

[www.pwc.com](http://www.pwc.com)

# *Risk Management & Data Security in an Outsourced World*

**January 11, 2011**

**pwc**

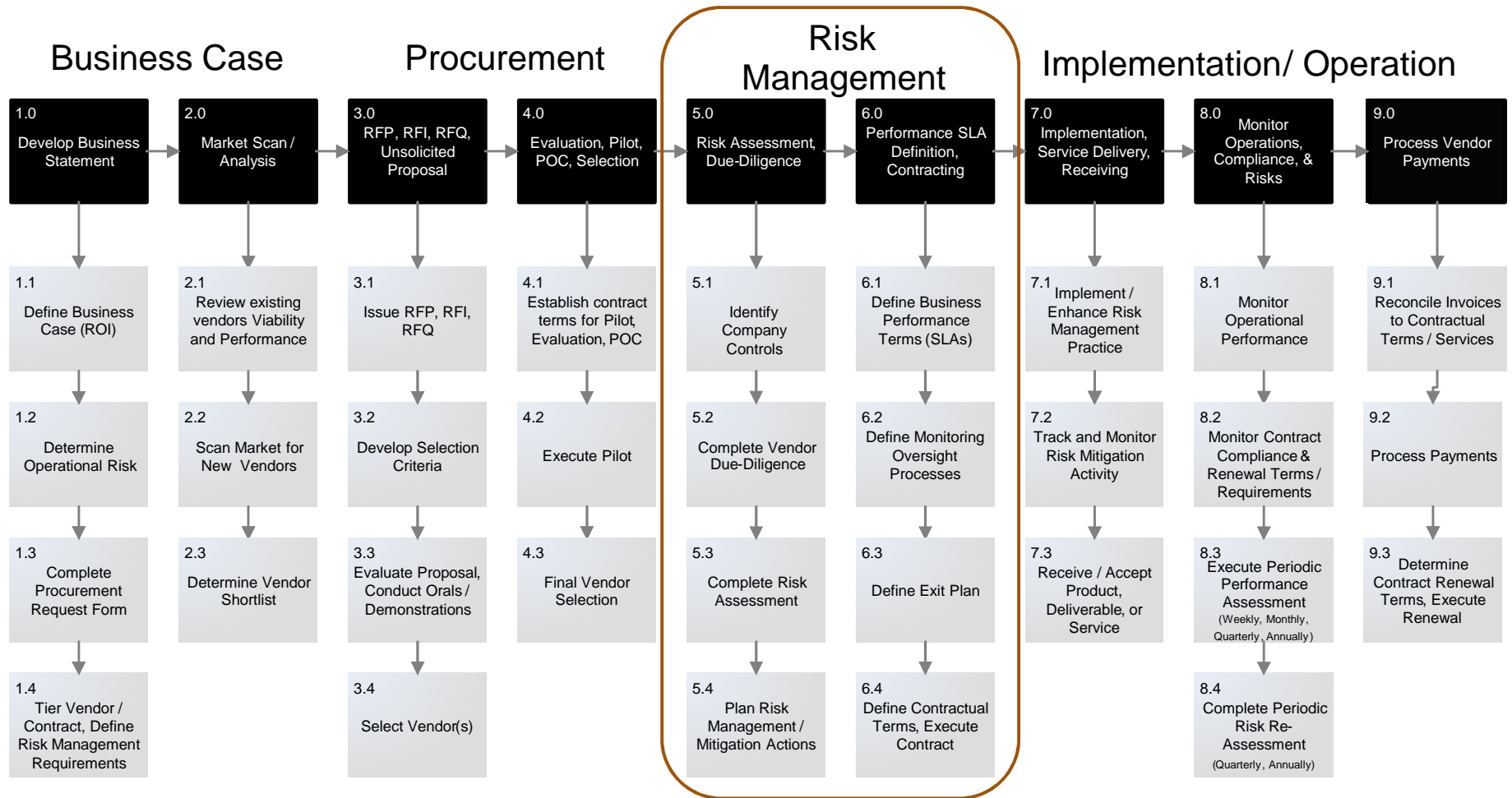
---

## ***Table of Contents***

Background and Context.....	3
Common Risk Management Frameworks.....	6
Leading Practices and Guidance.....	7
Key Stakeholders & Categories.....	8
A ‘Good Practices’ Approach.....	9
Sample Vendor Risk Management Program Structure .....	10
Vendor Risk Assessment Approach.....	11
Examples - Network Considerations / User-Access Considerations .....	13
Vendor Simplification.....	15
Risk Management for Larger Sourcing Vendors .....	17

