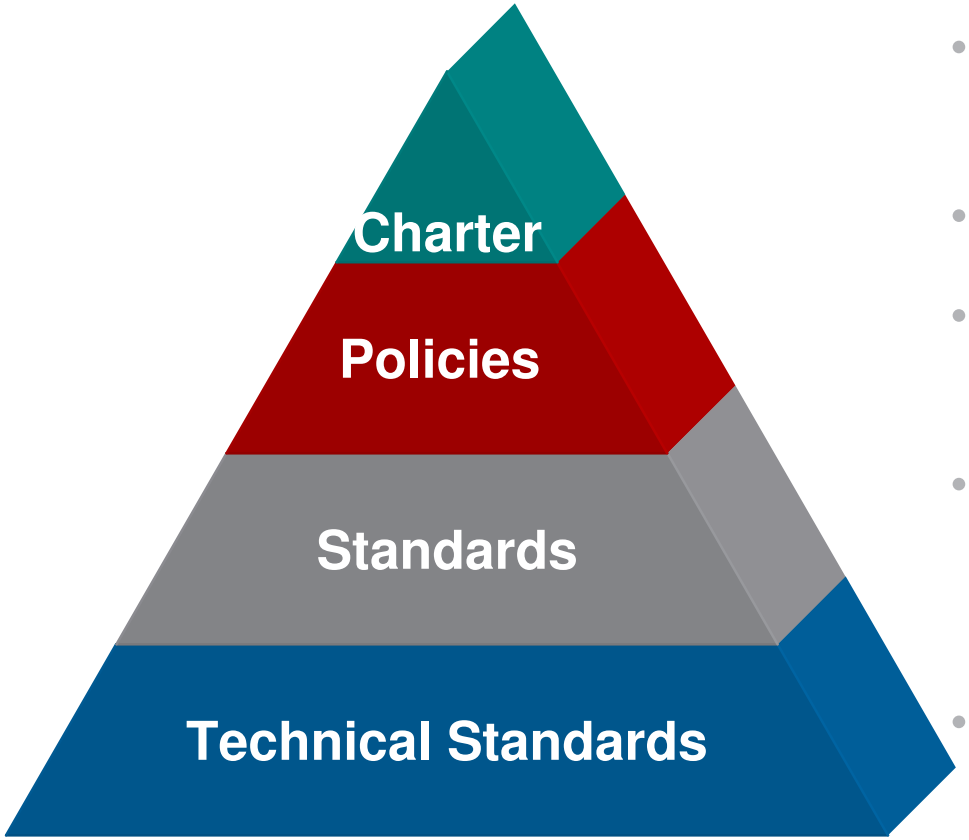
Key questions

- How do we determine the appropriate risk appetite for our organization?
- How can we translate our risk goals into action?
- How can we determine if our risk posture matches our risk appetite?
- Do the answers to these questions change given our new regulatory responsibilities.

Outline

- Introduction and context (done)
- Five tools of risk management
- Overview of regulatory compliance
- Changes to risk management for compliance
- Resources, review and Q&A

