INFORMATION SECURITY
SearchSecurity.com
INFORMATION SECURITY DECISIONS

Building A Framework-based Compliance Program

Richard E. Mackey, Jr.
Vice President, SystemExperts Corp.
dick.mackey@systemexperts.com

Agenda

- The compliance process
- Assembling requirements
- Useful frameworks
- Capturing your state
- Achieving compliance
- Using ISO with PCI

The Key to Compliance

- Compliance with any regulation, contract or standard requires a process
- The keys to success:
  - Understanding your goals
  - Choosing appropriate metrics
  - Following a consistent approach
  - Establishing realistic expectations for progress
  - Ensuring discipline and organizational commitment
- Remember two themes
  - Compliance, like all of security, is a process
  - Good security is good security

Assembling Requirements

- There are many possible compliance objectives
- Regulatory
  - SOX
  - GLBA
  - HIPAA
  - FFIEC
- Contractual (e.g., PCI, partnerships)
- Standards of practice (e.g., ISO 17799)
- Which ones does your organization require?

Sources of Requirements

- HIPAA
  - The HIPAA Security and Privacy Rules focus on protecting electronic protected health information
  - *NIST guides (e.g., SP 800-66)*
  - Medicare HIPAA guides @ cms.hhs.gov
- PCI
  - *Payment Card Industry (PCI) Data Security Standard*
  - *Self-Assessment Questionnaire*
  - *Security Audit Procedures*
  - *Security Scanning Procedures*

More Sources

- SOX
  - Sarbanes-Oxley Act
  - *IT Control Objectives for Sarbanes Oxley* from ITGI
- GLBA
  - *Interagency Guidelines Establishing Information Security Standards*
  - GLBA
- FFIEC
  - *IT Security Examination Handbook*
- ISO 17799 and COBIT
- Partnership contracts
  - Required for regulations like FFIEC, HIPAA and GLBA

Charting Your Course

- *Understand* your regulatory requirements
  - Regulatory rules and *interpretation*
  - Scope required for compliance
  - Apply risks and controls *to your organization*
- Choose appropriate control objectives
  - Analyze standards for control objectives
- Establish metrics
  - Use previous audits as a guide
  - Enlist professional help in understanding current practice and audit guidelines
  - Document your control objectives

ISO 17799 Overview

- “Code of Practice for Information Security Management”
- A laundry list of practices
- Not prescriptive
- Now called ISO 27002
- Needs to be interpreted according to business needs
- Can be used to find specific practices and controls to meet requirements
- Every major section is required by virtually every regulation

ISO Sections

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Incident Response
- Business continuity
- Compliance

Assess Yourself

- Document your required controls
  - Derived from ISO 17799 or COBIT
- Review the current state of controls versus your required controls
- Capture your state
  - Give yourself a report card
  - Document *why* each area was judged to be compliant, partially compliant or noncompliant
  - Store your results for future analysis

Measuring Maturity

- Evaluate the maturity of controls
  - Stage 0: Non-existent
  - Stage 1: Ad hoc
  - Stage 2: Repeatable but intuitive
  - Stage 3: Defined process
  - Stage 4: Managed and measurable
  - Stage 5: Optimized
- Evaluate the effectiveness of controls
  - Look critically at where measures have failed