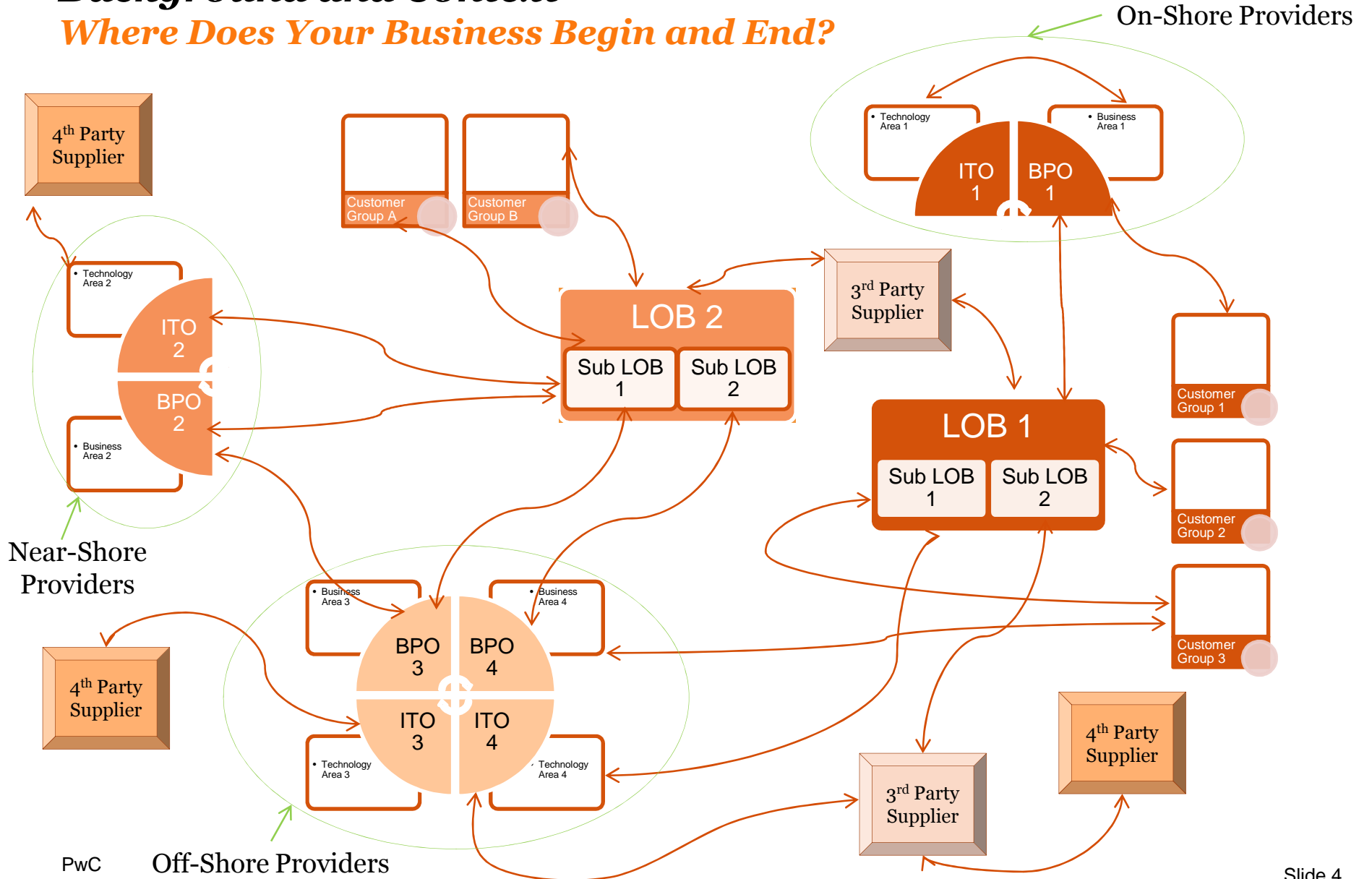
# Background and Context

## Overview of Vendor Management Functions



# Background and Context

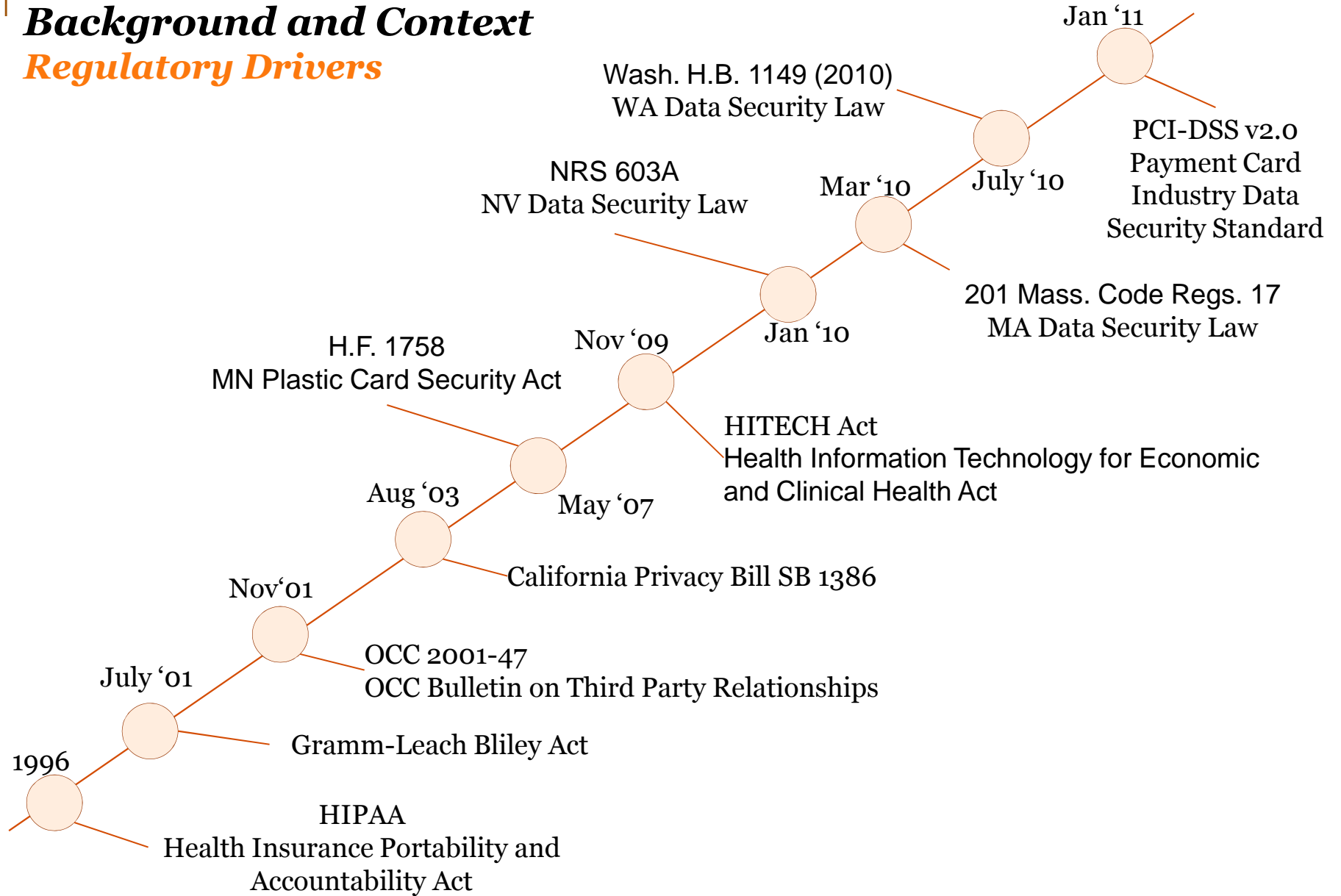
## Where Does Your Business Begin and End?



PwC

# Background and Context

## Regulatory Drivers



# Common Risk Management Frameworks

PCI-DSS

1. Use firewalls	7. Need-to-know access
2. No default passwords	8. Unique IDs
3. Protect stored data	9. Physical access controls
4. Encrypt data in transit	10. Track & Monitor access
5. Use current anti-virus	11. Test systems and processes regularly
6. Secure systems & apps	12. Information Security Policy

Privacy

1. Accountability	6. Accuracy
2. Identifying Purpose	7. Safeguards
3. Consent	8. Openness
4. Limiting Collection	9. Individual Access
5. Limiting use, disclosure & retention	10. Challenging Compliance

ISO 27001

1. BCP	7. Personnel
2. System Access Control	8. Security Organization
3. System Dev & Maintenance	9. Computer & Network Management
4. Physical & Environmental	10. Asset Classification & Control
5. Compliance	11. Security Policy
6. Incident Management	

