# ISACA – San Francisco
# Fall Conference 2007

## Vendor Security Risk Management

**Dan Morrison**

**September 17, 2007**

PRICEWATERHOUSECOOPERS

## Topics of Discussion

- Context-Information, operations & organization challenges
- Vendor Security Risk within a System Lifecycle
- Changing Regulatory Expectations
- Example - FFIEC Vendor Management Requirements
- Vendor Related Risks - Information Security
- Key Elements of Vendor Relationship Maturity Model
- Managing Vendor Information Security Risks
- Sample Best Practices for Vendor Security Risk Management
- Final Thoughts – Do's / Don'ts / Remembers

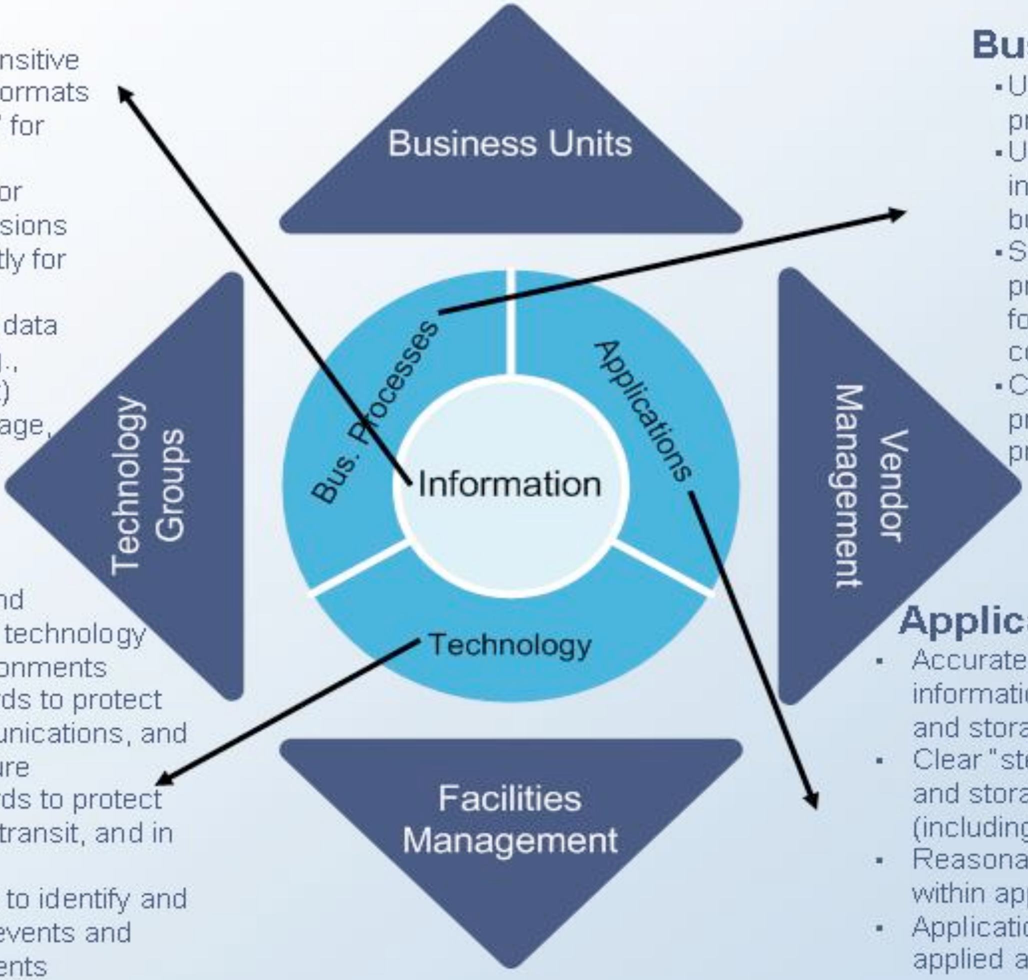
# Context: Information & operational challenges

## Information

- Inventory of all sensitive information in all formats
- Clear "ownership" for information sets
- Information "risk" or classification decisions applied consistently for all data
- Ability to produce data when needed (e.g., discovery request)
- Data quality, heritage, and duplication is managed

## Technology

- Known inventory and "stewardship" of all technology infrastructure environments
- Technical safeguards to protect processing, communications, and storage infrastructure
- Technical safeguards to protect data in storage, in transit, and in archives
- Monitoring controls to identify and manage technical events and data movement events



