Ensuring Your Outsourcers Meet Your Compliance Mandates

Richard E. Mackey, Jr.

Vice President

SystemExperts Corporation

dick.mackey@systemexperts.com

Agenda

- Roles of service providers
- Compliance impact
- Risk analysis
- Reviewing service provider practices
- Example regulatory requirements
- Monitoring relationships
- Incident response & business continuity
- Technology

Service Providers & Partners

- **Service partners are a fact of life**
- **Organizations can outsource everything**
  - Record keeping
  - Printing
  - Advice
  - Customer service
  - Managed security services
  - Human resources
  - Cafeteria services
  - Sales
- **With all these relationships, comes risk**

Service Providers and Compliance

- One risk is compliance…
- Information you share with service providers can have regulatory implications
- The risks include fines, suspension of privileges, increased audit frequency, and criminal charges

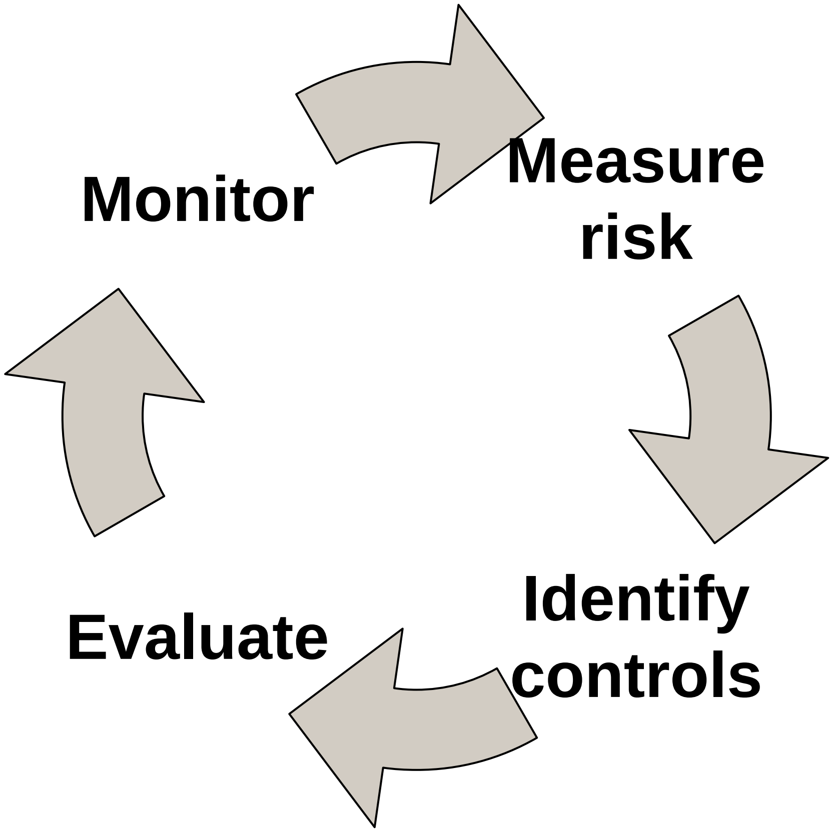
Information	Regulation
PII	Privacy
Payment card	PCI
Personal Financial	GLB
Health	HIPAA
Corporate Financials	SOX

Regulations and Service Providers

- **Regulations often project requirements on service providers**
  - PCI states that it must be complied with by any organization that processes, transmits or stores payment card data
  - HIPAA holds “Covered Entities” accountable for their service providers’ behavior
  - GLB requires due diligence in sharing private financial data
- **You need to know how a particular relationship affects your compliance**
- **If you are a service provider, you need to know what requirements you must meet**

Ensuring Compliance

- Ensuring compliance requires a process
- Standards like ISO 27002 and COBIT describe lifecycle processes that can be applied to service providers



Monitor

Measure risk

Identify controls

Evaluate

Recognizing Requirements

- **The first step in understanding risk is understanding the information shared**
  - What does the service provider require?
  - What does the business propose to share?
- **Map to compliance requirements**
  - Assemble a mapping of data to regulatory requirements
  - Identify specific data elements
  - Understand thresholds of sensitivity
- **Standards call for tools to aid in this exercise**
  - Information catalog
  - Information classification and handling policies

