Managing Third Party Risk

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

Agenda

- Roles of service providers
- Operational versus compliance risk
- Risk analysis
- Reviewing service provider practices
- Using third party reviews
- Conducting reviews
- Getting help
- Monitoring relationships
- Technology

Service Providers & Partners

- Service partners are a fact of life
- These partners are particularly important when they process information that is covered by regulations and contracts
  - Payment card data
  - Health information
  - Private financial information
  - Sensitive personal information (e.g., employee data)
- These relationships bring with them operational as well as regulatory risk

Regulatory vs. Operational Risk

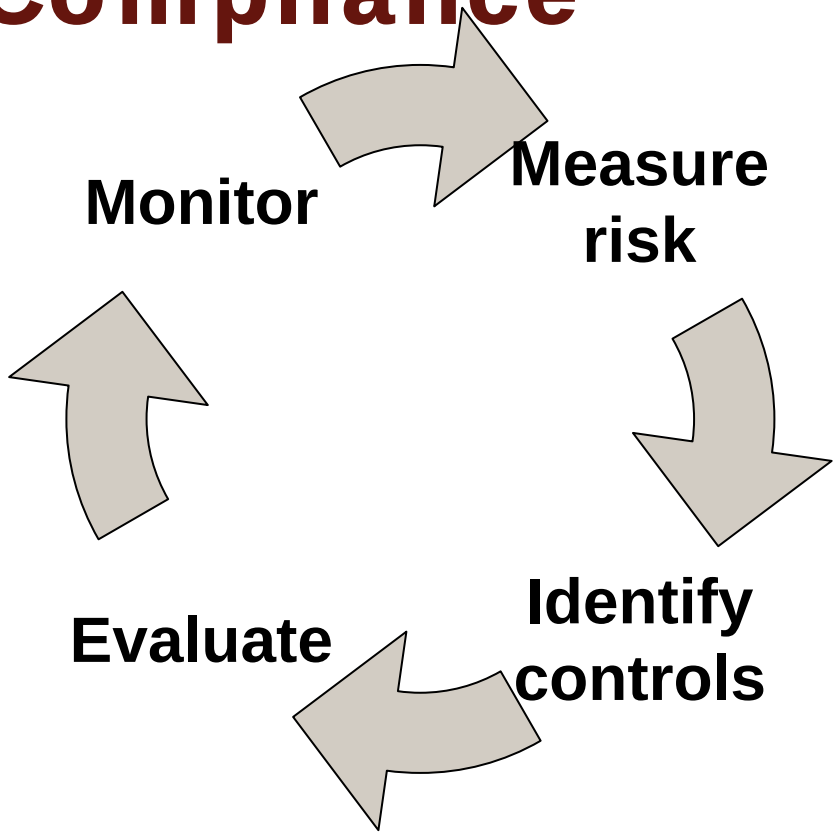
- Operational risk – compromise and damage
  - Availability
  - Confidentiality
  - Integrity
  - Reputation
- Regulatory risk
  - Even without a compromise, service providers can affect your compliance
  - Policies, procedures, and practices
  - Your service providers may not be directly responsible for compliance
  - It's often your job to enforce compliance
  - The result: fines, suspension of privileges, higher audit costs, more scrutiny

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
- If the service provider handles the regulated information, it must comply

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

- Most regulations require you to be the regulator
  - Require you to establish contracts that require compliance
  - Hold you accountable for breaches or deficiencies
- PCI requires you to ensure that your service providers are PCI compliant in the specific services they provide
- HIPAA requires you to ensure that *business associates* adhere to the security rule
- GLB requires financial organizations to exercise due diligence
- FFIEC provides guidelines for measuring service provider practice
  - SAS 70
  - WebTrust
  - SysTrust
- FDIC requires specification of practice or proof of audit for service providers

Assessment Framework

- When in-depth assessments are necessary, it helps to have a defined framework
- ISO27002 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

Looking Beyond Standards

- Standards-based assessments/audits are excellent tools
- Consumers of these reports need to understand the details of the assessment and what the results mean
- Questions to ask:
  - What was the scope of the assessment?
  - What metrics were used to determine acceptable practice?
  - What control objectives were used for the audit?
  - Were specific regulatory requirements specified as objectives?
  - Can I see the report?
  - Can I speak with the auditor?
- Service providers: anticipate these questions

Conducting Your Own Assessments

- Assessments need to concentrate on the risks of the service provided
  - What service is the partner providing?
  - What are your risks as a consumer?
  - How does the service relate to others provided?
  - Is your risk the same as the provider's other customers?
- Avoid generic assessments and questionnaires
- Focus on operational security
  - Policies are good, strong operational security is better
- Look for an understanding of sound security practice
  - Security reviews
  - Security testing
- Look for consistency and discipline in administration

Get Help

- Security auditors/assessors can improve the effectiveness of your assessments
  - More exposure to common industry practice
  - Better understanding of regulatory interpretation
  - Better methodology
  - More objectivity
- Third party assessors can help with bad news
  - Management is more accepting of critique from outsiders
  - Avoid political battles between departments (e.g., Information security versus Human Resources)
- Third parties don’t spoil the relationship
  - Internal groups don’t make enemies of the partner

Understand Associate Compliance

- Understand regulatory requirements for your business partners
- Regulations often have specific requirements for specific roles
  - PCI Service Providers
  - HIPAA business associates
  - PCI Hosting Providers
- Determine whether your partner understands the role
- Gather compliance information
  - Existing assessment results
  - Compliance state
  - Assessment dates
  - Auditor identity
  - Is the provider on “the list?”

Special Treatment: Incidents & BCP

- 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

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

Technology

- Technology is a critical part of service provider relationships
  - Firewalls to define connections
  - VPNs for communication across untrusted networks
  - Intrusion detection – trust but verify
  - 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
- Establish a program to assess and manage your service providers according to risk
- Share only the data required
- Review your requirements, risk, and service providers regularly