Tool #1: Security Policy Framework

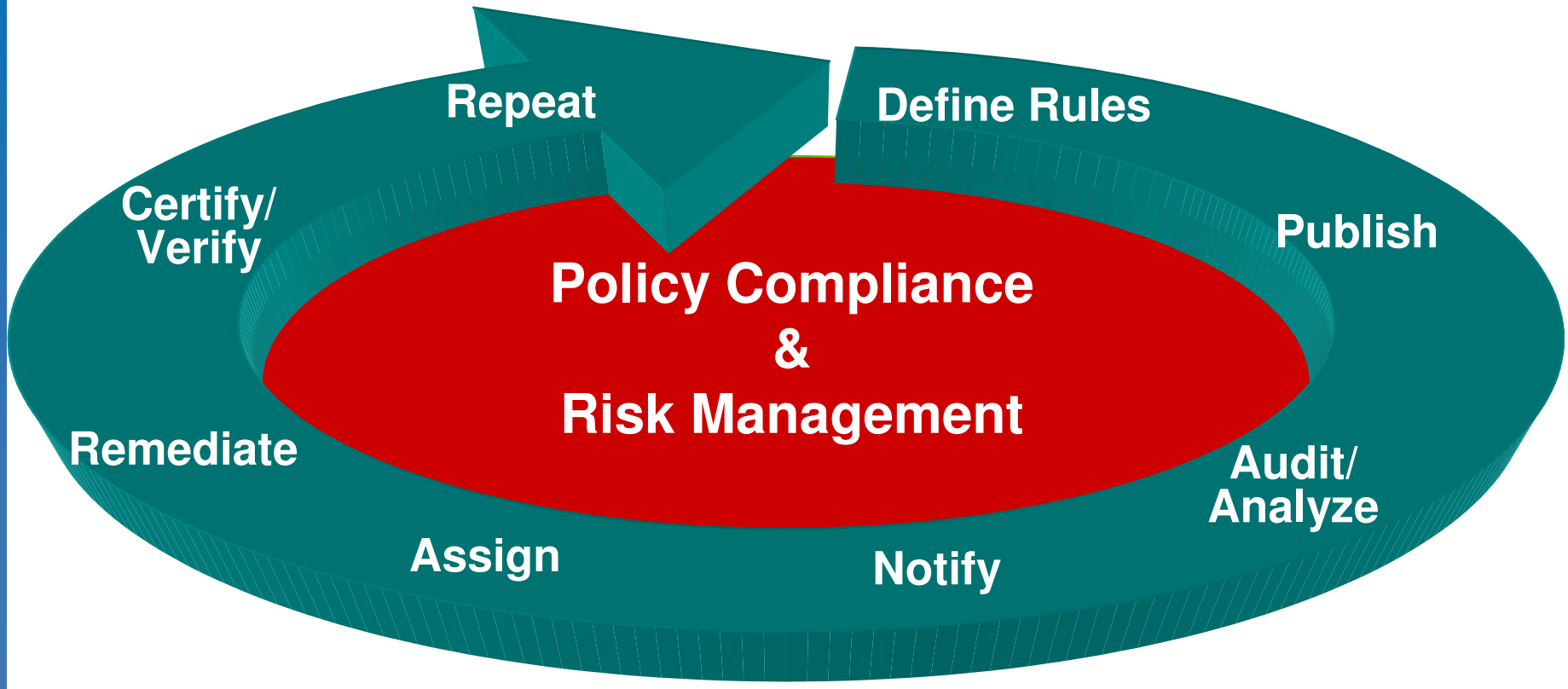


- Charter - Authorization and commitment
- Policies - Defines goals
- Standards – People & procedures
- Technical Standards - Specific configurations for technologies
- Structure should be
  - Hierarchical
  - Modular

IT and Security Policy

- Hierarchical models facilitates discussion and buy-in at appropriate levels
- Modular structure:
  - Focused update and revision process
  - Step-wise improvement and roll-out
  - Faster, easier navigation
- Avoid puny policies
  - Consider the “laugh” test
- Avoid monolithic monstrosities
  - The perfect is the enemy of the good

Tool #2: Risk Management Life-Cycle



Life-Cycle Methodology

- Applied to Policies and Procedures
  - Are the policies defined?
  - Are they sufficient?
  - Are people aware of them?
  - Do they need to be revised?
- Applied to Processes and Implementations
  - What are the policy goals?
  - How can they be implemented?
  - Is the implementation sufficient?
  - Who needs to be notified to make changes?
  - Fix it!
  - Verify it!

Tool #3: Risk Analysis

- Goal: Make informed cost/benefit decisions regarding risk
- General Definitions
  - Risk = Probability x Impact
  - Probability = Chance of something bad happening
  - Impact = The cost of something bad happening
- E.g. Rock Climbing & Driving
  - Risk (Climbing) = Chance of falling x Impact of falling
  - Risk (Driving) = Chance of accident x Impact of crash

Defining Risk for IT

- Risk = (Threat x Vulnerability) x Value Lost
- Threat = Something that could do harm (storm, hacker, mike in accounting)
- Vulnerability = Weakness that allows threat in
- Value = Hard value of asset in question
- E.g. Customer data in a DB
  - Threat: Mike in accounting
  - Vulnerability: Weak passwords