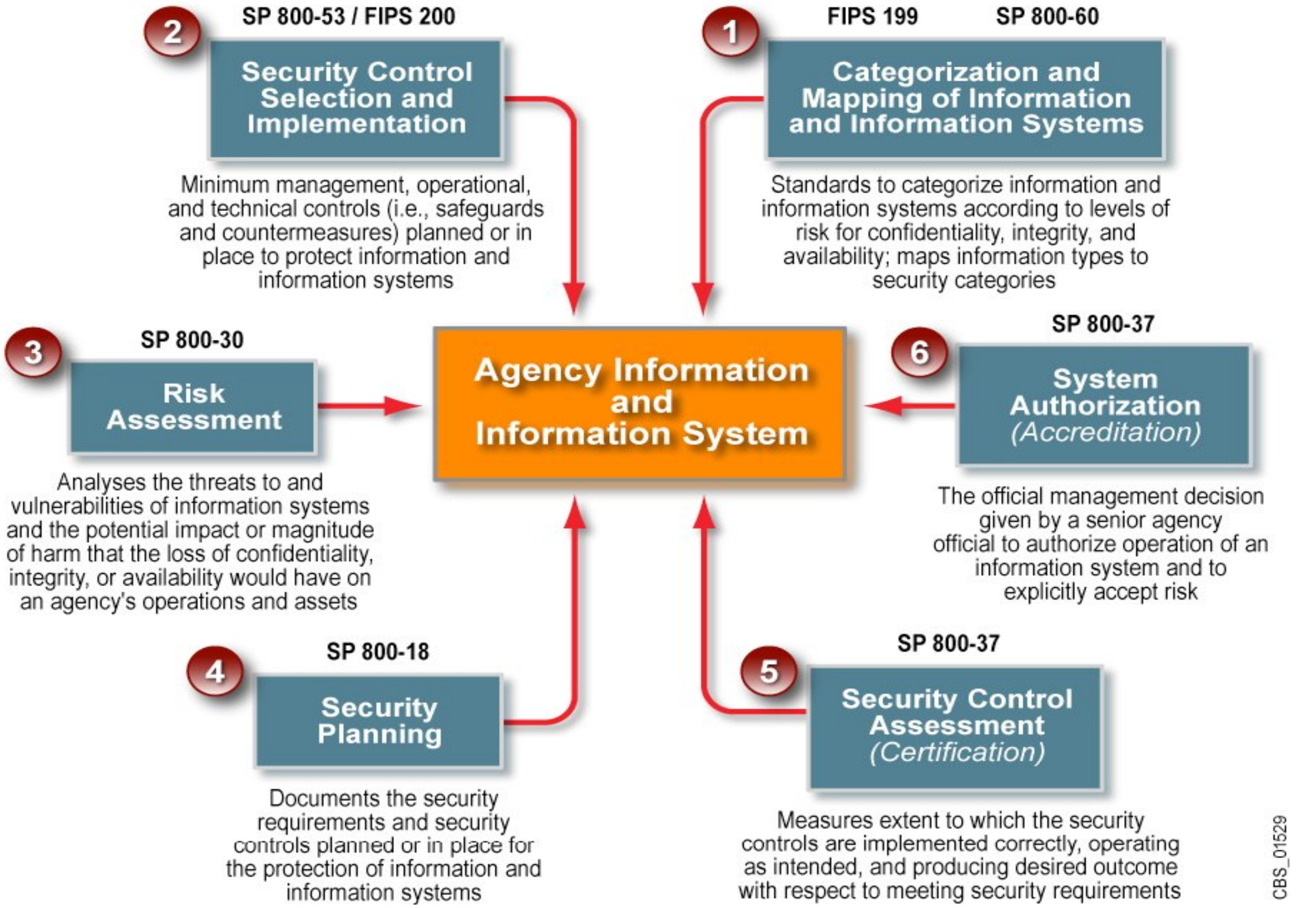
Achieving Compliance

- Assemble the list of non-compliant areas
- Assign a priority to each
- Look for tasks that address root causes
  - Examples: Risk assessment processes, information cataloging and classification, data handling policies and procedures, policy and organization
- Look for easy tasks
- Integrate process improvements into everyday operations

Common Elements of Compliance

- All compliance guidelines describe similar requirements
- Common elements
  - Information analysis (ownership, custodianship, use, sensitivity)
  - Risk assessment
  - Policy, process and technical control establishment
  - Measurement of effectiveness
  - Adjustment and adaptation to improve
  - Repetition of steps
- ISO 27001 follows the PDCA process
  - Plan, do, check, act
- COSO, COBIT, HIPAA and FFIEC compliance require similar processes

NIST HIPAA Process



Agency Information and Information System

1 FIPS 199 SP 800-60

Categorization and Mapping of Information and Information Systems

Standards to categorize information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories

2 SP 800-53 / FIPS 200

Security Control Selection and Implementation

Minimum management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems

3 SP 800-30

Risk Assessment

Analyses the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets

4 SP 800-18

Security Planning

Documents the security requirements and security controls planned or in place for the protection of information and information systems