## Business Processes

- Understanding the business processes & sub-processes
- Understanding of the flow of information through a business process
- Secure information handling practices are known and followed (including hard copies, faxes, etc)
- Customers are notified of privacy practices and preferences are managed

## Applications

- Accurate inventory of all sensitive information collection, processing, and storage locations
- Clear "stewardship" for processing and storage environments (including data)
- Reasonable protective safeguards within applications
- Application safeguards consistently applied across applications

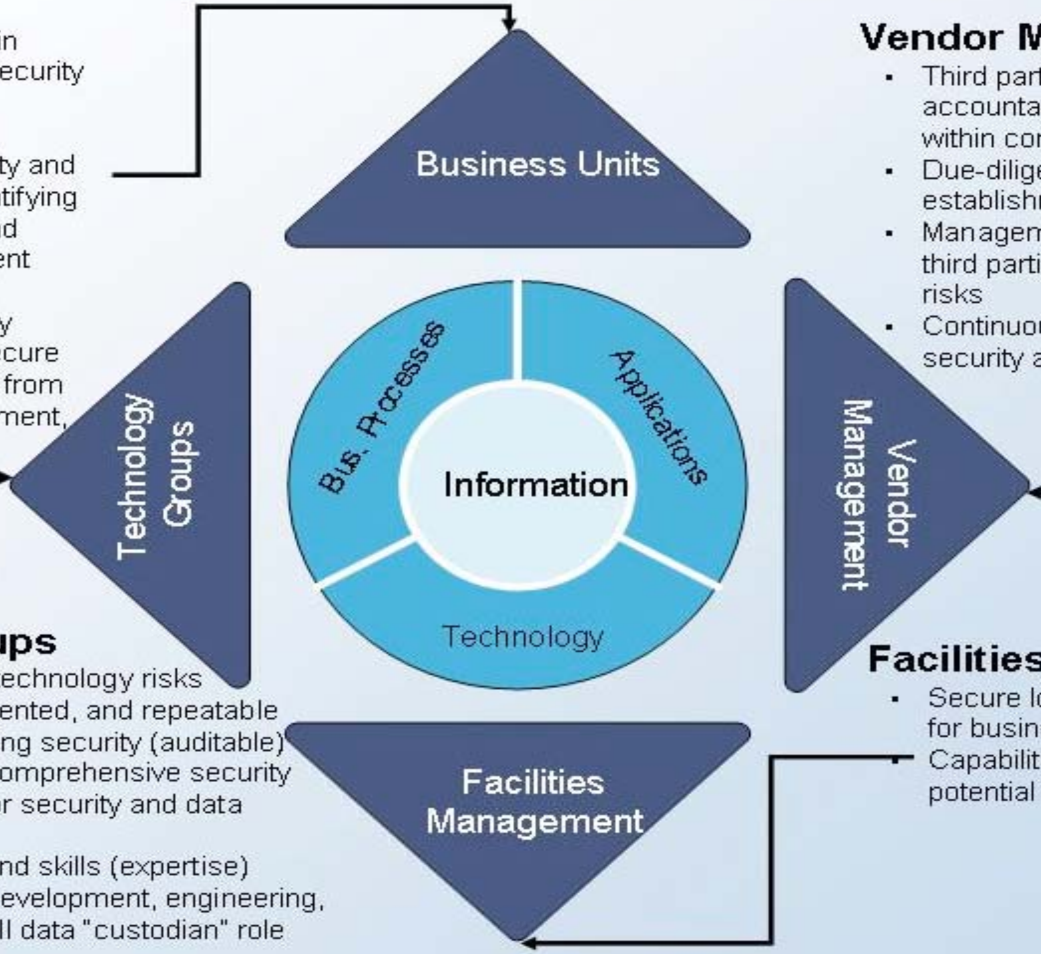
# Context: Organizational challenges

### Business Units

- Management involved in establishing practical security and privacy policies
- Business operates in compliance with security and privacy policies by identifying risks, "owning" risks and making risk management decisions
- Culture of accountability (data ownership) for secure handling of information from executives, to management, and down to process executors

### Technology Groups

- Identify and manage technology risks
- Standardized, documented, and repeatable processes for managing security (auditable)
- Design and operate comprehensive security solutions (a toolkit) for security and data privacy
- Security knowledge and skills (expertise) across architecture, development, engineering, and operations to fulfill data "custodian" role



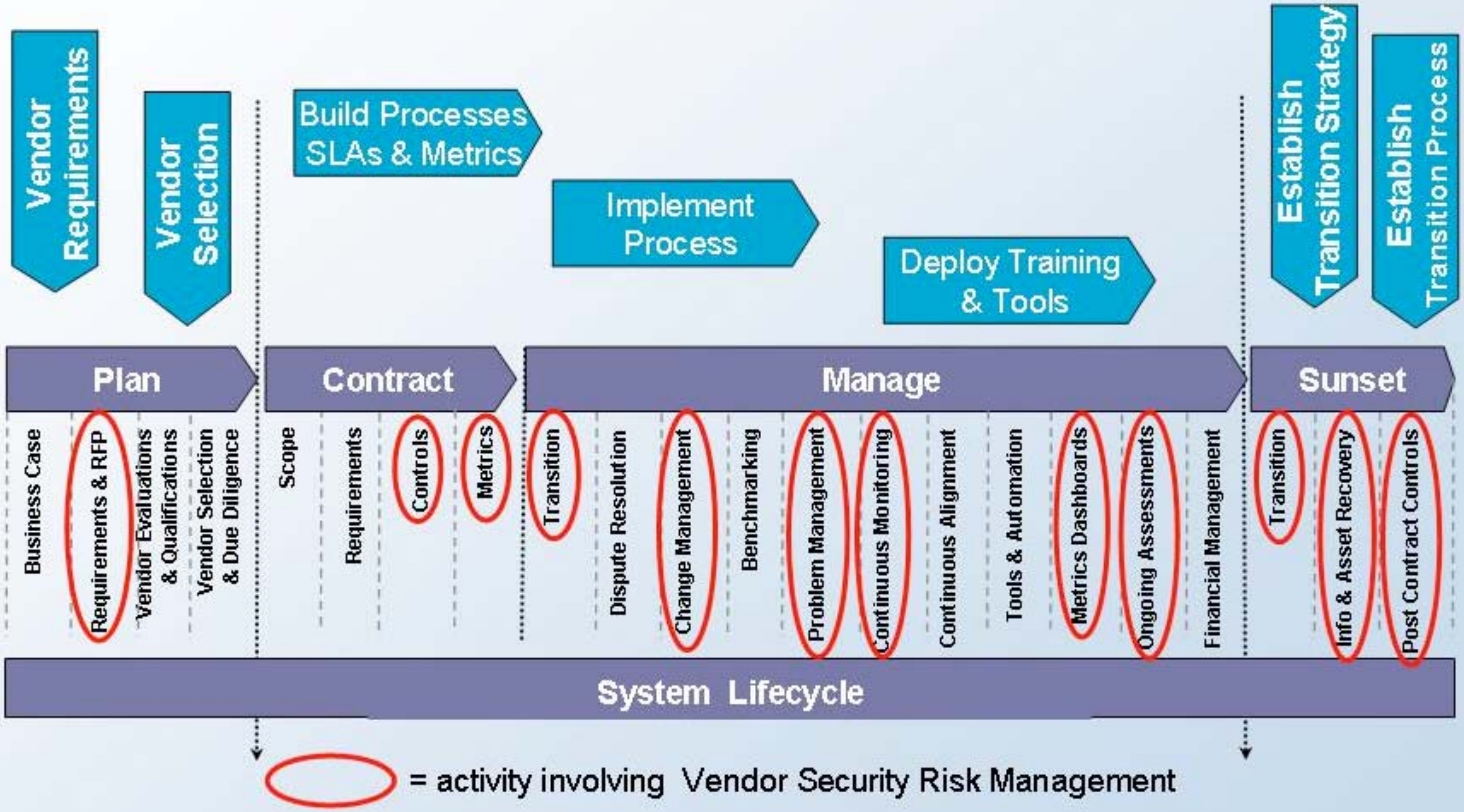
### Vendor Management

- Third parties are held accountable by reasonable terms within contracts
- Due-diligence performed prior to establishment of contract or SLA
- Management discipline to ensure third parties mitigate identified risks
- Continuous monitoring of vendor security and privacy

### Facilities Management

- Secure location and environment for business and data processing
- Capabilities to investigate potential security incidents

## Vendor Security Risk within a System Lifecycle



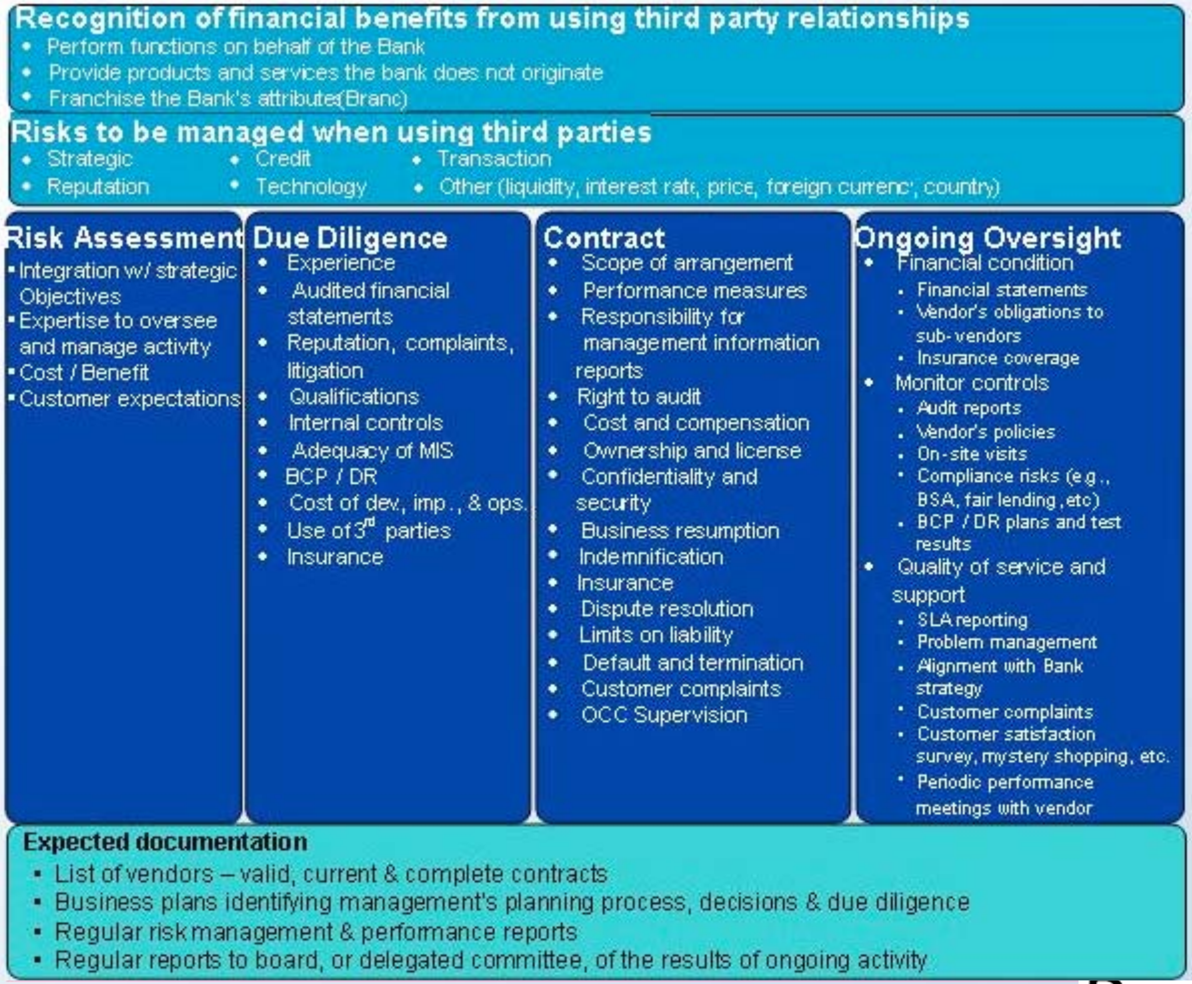
# Changing Regulatory Expectations

| Then | Now |
|---|---|
| **GLBA** | **GLBA** |
| – Risk assessment completed | – Risk assessment capability |
| – Core processing system | – All data, all forms, all locations |
| – Contracts with third parties | – Oversight of vendors |
| **FFIEC** | **FFIEC** |
| – Annual risk assessment | – Enterprise risk assessment |
| – Technology centric | – Information focus with increasing technology focus |
| – Vendors assessed separately | – Vendors extension of enterprise |
| | – Ability to demonstrate & communicate Risk Management |

ISACA®
Serving IT Governance Professionals

**FFIEC Example**

# Federal Financial Institutions Examination Council Vendor Management Requirements



**Recognition of financial benefits from using third party relationships**

- Perform functions on behalf of the Bank
- Provide products and services the bank does not originate
- Franchise the Bank's attribute(Branc)

**Risks to be managed when using third parties**

- Strategic
- Credit
- Transaction
- Reputation
- Technology
- Other (liquidity, interest rat, price, foreign currenc', country)

**Risk Assessment**

- Integration w/ strategic Objectives
- Expertise to oversee and manage activity
- Cost / Benefit
- Customer expectations

**Due Diligence**

- Experience
- Audited financial statements
- Reputation, complaints, litigation
- Qualifications
- Internal controls
- Adequacy of MIS
- BCP / DR
- Cost of dev., imp., & ops.
- Use of 3rd parties
- Insurance

**Contract**

- Scope of arrangement
- Performance measures
- Responsibility for management information reports
- Right to audit
- Cost and compensation
- Ownership and license
- Confidentiality and security
- Business resumption
- Indemnification
- Insurance
- Dispute resolution
- Limits on liability
- Default and termination
- Customer complaints
- OCC Supervision

**Ongoing Oversight**

- Financial condition
  - Financial statements
  - Vendor's obligations to sub-vendors
  - Insurance coverage
- Monitor controls
  - Audit reports
  - Vendor's policies
  - On-site visits
  - Compliance risks (e.g., BSA, fair lending, etc)
  - BCP / DR plans and test results
- Quality of service and support
  - SLA reporting
  - Problem management
  - Alignment with Bank strategy
  - Customer complaints
  - Customer satisfaction survey, mystery shopping, etc.
  - Periodic performance meetings with vendor

**Expected documentation**

- List of vendors – valid, current & complete contracts
- Business plans identifying management's planning process, decisions & due diligence
- Regular risk management & performance reports
- Regular reports to board, or delegated committee, of the results of ongoing activity

## Special Interest Vendors

- Tech Services Providers
- ITO Services
- Retail Payment Systems Providers
- Wholesale Payment Systems Providers
- eBanking
- FedLine
- Development & Acquisition
- Business Continuity Planning
- Internal Audit

## Special Interest Risks

- Information Security
- Transaction Risks

# Vendor Related Risks - Information Security

| *Key Focus Areas* | *Your Current Maturity Level* | *Your Future State Level* |
|---|---|---|
| 1. Vendor Access to Data/Technology | ? | TBD |
| 2. Vendor Identity Management/Provisioning | TBD | ? |
| 3. Governance:- Contract Compliance (Metrics) | TBD | ? |
| 4. Vendor Compliance to Sub-Contracting | ? | TBD |
| 5. Business Continuity/DR Planning | ? | TBD |
| 6. Privacy: (GLBA, HIPAA, CA1386) | ? | TBD |
| 7. Industry Regulations: (Federal, OCC etc.) | ? | TBD |

**Business Impact**

**Cost, Quality, Service, Reputation & Risk**

# Key Elements of Vendor Relationship Maturity Model

1. Management Structures
2. Vendor Rationalization
3. Vendor Selection
4. Vendor Relationships
5. Manage Costs
6. Manage Performance & Quality
7. Use of Technology
8. Manage Information Security Risk