Putting Dollars on IT Risk

- Annualized Loss Expectancy (ALE) =
  - Probability x Value Lost x Expected Frequency
  - (Threat x Vulnerability) x Value Lost x Expected Frequency
- Example: Worm infestation
  - 45% of systems unpatched
  - $450,000 hard costs to recover per incident
  - 5 year average of incidents = 3 active worms / year
  - ALE = (.45) x ($450,000) x 3 = $607,500

Classic cost/benefit analysis using ALE

- Goal: Determine value of counter-measure
- Value of counter-measure =
  ALE before counter-measure –
  ALE after counter-measure –
  Annualized cost of counter-measure
- Example: Patch Solution

(ALE before)	$607,500 –
(ALE after)	$ 53,000 –
(Patch cost)	$200,000 =
(Value)	$354,500

Two approaches to Risk Analysis

- Quantitative:
  - Drives toward hard numbers
  - Expensive and time consuming
- Qualitative:
  - Softer numbers and heuristics
  - Cheaper and faster
- Which is better?
  - Depends on your organization/audience
  - Law of diminishing returns applies

Tool #4: Technical Standards

- Interprets policy for different technologies
- Specific to technology platform
  - Windows 2000 versus HP-UX
- Specific to business use and threat model
  - Internet-facing web server versus internal file-server
- Common approach:
  - Define all types of deployed “business systems”
  - Document Technical Standard for each class

Tool #5: Internal Audit

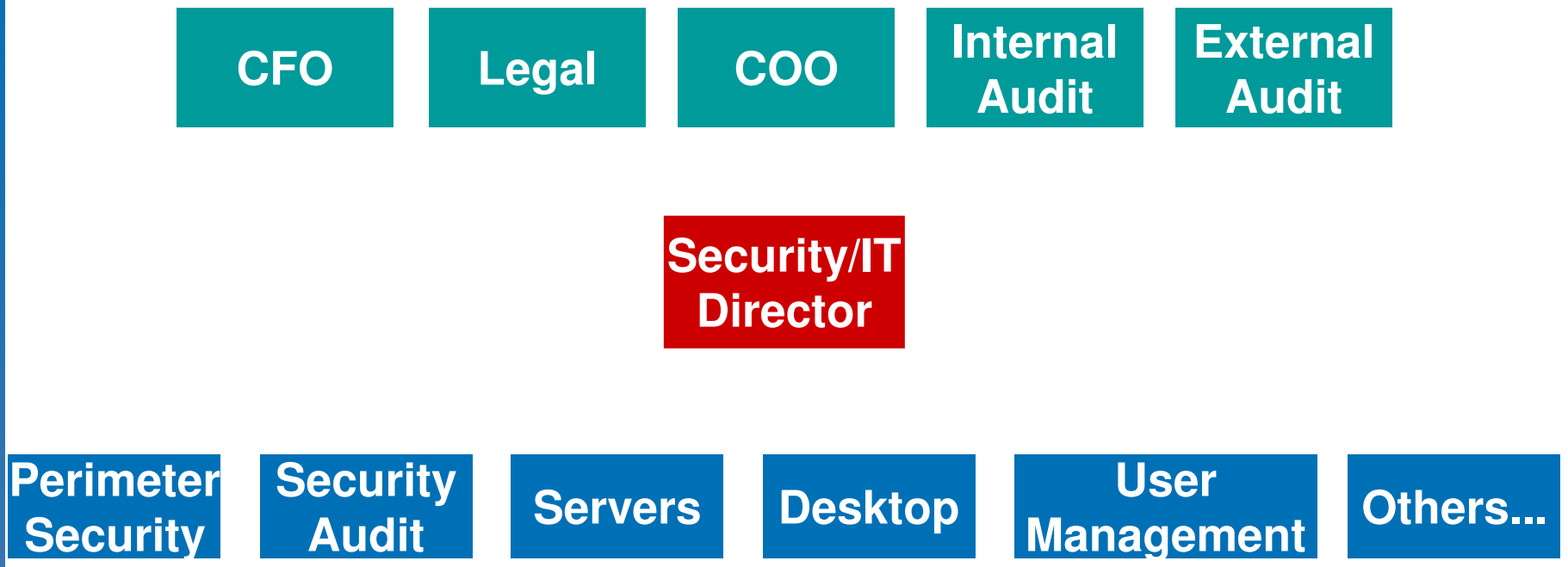
- Critical part of Risk Management Life-cycle
  - Initial audit drives gap analysis
  - Retest to certify compliance
- Standards (procedures) and Technical Standards should be auditable by design
  - You can not manage what you can not measure
- Audit against Technical Standards
- Goals:
  - Audit on demand (good)
  - On-going audit (better)