5 SP 800-37

Security Control Assessment *(Certification)*

Measures extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

6 SP 800-37

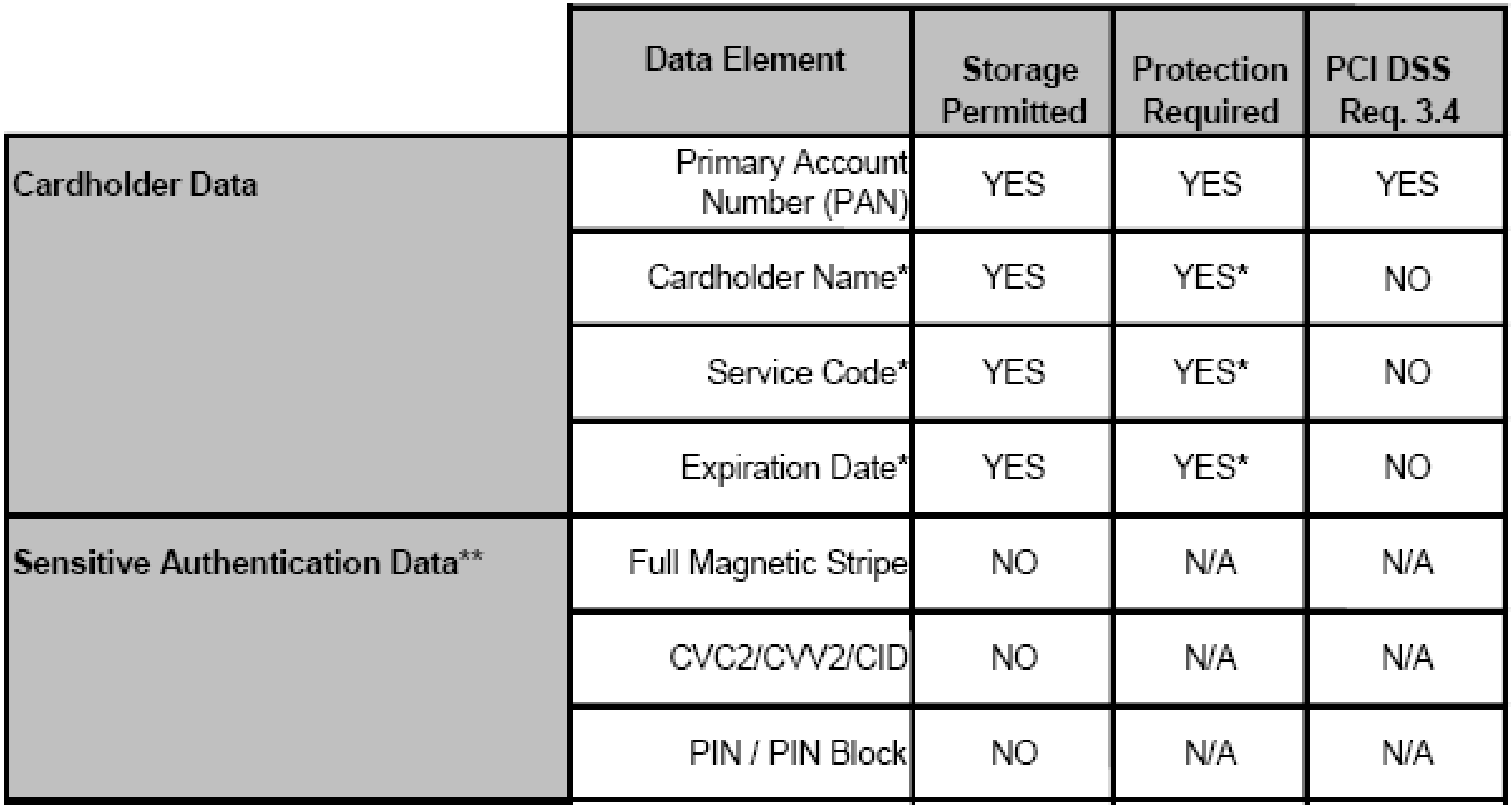
System Authorization *(Accreditation)*

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept risk

PCI

- Payment Card Industry Data Security Standard
- PCI Standards Security Council establishes common standard for ensuring security measures
  - VISA, Mastercard, Amex, JCB, Discover, etc.
- The standard must be followed by any organization that stores or processes credit card data
  - PAN – The number on the card
  - Stripe data
  - ID code

PCI Information Handling



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

Applying ISO to PCI

- Assemble requirements from PCI DSS “digital dozen”
- Map to ISO practices
- Determine level of practice necessary
- Conduct assessment according to merchant level

Example PCI Requirement	ISO Section Mapping
Protect cardholder data	7. Asset management, 11. Access control
Maintain security policy	5. Security policy, 6. Security organization, 8. Human resources (training and awareness)
Restrict physical access to cardholder data	9. Physical and environmental security

The Long and Short of PCI

- PCI provides relatively specific requirements
- PCI defines the scope
- PCI defines data classification
- PCI concentrates on data handling
- Challenges
  - Soft areas like policy
  - Partner management
  - Product security

Summary

- Challenges
  - Assembling all *your* compliance requirements from a common framework
  - Understanding *your* risk
  - Having good metrics that apply to your organization
  - Establishing a sustainable process
  - Creating and maintaining documentation
- Be sure to include
  - Regular review of goals and metrics
  - Integration of compliance activities into everyday operation