# MANAGING VENDOR INFORMATION SECURITY RISKS

## Within a Vendor Relationship Maturity Model

**EXAMPLE ONLY**

| Initial<br>1 | Repeatable<br>2 | Defined<br>3 | Managed<br>4 | Optimizing<br>5 |
|---|---|---|---|---|
| ▪ Information Security risks associated with supplier selection are not formally assessed or understood.<br>▪ Vendor data is scattered across the organization.<br>▪ Organization data, information and privacy policies and concerns not understood by suppliers.<br>▪ No (or poor) metrics and/or SLAs associated with risk management, information security, privacy, etc.<br>▪ Regulatory and/or other compliance requirements are not well understood between organization and supplier.<br>▪ Organization generally unaware of supplier use of 3rd party providers.<br>▪ Business contingency planning/recovery or disaster recovery plans not in place or tested on a regular basis | ▪ Procurement/sourcing organization is asked to manage business risks, which may not be fully understood, in sourcing however processes, policies and practices are not standardized or measured.<br>▪ Organization security/risk management function is not formally involved.<br>▪ Business risks of suppliers informally considered in supplier selection, selective background checks required.<br>▪ Electronic interfaces with vendors have been secured through simple authentication and the nature of the security measures disclosed.<br>▪ Organization data, information and privacy policies have been communicated to suppliers.<br>▪ Contracts require compliance with key regulatory or other compliance requirements of the supplier, however contract performance , metrics, and/or SLAs are not in place.<br>▪ Vendor use of 3rd party suppliers is discouraged and not monitored.<br>▪ Business disaster recovery plans developed between a few key suppliers and organization and may or may not be tested on a regular basis | ▪ The Organization has established a cross functional team involving corporate security/risk management as a member of the sourcing team.<br>▪ Standard information security and risk management policies, practices and processes are developed for the procurement/sourcing org.<br>▪ Vendor relationship managers are trained on key business risk and information security practices/policies.<br>▪ Potential suppliers are formally assessed for business risk in selection process, background checks & other security testing required<br>▪ Data/information access by 3rd party suppliers is controlled through passwords, firewalls and other screening methods.<br>▪ Regulatory and other compliance requirements are documented and measured/SLAs in the contracts.<br>▪ Vendor use of 3rd party suppliers is restricted and requires approval.<br>▪ Business contingency/recovery and disaster recovery plans developed between all key suppliers and organization and SLAs in contract.<br>▪ Monitoring of suppliers and third parties follow a formal process that is reviewed and monitored for effectiveness | ▪ Organization assesses the sourcing team's compliance to business risk & information security requirements.<br>▪ Vendors perform scheduled (or ad-hoc when there is cause) self assessment of business risk, info security and regulatory compliance.<br>▪ Potential vendors must pre-qualify themselves regarding business and info security risk prior to consideration.<br>▪ Incidents of breaches of business risk &/or information security are measured and reported per an established schedule.<br>▪ Regulatory and other compliance requirements are monitored, measured and reported per an established schedule.<br>▪ Vendor use of 3rd party suppliers is controlled, monitored and reported to insure cost, quality, risk management and appropriate flow downs occur.<br>▪ Business contingency, recovery & disaster recovery plans tested and updated based on business conditions & established schedules.<br>▪ Vendor Contracts reviewed for currency related to business risk, information security, regulatory & other compliance requirements by local, state, federal or other entities. | ▪ The organization has automated processes to collect and process cross functional team and suppliers input to business risk and information security processes to improve processes, tools and technologies to enable optimized performance.<br>▪ Vendor and prospective vendor compliance assessments are automated.<br>▪ Data access and information security threats are tested and actual incidents are reported and continuously analyzed for trending/breach anticipation.<br>▪ Vendor use of alternative sources of supply is considered a strategic sourcing alternative, monitored, measured and potentially mutually funded/invested.<br>▪ The assessments of Vendor contracts is automated and assessments against performance goals and SLAs are done in real-time.<br>▪ Vendor Relationship processes are assessed in real-time using automated assessment tools and metrics collected in terms, costs, quality, risk management, flexibility & other SLA performance measures. |

# Sample Best Practices for Vendor Security Risk Management

## People

- Line of Business responsibility for vendor risk

- Qualified and trained VRMs
- Support from centralized team

## Process

- Standard repeatable processes for requirements gathering, risk assessment, controls validation, contracting, service level management, etc.

- Quality measures for process
- Alternative validation methods
- Define Key Process

## Technology

security risk

- Repository to support Vendor Security Management
- Tools that provide KPI data

- Vendor security risk, assessment, monitoring and reporting tools

# Final Thoughts – Do's

- Know where your data is and who has access to it
- Work with stakeholders within your organization to understand what security risks are important and how they apply to your vendor community
- Collect as much supporting information as possible – specific to your organization and your vendors
- Leverage existing vendor information ***if*** it is applicable
- Make sure the vendor information is *Accurate*

# Final Thoughts – Don'ts

- Ignore vendor security risk management
- Outsource the issue, thinking it will go away
- Cut corners – be smart by leveraging information, tools and processes, however, BE DILIGENT
- "Over-survey" stakeholders
- Believe everything you're told – look for alternative validation methods

# Final Thoughts – Remember

- Outsourcing does not remove your Risk Management responsibilities
- Be able to defend your risk decisions with hard data through repeatable processes and standard tools
- Keep your information accurate and current, and your processes tuned
- Think ahead – start collecting information now

# Contact Information

Dan Morrison
(415) 498-7066
daniel.morrison@us.pwc.com