Outline

- Introduction and context
- Five tools of risk management
- Overview of regulatory compliance
- Changes to risk management for compliance
- Resources, review and Q&A

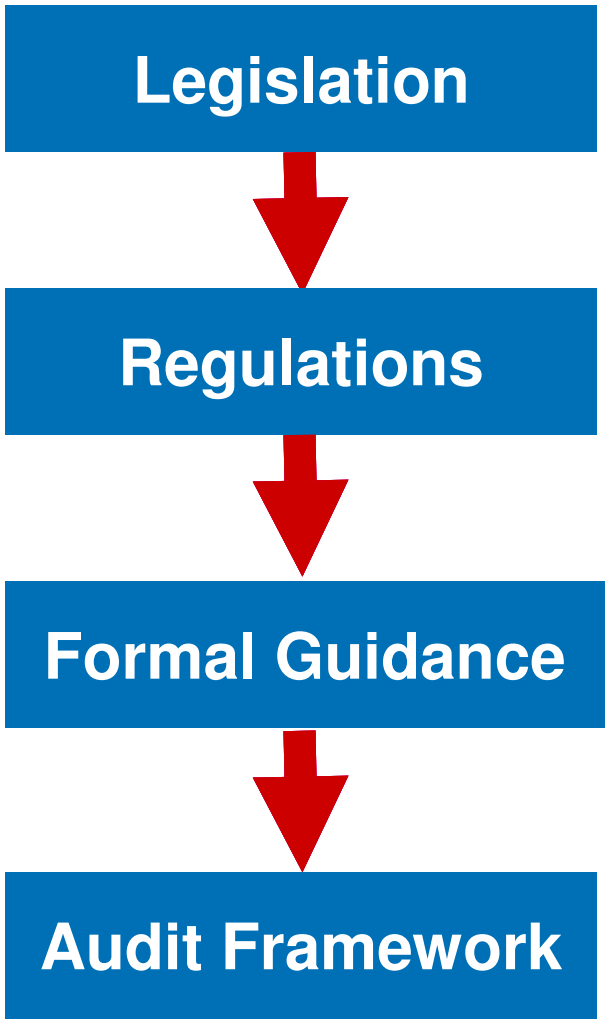
New business challenge
Surrender: You are surrounded!

New internal challenge
Multiple stakeholders



Looking for Shared:
Language, Experience, Expectations…

Pieces of the puzzle
An example



- **Sarbanes-Oxley Act**
  - **Issued by Congress**
- **Securities Exchange Act of 1934**
  - **Section 240, 13a – 15**
  - **Published by SEC**

SOX

- **Public Company Accounting Oversight Board**
  - **Financial reporting guidance**
- **COSO**
  - **Financial auditing framework**
- **COBIT**
  - **IT governance framework**

The real challenge

Pass the audit - 2 Layers of interest

Business Process Layer

COSO is the standard the "Big Four" have created for use in evaluating best practices and financial controls

IT Infrastructure Layer

COBIT is the standard the "Big Four" have created for use in evaluating best practices and controls for IT governance

ISO 17799 is a detailed security standard that auditors use (ISO 17799 maps into COBIT)