Measure Inherent Risk

- **Conduct a preliminary risk assessment**
  - What are the business risks?
  - What are the initial technical risks?
- **Eliminate unnecessary information**
  - The most effective way to mitigate risk is to avoid sharing the information
  - Mask information
  - Anonymize information
- **Rank the service risk after removal of any unnecessary information**
- **Let the level of risk determine your next steps**

Evaluate Service Provider Practice

- **Regulations require due diligence in assessing provider controls**
  - FFIEC
  - PCI
  - GLB
- **Depth of inspection should correspond to risk**
  - Contractual language may be good enough for low risk partners
  - Questionnaires/self assessments may suffice for medium risk
  - Interviews, on-site inspections, third party audits may be necessary for high risk partners
- **Establish a set of rules to guide evaluations**
- **View the evaluation as a partnership**
  - Work to establish necessary controls rather than finding fault
  - Lay the groundwork for periodic reviews and communications

Regulatory Oddities

- **PCI requires all organizations that handle payment card data to comply**
  - There may be no direct business relationship with a bank to enforce compliance
- **HIPAA covered entities must manage providers entrusted with data as if they were extensions of the organization**
  - Service providers appear to have no place in the regulation
  - Service providers often have more data than covered entities
- **There continue to be grey areas in determining who needs to comply and even what “compliance” means**

Standards-based Assessments

- When in-depth assessments are necessary, it helps to have a defined framework
- ISO27002/17799 is a useful standard for evaluating practices
- Superset of most regulatory requirements
  - Laundry list of practices
  - Some applicable, some not
- May be an end unto itself
  - Service providers are increasingly using it as a benchmark
- Provides a logical and objective framework for evaluation (not completely arbitrary)
- Allows (some) comparison of practice from organization to organization and assessment to assessment

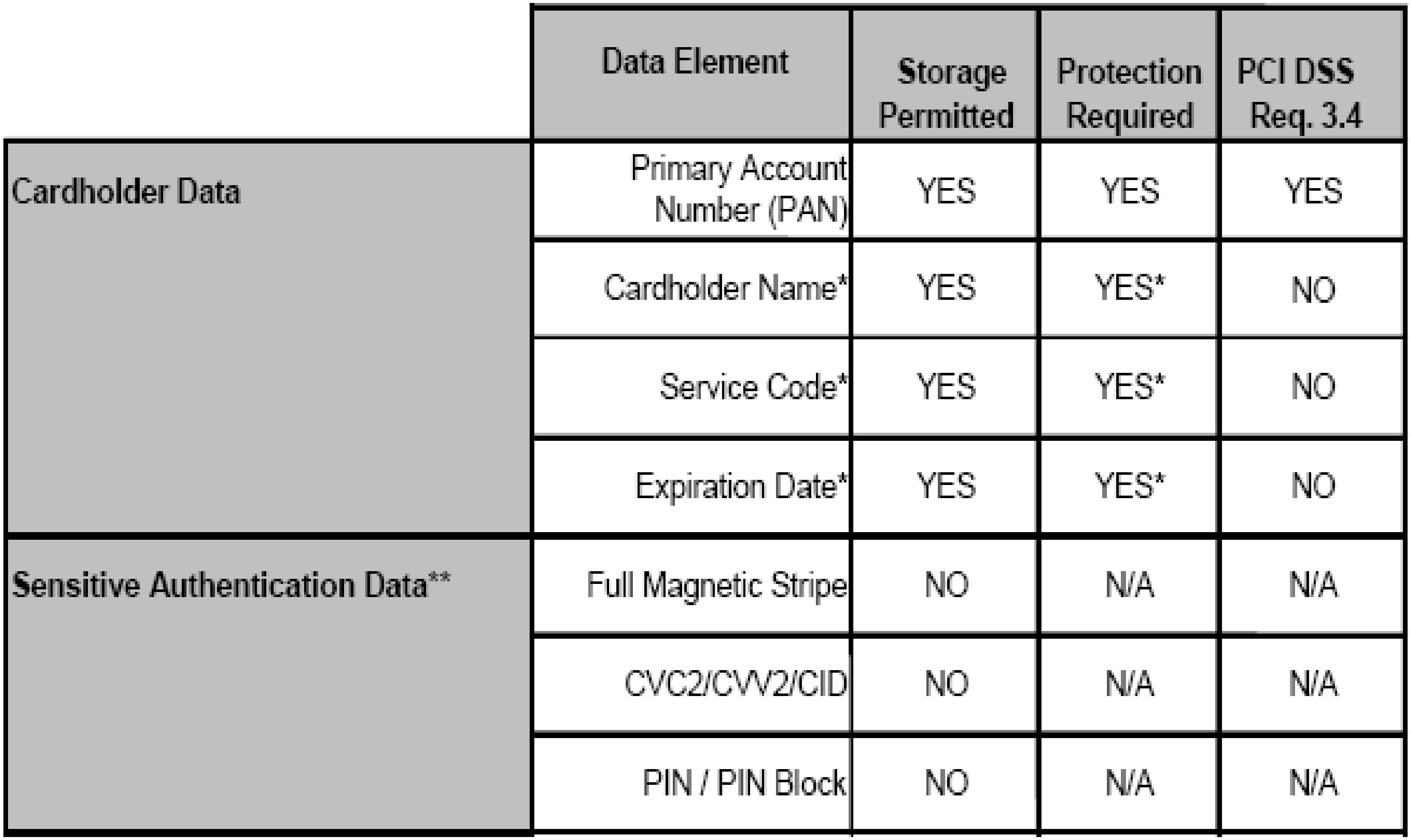
Regulatory Specifics

- While standards and most regulations are consistent in the types of controls they require, each regulation requires specific controls
- Standards based reviews are good, but not complete
- You must supplement the standard control requirements with those from the specific regulation
- Here are some specifics from PCI and FFIEC

Example FFIEC Controls

- FFIEC Security Handbook requires effective access rights management for financial organizations and their service providers
  - **Request and approval workflow (no technology reference)**
  - **Rights/privileges assigned by business need**
  - **Timely updates in response to personnel and system changes**
  - **Periodic review (frequency based on risk)**
- **The Handbook also requires policy, training, and user acceptance of an acceptable use policy**
- **The Handbook also recommends mechanisms for assessment of service providers**
  - SAS70
  - WebTrust
  - SysTrust

PCI Data 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

PCI Service Providers

- Fortunately for service consumers, Brand compliance programs require “service providers” to validate their compliance with on-site assessments
- Unfortunately, many organizations do not fit the “service provider” definition
- Many service providers handle payment card data without being part of the transaction
- Compliance levels either don’t apply or every “service provider” needs to be treated as a Level 1
- This should reduce the evaluation to an inspection of a Report on Compliance

Monitoring relationships

- **Service provider management requires monitoring and periodic re-evaluation**
- **Many organizations run set-and-forget service provider “programs”**
- **Problems with this approach:**
  - Companies change (yours and theirs)
  - Threats change
  - Technologies change
  - Regulatory requirements change
- **A good program requires revisiting the relationship at least annually**
- **Each year reassess the risk and the effectiveness of the controls**

Incident Response & BCM

- **Appropriate response to incidents and business interruptions requires planning**
  - Communications
  - Responsibilities
  - Roles
  - Logistics
  - Expectations
- **Evaluate the service provider's capabilities**
- **Define the roles and responsibilities**
- **Practice (together)**

Technology

- **Technology is a critical part of service provider relationships**
  - Firewalls to define connections
  - VPNs for communication across untrusted networks
  - Intrusion detection to detect problems on the connection
  - Data Loss Prevention to monitor content
  - Encryption to protect against disclosure
- **Unfortunately, there is no silver bullet**

Summary

- Service providers are viewed as an extension of your organization by regulations
- You need to understand the information you share and compliance requirements for that information
- The most effective risk mitigation is elimination of data
- Establish a program to assess and manage your service providers according to risk
- Ensure that you review the effectiveness of your controls periodically