ITIL

Service Delivery: (Management) Service Level, Capacity, Availability, Continuity, Financial Mgt of Services, Security
Business Perspective: Business Continuity, Partnership, Outsourcing, Surviving Change, Transformation, Security
Managing Applications: Lifecycle Support, Testing of IT Services, Security Management
Service Support: Run Service Desk, (Management) Incident, Problem, Change, Configuration, Release, Security
Infrastructure Management: Installation & Acceptance, (Management) Network, Operations, Systems, Security

COSO

Control Activities
Risk Assessment
Control Environment
Information & Communications
Monitoring

COBIT

Planning and Organization
Acquisition & Implementation
Delivery and Support
Monitoring

# Leading Practices and Guidance

## Focus on third parties that:

- Perform functions on behalf of the firm
- Provide products and services that the firm does not originate
- Franchise the firm's attributes (Brand)

## Risks to be managed when using third parties

- Strategic
- Reputation
- Transaction
- Credit
- Compliance
- Other (liquidity, interest rate, price, foreign currency, country)
- Technology
- Security
- Privacy
- Operations

### Due Diligence

- Experience
- Audited financial statements
- Reputation, complaints, litigation
- Qualifications
- Internal controls
- Adequacy of MIS
- BCP/DR
- Cost of development, implementation and support
- Use of third parties
- Insurance

### Risk Assessment

- Integration with strategic objectives
- Expertise to oversee and manage activity
- Cost/Benefit
- Customer expectations

### 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

### Ongoing Oversight

- Financial condition
  - Financial statements
  - Supplier's obligations to sub-Suppliers
  - Insurance coverage
- Monitor controls
  - Audit reports
  - Supplier policies
  - On-site visits
  - Compliance risks
  - BC/DR plans and test results
- Quality of service and support
  - SLA reporting
  - Problem management
  - Alignment with organization's strategy
  - Customer complaints
  - Customer satisfaction survey
  - Periodic performance meetings with Supplier

## Expected documentation

- List of suppliers - valid, current and complete contracts
- Business plans identifying management's planning process, decisions and due diligence
- Evidence the firm evaluated supplier's controls and monitors supplier's performance
- Regular reports to board, or delegated committee, of the results of ongoing oversight activity

Additional financial services regulatory guidance is available separately for the following:

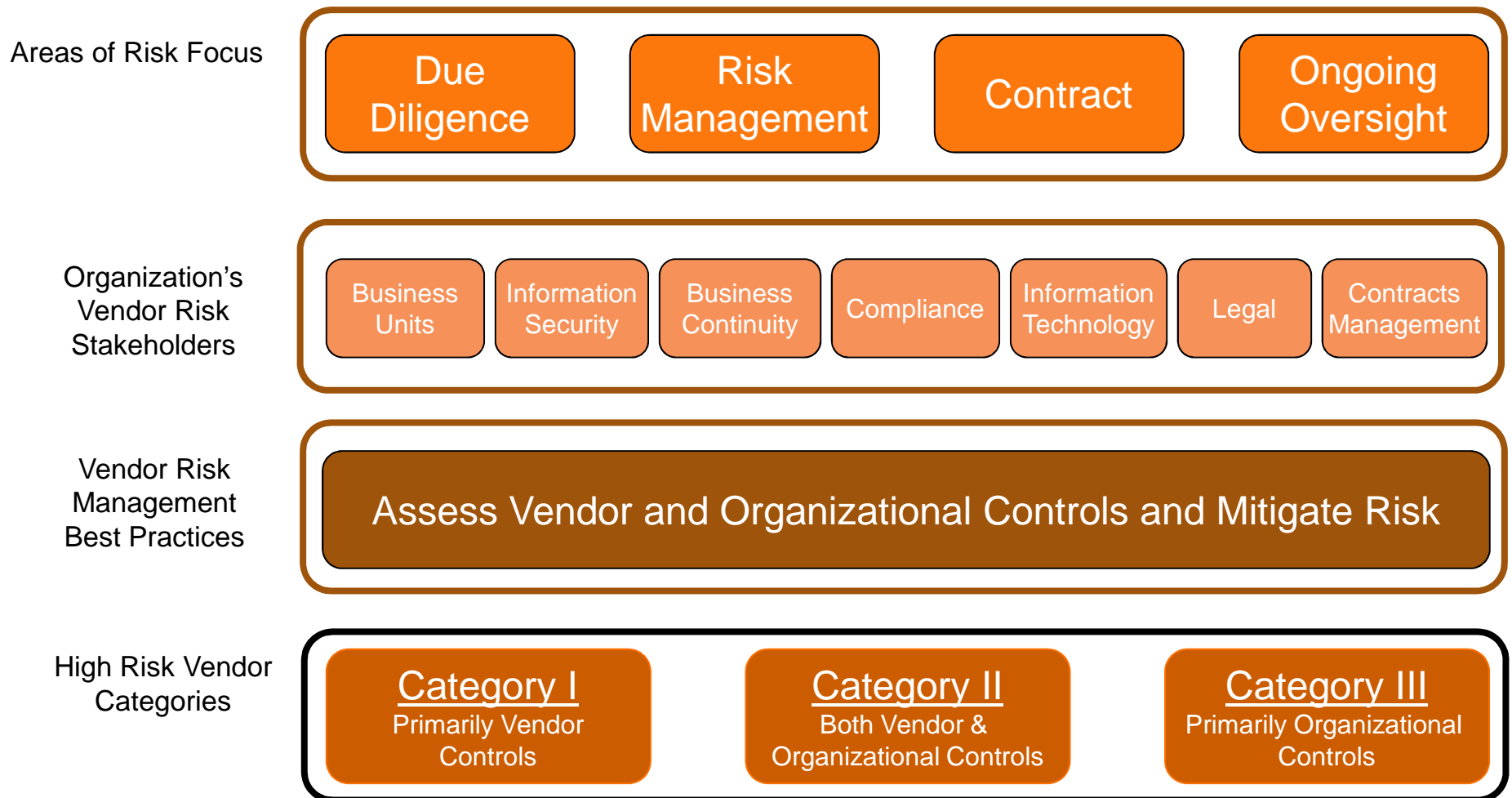
### • Vendors

- Technology Service Providers
- IT Outsourcing Services
- Retail Payment Systems Providers
- Wholesale Payment Systems Providers
- eBanking
- FedLine
- Development & Acquisition
- Business Continuity Planning
- Internal Audit

### • Special Risks

- Information Security
- Transaction Risks
- Offshore Vendors
- Third Party Lending

## Key Stakeholders and Categories

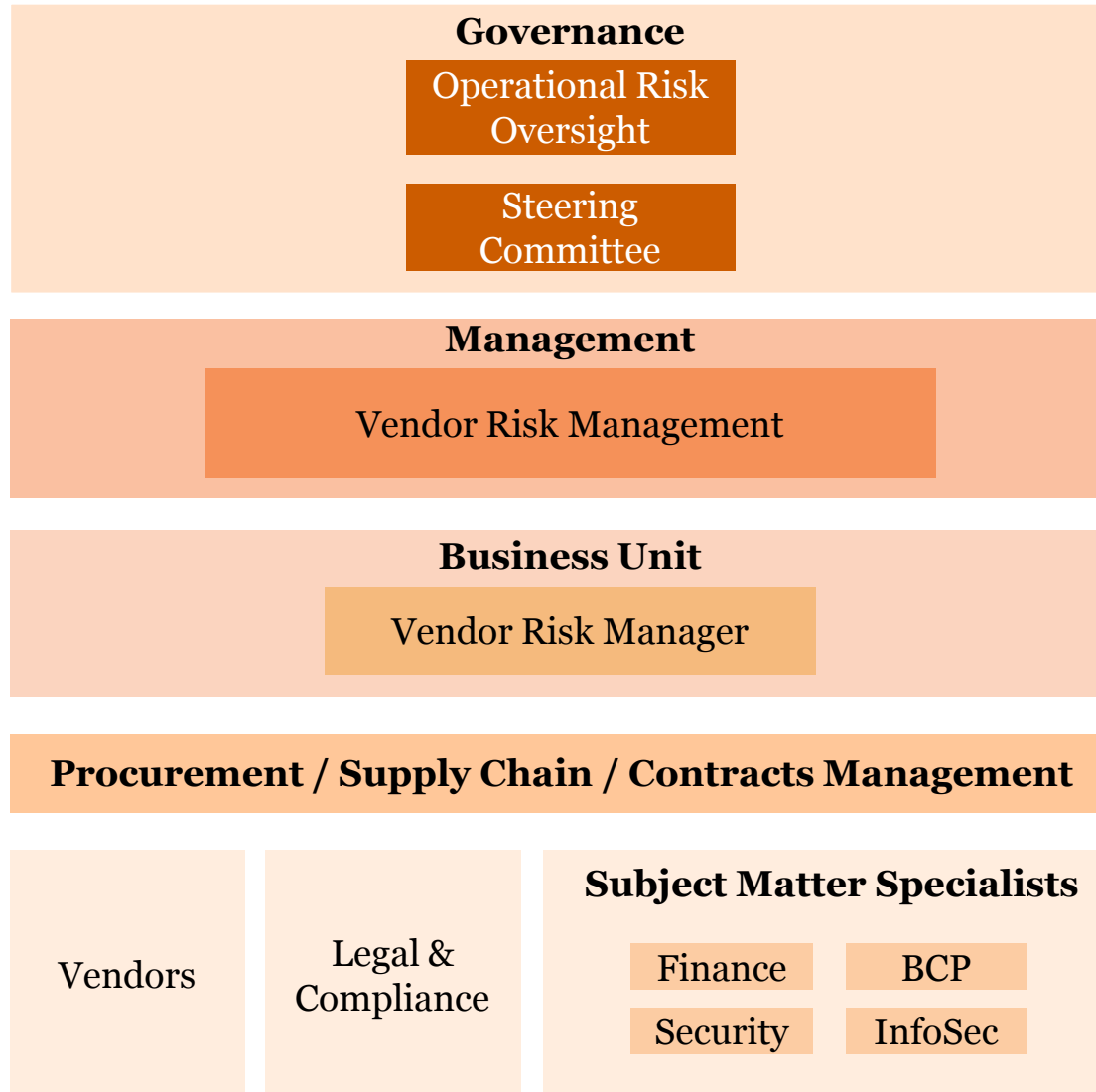


---

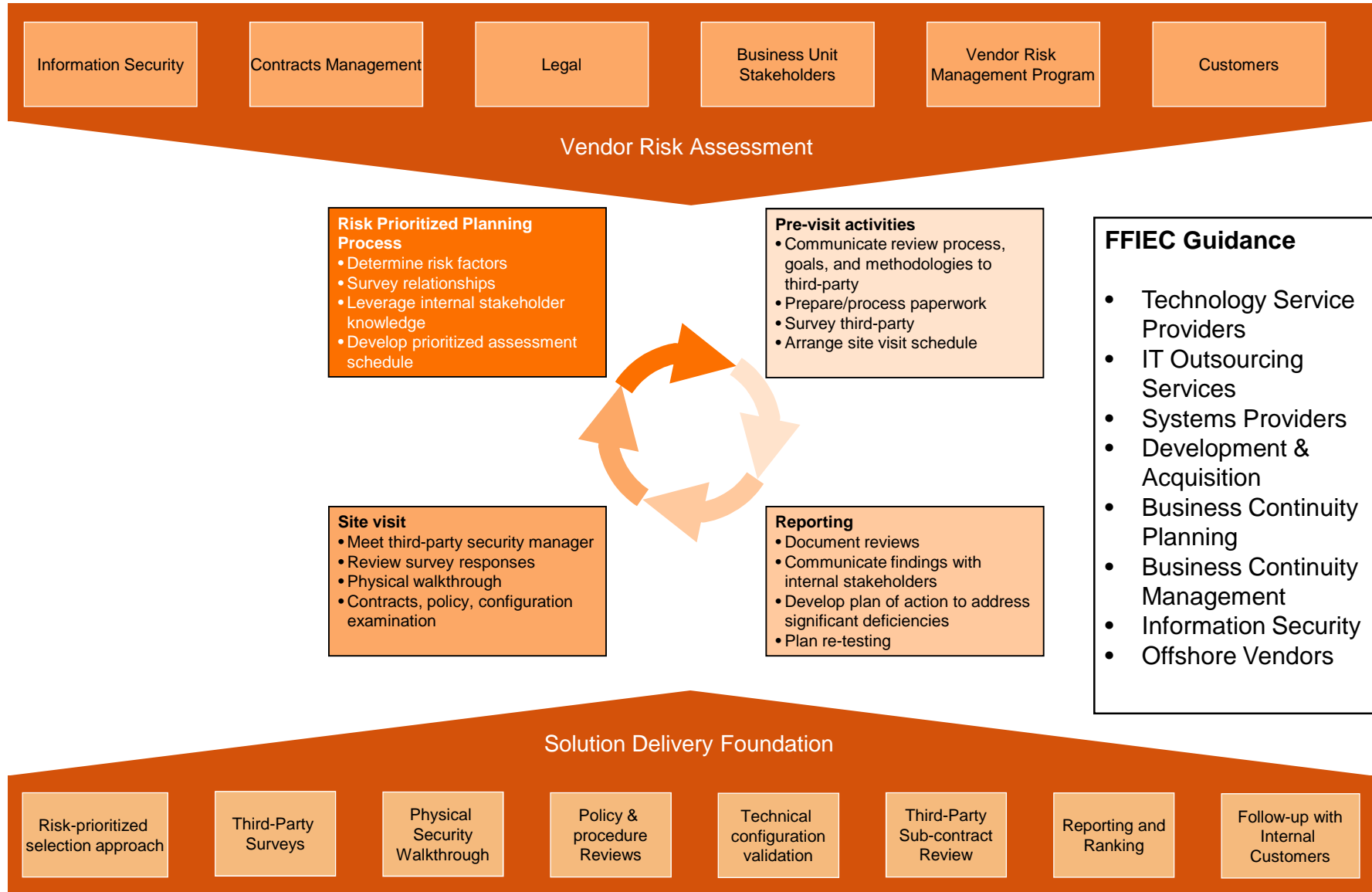
## A “Good Practices” Approach



# *Sample Vendor Risk Management Program Structure*



# Vendor Risk Assessment Approach



---

## ***Additional Vendor Risk Assessment Considerations***

***The following considerations may be incorporated into the vendor assessment upon request:***

### Due Diligence

- Experience
- Audited financial statements
- Reputation, complaints, litigation
- Qualifications
- Internal controls
- Adequacy of MIS
- BCP/DR
- Cost of development, implementation and support
- Use of third 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

### Ongoing Oversight

- Financial condition
  - Current financial statements
  - Vendor's obligations to sub-vendors
  - Insurance coverage
- Monitor controls
  - Audit reports
  - Vendor policies
  - On-site visits
  - Compliance risks
  - BC/DR plans and test results
- Quality of service and support
  - SLA reporting
  - Problem management
  - Alignment with organization's strategy
  - Customer complaints
  - Customer satisfaction survey
  - Performance meetings with Vendor

---

## ***Examples - Network Considerations***

### **Process related**

- Current network topology and connectivity diagrams
- Current technology hosting or processing environment designs
- Document of technical controls specific to the services being provided
- IT Management and Governance Processes and Functions document
- Document describing the effective supervision of each Provider

### **Technology related**

- Focus on monitoring and protecting organizations data exposed to 3<sup>rd</sup> party versus traditional network controls
- Consider using dedicated 3<sup>rd</sup> party connection firewalls to limit addresses and ports that can be accessed
- Consider using a risk-based data-centric approach to move systems being accessed by 3<sup>rd</sup> parties into self contained private VLAN's

---

## ***Examples-***

### ***User Access Considerations***

**Identity & Access Management strategy should include 3<sup>rd</sup> party user issues**

#### **Enforce Access (Real Time Access Controls)**

- Provide secure and seamless access to web resources across organizational boundaries through standards-based Federation
- Leverage 3<sup>rd</sup> party identity providers

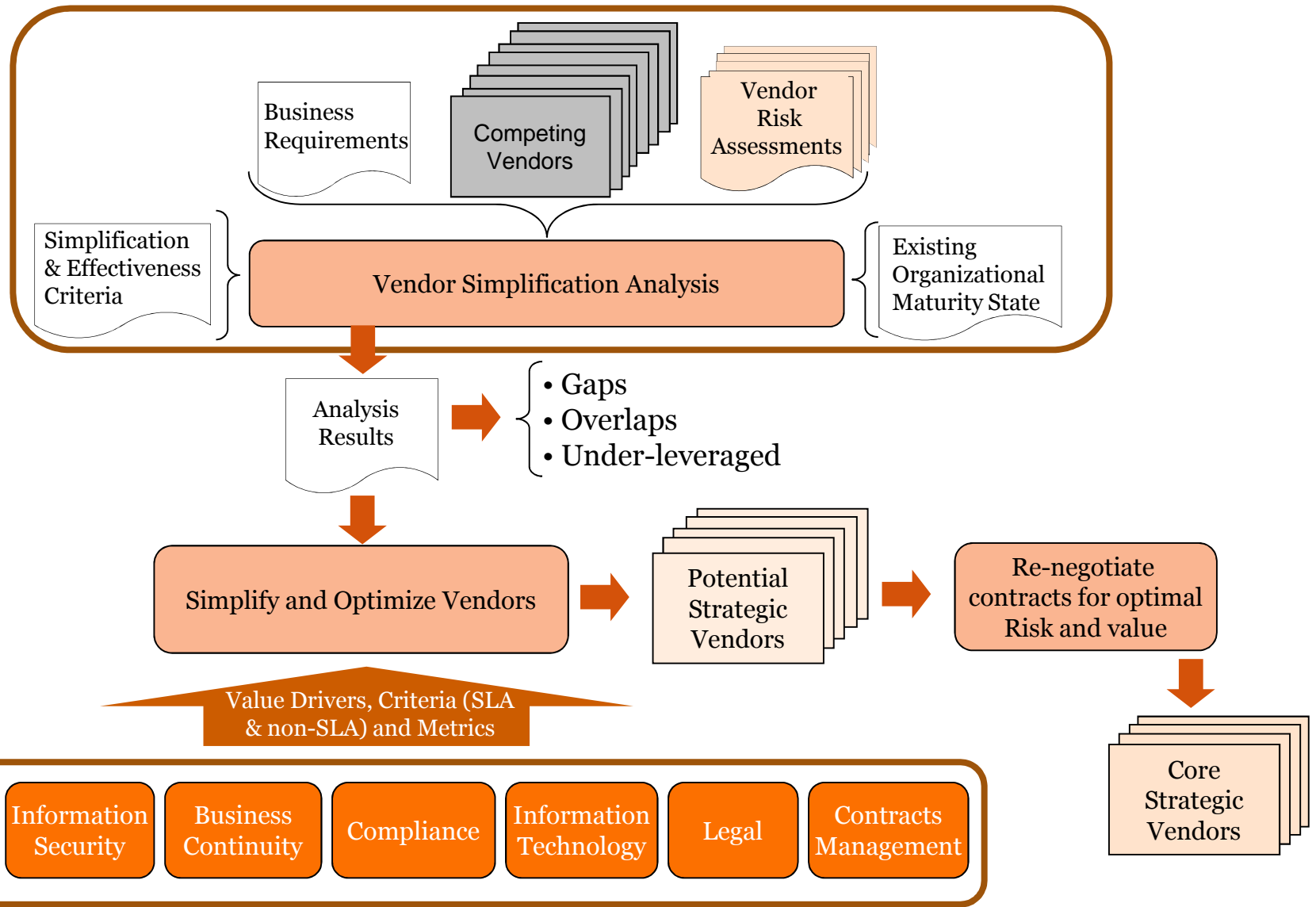
#### **Manage Access (User Lifecycle Events)**

- Review 3<sup>rd</sup> party controls around joiner/mover/leaver processes as relates to users having access to organizational resources
- Review 3<sup>rd</sup> party controls around how users request and gain access to organizational resources
- Validate controls in place to periodically review and certify user access for typical issues (e.g. Segregation of Duty, Least Privilege)

#### **Privileged Access**

- Ensure strict controls around 3<sup>rd</sup> party users who have elevated or privileged access to organizational resources

# Vendor Simplification



---

## ***Simplification and Effectiveness Criteria - Example***

- Existence of competing Vendors
- Sufficient competent Vendor Relationship Managers
- Vendor's capability maximized
- Funding model optimization
- Alignment of Vendor with Organization's business strategy & objectives
- Currency of Vendor's delivery model and value
- Vendor's Risk to Organization

---

## ***Risk Management for Larger Sourcing Vendors***


Business and regulatory environments have become increasingly complex, raising corporate risk profiles. Global Outsourcing is getting attention!

### Higher risk profiles

- Increasing scope and complexity of globally sourced business activities (i.e. product design, R&D, data intensive processes etc.)
- Continuous changes in regulatory requirements and expectations in response to market events (e.g. Financial and Healthcare responses)
- Increasing risks from technology (e.g., speed of execution, data vulnerability)

### Higher expectations

- Regulators expect corporate risk infrastructure to be commensurate with the scope and scale of current and planned business activities
- Investors demand more corporate visibility and accountability for risk management
- Rating agencies require evidence of effective governance, risk management and compliance programs



Strategic consequences exist if companies are unable to manage governance, risk and compliance requirements effectively

- Regulatory enforcement actions which limit acquisition/strategic plans
- Depressed market value and share price, triggering vulnerability to acquisition
- Financial losses and/or damaged reputation
- Systemic noncompliance resulting in litigation, fines, money penalties

---

***Thank you***

**Dan Morrison**

**(602) 206-3273**

**daniel.morrison@us.pwc.com**