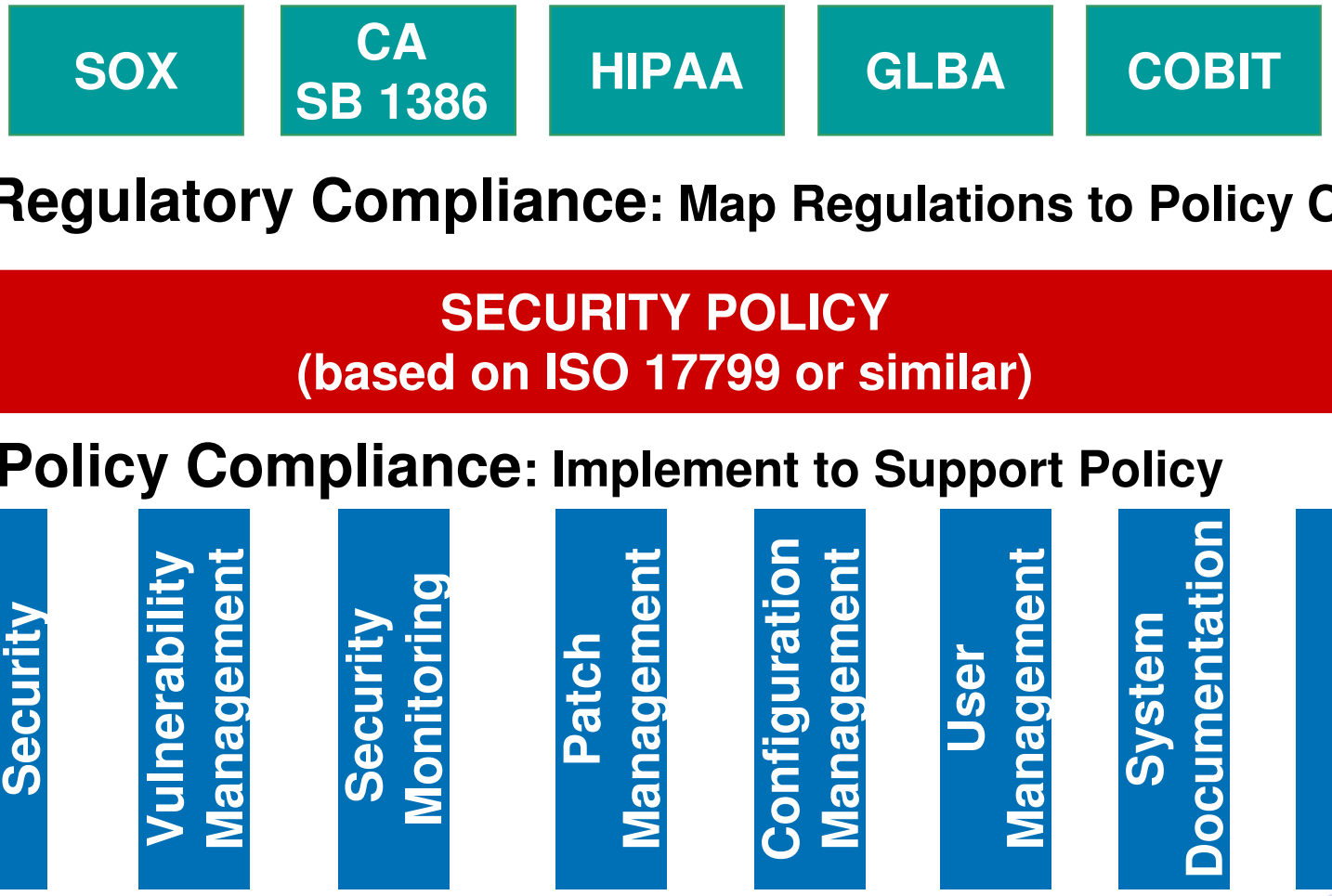
Center for Internet Security Benchmarks are industry backed configuration best practices for specific technical platforms

Case Study – Health Insurance

	Sarbanes-Oxley	HIPAA	FISMA
Business Process Controls	☑	☑	☑
IT General Controls	**ISO 17799 or CobiT each cover all the bases**		

Our approach to meet the general controls requirements for all of our requirements is to implement a security program based on ISO 17799 – Source: Director of Security

