Compliance and Outsourcing

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 in the financial industry**
- **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

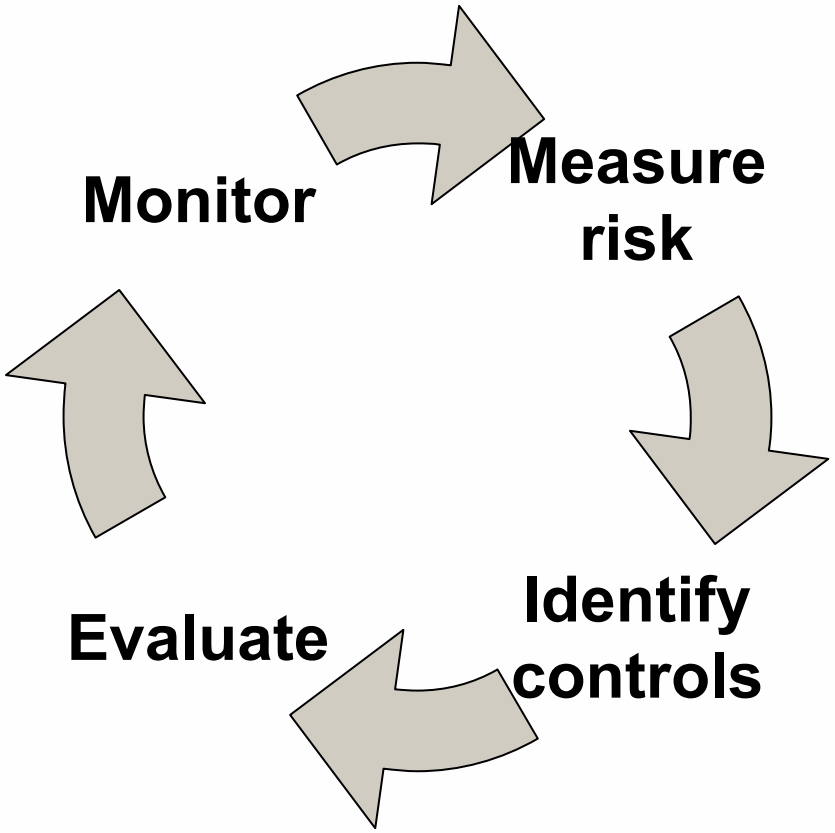
Information	Regulation
PII	Privacy
Payment card	PCI
Personal Financial	GLB
Health	HIPAA
Corporate Financials	SOX

Regulations and Service Providers

- **Typically, regulations 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 you 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



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**
  - Is the benefit of the service worth the risk of exposure?
  - 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 control rather than finding fault
  - Lay the groundwork for periodic reviews and communications

Compliance of Service Providers

- **A common practice is to project the same requirements to providers as the institution itself must meet**
- **PCI requires all organizations that handle payment card data to comply**
  - There may be no direct business relationship to enforce it
- **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
- **FFIEC provides guidelines for managing service providers – cites SAS70, WebTrust, and SysTrust as useful methods for measuring and ensuring quality**

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 assess the adequacy of specific controls required by the contract or regulation**

Example FFIEC Controls

- **FFIEC Security Handbook requires effective access rights management**
  - **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)**
- **Policies, training, and user acceptance of Acceptable Use Policy**
- **FFIEC requires "appropriate" authentication**
  - **Passwords or multi-factor authentication based on risk and specific regulatory requirements**
  - **"Multi-factor" may be necessary**
- **FFIEC provides guidelines for managing service providers – cites SAS70, WebTrust, and SysTrust as useful methods for measuring and ensuring quality**

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

Example PCI Requirements

- **3 of 12 PCI DSS requirements address access control**
  - Implement Strong Access Control Measures
  - **7: Restrict access to cardholder data by business need-to-know**
  - **8: Assign a unique ID to each person with computer access**
  - **9: Restrict physical access to cardholder data**
- **Fortunately for service consumers, Brand compliance programs require "service providers" to validate their compliance with on-site assessments**
- **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 & Business Continuity

- **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**

Technology

- **Technology is a critical part of service provider relationships**
  - Firewalls to define connections
  - VPNs for communication across untrusted networks
  - Intrusion detection
  - Data Loss Prevention
  - Encryption
  - Scanners
- **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