Policy-Based Compliance Strategy



Outline

- Introduction and context
- Five tools of risk management
- Overview of regulatory compliance
- Changes to risk management for compliance
- Resources, review and Q&A

Increased role of “best practices”

- Defends “due-care”
  - Looked for by auditors
  - Consider the “mom” test
- Must be customized to your environment
  - Reasonability and documentation are key
  - Document what you do and do what you document
- Applies to every level
  - IT Governance: COBIT
  - IT / Security Policy: ISO 17799, NIST sp800-53
  - OS Configurations: CIS Benchmarks

The auditor will interpret the regulations, beginning with an assumption of compliance best practices, and look for a policy statement that describes how the company will comply with different aspects of the regulations. (Gartner COM-22-1253)

Increased need for documentation

- Not enough to be right
- Must produce documentation for
  - Audits
  - Regulatory inspection
- Document what you do & do what you document
- Applies to every level
  - Policies
  - Procedures
  - People
  - Technical Standards

Documentation tips

- Map requirements into policy layers
  - Charter: HIPAA, GLBA, FISMA, SOX
  - Policy: COBIT, ISO 17799, NIST sp800-53
  - Standards: ISO 17799, FFIEC
  - Technical Standards: CIS Benchmarks
- Use RTM to map requirements to controls

SECURITY REQUIREMENTS	MAPPING	NEEDED SECURITY CONTROLS
Security Requirement No. 1	1 TO 1	PS-1.b
Security Requirement No. 2	1 TO MANY	PE-2.b, PE-3.b, PE-6.c, PE-7.b
Security Requirement No. 3 Security Requirement No. 4	MANY TO 1	CM-2.c
Security Requirement No. 5 Security Requirement No. 6	MANY TO MANY	IA-1.c, IA-2.c, IA-4.b

TABLE 2: SAMPLE REQUIREMENTS TRACEABILITY MATRIX

Regulations forcing IT to mature
Interface among governance frameworks clarifying

- Public Sector:
  - COSO becoming standard for financial governance
  - COBIT is IT governance extension to COSO
  - ISO 17799 maps into COBIT
  - CIS Benchmarks support ISO 17799
- Prediction: You will deal with ISO 17799 in next 2 years
- Federal Sector:
  - NIST guidance continuing to mature
  - sp800-53 should finalize by 2005

Requirements bringing shift in emphasis

- More need for…
  - Configuration Management
  - User Management
  - System Documentation
- Tried and true practices remain relevant
  - Vulnerability Management
  - Patch Management remain

Policy Management

- ISO 17799 Requirements
  - 3.1.1 Information security policy document
  - 3.1.2 Review and evaluation
  - 4.1.1 Management information security forum
  - 4.1.2 Information security co-ordination
  - 4.1.3 Allocation of information security responsibilities
  - 4.1.4 Authorization process for information processing facilities
  - 4.1.5 Specialist information security advice
  - 4.1.6 Co-operation between organizations
  - 4.1.7 Independent review of information security
  - 4.2.1 Identification of risks from third party access
  - 4.2.2 Security requirements in third party contracts
  - 4.3.1 Security requirements in outsourcing contracts

Vulnerability Management

- ISO 17799 Requirements
  - 8.3.1 Controls against malicious software
  - 9.4.9 Security of network services
  - 12.2.2 Technical compliance checking

Configuration Management

- ISO 17799 Requirements
  - 7.3.1 Clear desk and clear screen policy
  - 8.1.3 Incident management procedures
  - 8.3.1 Controls against malicious software
  - 9.3.1 Password use
  - 9.3.2 Unattended user equipment
  - 9.4.1 Policy on use of network services
  - 9.4.3 User authentication for external connections
  - 9.4.7 Network connection control
  - 9.4.9 Security of network services
  - 9.5.2 Terminal log-on procedures
  - 9.5.3 User identification and authentication
  - 9.5.4 Password management system
  - 9.5.5 Use of system utilities
  - 9.6.1 Information access restriction
  - 9.7.1 Event logging
  - 9.7.2 Monitoring system use
  - 10.3.2 Encryption
  - 10.4.1 Control of operational software
  - 10.4.3 Access control to program source library
  - 12.1.5 Prevention of misuse of information processing facilities
  - 12.2.2 Technical compliance checking

Patch Management

- ISO 17799 Requirements
  - 5.1.1 Inventory of assets
  - 9.4.9 Security of network services
  - 9.7.3 Clock synchronization
  - 10.4.1 Control of operational software
  - 10.5.3 Restrictions on changes to software packages

User Management

- ISO 17799 Requirements
  - 8.1.4 Separation of IT administrative duties
  - 9.2.1 IT user account management
  - 9.2.2 Manage user privileges
  - 9.2.3 user PW management
  - 9.2.4 Controls and audits rights
  - 9.2.1 User registration
  - 9.2.2 Privilege management
  - 9.2.3 User password management
  - 9.2.4 Review of user access rights
  - 9.3.1 Password use
  - 9.4.3 Enforced path
  - 9.4.3 User authentication for external connections
  - 9.5.2 Terminal log-on procedures
  - 9.5.3 User identification and authentication
  - 9.5.4 Password management system
  - 9.5.8 Limitation of connection time
  - 9.6.1 Information access restriction
  - 9.6.2 Sensitive system isolation
  - 9.7.1 Event logging
  - 9.7.2 Monitoring system use

Again, a shift in emphasis

- More need for…
  - Configuration Management
  - User Management
  - System Documentation
- Tried and true practices remain relevant
  - Vulnerability Management
  - Patch Management remain

Risk analysis calculus must change

- Classic RA only considers value of asset to organization
- Audit failure must be considered as new threat
- Deviation from “best-practices” must be considered as new vulnerability
- Valuation of asset loss must include fines, penalties and remediation costs
- E.g. Consider loss of confidentiality of customer data
  - Then: Small cost
  - Now: High cost

Outline

- Introduction and context
- Five tools of risk management
- Overview of regulatory compliance
- Changes to risk management for compliance
- Resources, review and Q&A

Additional Resources
Regulatory Information

- Sarbanes-Oxley
  - http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
  - PCAOB – http://www.pcaobus.org/
- HIPAA
  - http://www.cms.hhs.gov/hipaa/
  - http://aspe.hhs.gov/admnsimp/nprm/seclist.htm
- FISMA
  - http://www.fedcirc.gov/library/legislation/FISMA.html
  - http://csrc.nist.gov/sec-cert/

Additional Resources
Security Frameworks

- ISO 17799
  - http://www.iso.org/iso/en/ISOOnline.frontpage
- COBIT
  - www.isaca.org/cobit.htm
- NIST SP 800-53
  - http://csrc.nist.gov/publications/nistpubs/index.html
- CERT/SEI
  - http://www.sei.cmu.edu/cmm/cmm.html

Additional Resources
Configuration Standards

- CIS Benchmarks
  - www.cisecurity.org/
- NSA Security Guides
  - http://www.nsa.gov/snac/index.html
- NIST Checklist Portal
  - http://csrc.nist.gov/checklists/

Additional Resources
Vulnerability Information

- MITRE CVE List
  - http://cve.mitre.org/
- SANS Top 20 List and SANS Alerts
  - http://www.sans.org/top20/
- CERT Advisories
  - http://www.cert.org/advisories/
- Neohapsis Archives
  - http://archives.neohapsis.com/
- NIST ICAT Vulnerability Database
  - http://icat.nist.gov/icat.cfm
- Vuln-Dev Mail List
  - http://www.vulnwatch.org/

Additional Resources
BindView White Papers

- Implementing ISO 17799:
  A Practical Guide
  - http://www.bindview.com/iso17799
- Practical Security and Risk Management: The Good Guys Fight Back
  - http://www.bindview.com/riskmanagement1

Summary

- Policy defines corporate risk appetite
  - Bridge between business goals and reality
  - Lynch-pin of compliance strategy
- Life-cycle methodology for risk management
- Use appropriate rigor to analyze options
  - Consider cost of audit failure and penalties
- Get familiar with ISO 17799
- Get organized and specific with Configuration Standards
- Document your decisions

THANK YOU!

- Questions and Answers

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP