



# Managing vendor risk and performing vendor assessments

ISACA Geek Week  
September 2008



---

# Abstract

---

- ▶ As organizations increasingly rely on external parties to execute certain business processes, companies need to ensure data is secure outside of the enterprise.
- ▶ This presentation provides an overview of outsourcing, describes key risks and challenges with outsourcing and approaches to vendor assessments that address privacy physical, procedural, and technical controls over data protection.
- ▶ The term “outsourcing” is used to describe many different vendor relationships in which data is transferred outside of the organization.

---

# Presentation outline

---

- ▶ Introduction to outsourcing
- ▶ Key risks and challenges in outsourcing
- ▶ Managing data protection and privacy risks
- ▶ Industry approaches to vendor assessments
- ▶ Case study
- ▶ Summary
- ▶ Q&A

---

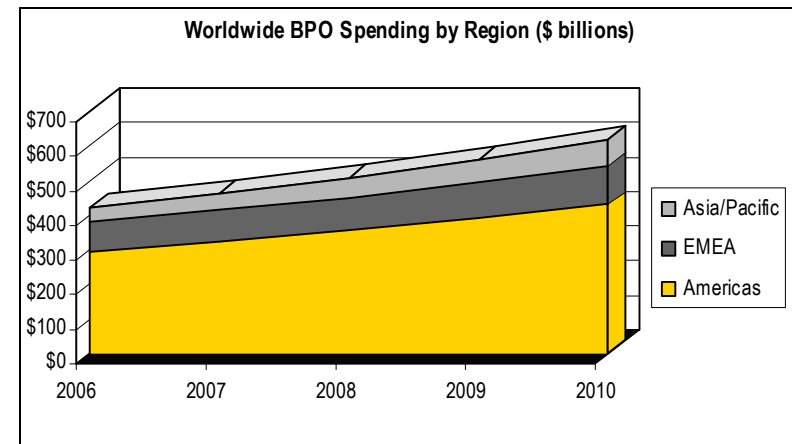
# Introduction to outsourcing



# Outsourcing market

- ▶ US companies have been steadily increasing their use of outsourcing (aka “strategic sourcing”)
- ▶ CAGR is approximately 9-10% per year
- ▶ Over 75% of IT organizations engage in some form of outsourcing

## *Business Process Outsourcing Spend*



Source: IDC

---

# Typical functions outsourced

---

- ▶ Information technology:
  - ▶ Help desk
  - ▶ Data center management
  - ▶ Network and IT infrastructure management
  - ▶ Application development and maintenance
  - ▶ Independent testing and validation
  - ▶ Systems integration
  - ▶ Research and development
  - ▶ Product development
  - ▶ Security management
  - ▶ Application hosting
- ▶ Business process:
  - ▶ Billing and clearing
  - ▶ Card processing
  - ▶ Credit services
  - ▶ Purchasing and accounts payable
  - ▶ Benefits/payroll
  - ▶ Other human resource functions
  - ▶ Document processing
  - ▶ CRM/Call centers
  - ▶ Marketing analysis

# Why outsource?

---

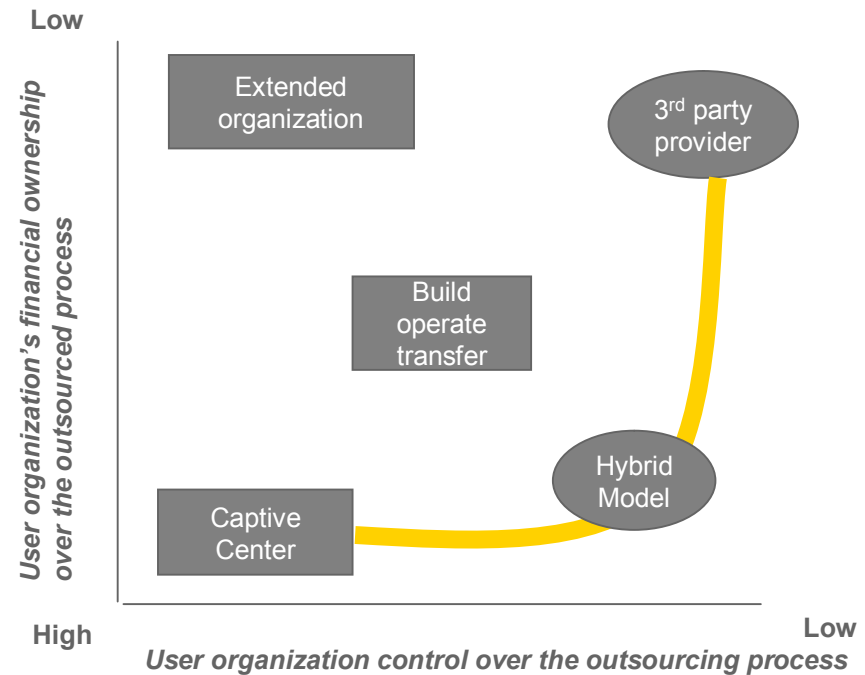
- ▶ Reduce workload and cost
- ▶ Improve processes
- ▶ Realign resources

## ▶ Case Study

- ▶ Health payer organization with over 1m members and 12,000 employees
- ▶ Needed to meet operational requirements for claims processing
- ▶ Utilized service providers business processing center in India to augment processing capabilities
- ▶ Benefits:
  - ▶ Faster claims processing
  - ▶ Meeting timeliness and accuracy goals
  - ▶ Quality improvements in data
  - ▶ Increased 1<sup>st</sup> pass auto resolution rate
- ▶ Reduced cost of operations by \$1m annually

# Outsourcing models

- ▶ Outsourcing may be:
  - ▶ Offshore
  - ▶ Near-shore
- ▶ Many different models
- ▶ Drivers include:
  - ▶ Cost
  - ▶ Control
  - ▶ Scalability
  - ▶ Operational risk
  - ▶ Management effort



---

# Key risks and challenges in outsourcing



# Outsourcing process

## Alignment

- Validating the strategy
- Identifying the options
- Preparing the business model
- Agreeing on sponsorship and building the team

## Transaction

- Structuring the deal
- Agreeing on outsourced assets
- Negotiating the contract
- Delivering the deal and the business case

## Optimization & Transformation

- Monitoring the contract and resolving disputes
- Transforming the business
- Reassessing the relationship
- Delivering the business case – realizing the benefits

## Governance Process



## Project and Risk Management

### Feasibility

- Building the business model and case
- Creating the baseline
- Understanding the market
- Assessing and benchmarking options

### Transition

- Delivering the change
- Getting quick returns on investment
- Establishing the culture
- Managing the people

### Termination & Renegotiation

- Planning the termination
- Renegotiating the contract
- Reassessing the relationship
- Decommissioning or reallocating outsourced services

Source: GTAG 7: Information Technology Outsourcing, Institute of Internal Auditors

# Overall outsourcing risks

Process Stage	Key Risks
Strategy	<ul style="list-style-type: none"> <li>▶ Not aligned</li> </ul>
Feasibility	<ul style="list-style-type: none"> <li>▶ Incorrect assumptions</li> <li>▶ Inadequate due diligence</li> <li>▶ Poor risk assessment</li> </ul>
Transaction	<ul style="list-style-type: none"> <li>▶ Procurement policies not met</li> <li>▶ SLA not negotiated</li> <li>▶ Operational, HR, regulatory issues not addressed</li> <li>▶ Contingencies not planned</li> </ul>
Transition	<ul style="list-style-type: none"> <li>▶ Lack of transition planning</li> <li>▶ Retention</li> <li>▶ Escalation and resolution</li> </ul>
Optimization & Transformation	<ul style="list-style-type: none"> <li>▶ Not managed effectively</li> <li>▶ Benefits not realized</li> <li>▶ Data not protected/secured</li> <li>▶ Vendor not scalable</li> <li>▶ Inability to meet regulatory requirements</li> </ul>
Termination & Renegotiation	<ul style="list-style-type: none"> <li>▶ Not planned</li> <li>▶ Poorly executed</li> </ul>

---

# Managing data protection and privacy risks



# Risks related to data protection

---

<b>Identification</b>	<ul style="list-style-type: none"><li>▶ What vendors are exchanging data?</li><li>▶ What is the business purpose?</li><li>▶ What types of data?</li></ul>
<b>Policy</b>	<ul style="list-style-type: none"><li>▶ Are data protection policies/requirements defined?</li><li>▶ Does vendor understand expectations?</li></ul>
<b>Contract</b>	<ul style="list-style-type: none"><li>▶ Have contract requirements been defined?</li><li>▶ Is “right to audit” clause included?</li></ul>
<b>Compliance</b>	<ul style="list-style-type: none"><li>▶ How do ensure vendor compliance?</li></ul>
<b>Termination</b>	<ul style="list-style-type: none"><li>▶ How is data treated in termination?</li></ul>

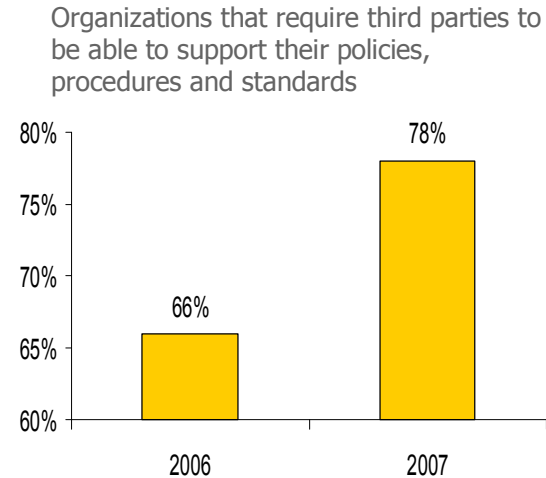
If not addressed impacts might include:

- Information loss
- IP misuse or theft
- Non compliance with regulatory requirements
- Reputation/brand damage

# Defining policies and requirements is key

## Key Findings

- ▶ Seventy-eight percent of respondents require third parties to be able to support the policies, procedures, and standards of their own organization – an increase of 12 percentage points over the number reported in 2006.
- ▶ Forty-eight percent of respondents also require the third party organization to have their own information security and privacy policies and procedures – up 7 percentage points from last year.



*Source: Ernst & Young 2007 Global Information Security Survey*

---

# Other lessons learned

---

- ▶ Review or develop inventory of vendors and data exchanges
- ▶ Get involved early in the outsourcing process
- ▶ Understand regulatory requirements in all impacted geographies
- ▶ Create audit expectations before contract signing, including “right to audit”
- ▶ Require outsourcers to implement security policy, not set it
- ▶ Consider impact of security on SLAs
- ▶ Don’t embed detailed security requirements into contracts

# Approach to managing data protection risks

<b>Assess</b>	<ul style="list-style-type: none"><li>▶ Identify outsourced vendor relationships</li><li>▶ Identify and assess the risks emanating from outsourced processes. Consider:<ul style="list-style-type: none"><li>▶ Corporate assets that vendor processes (public, confidential or highly confidential)</li><li>▶ Impact of a vendor outage</li><li>▶ Direct contact with customers</li><li>▶ Business unit risk tolerance</li><li>▶ Regulatory requirements</li></ul></li></ul>
<b>Develop</b>	<ul style="list-style-type: none"><li>▶ Define policies, technical and procedural controls</li><li>▶ Develop vendor compliance approach</li></ul>
<b>Implement</b>	<ul style="list-style-type: none"><li>▶ Implement technical controls</li><li>▶ Perform assessments</li><li>▶ Establish comprehensive repository of results</li><li>▶ Communicate risk management goals with business unit leads and the vendor</li></ul>
<b>Monitor</b>	<ul style="list-style-type: none"><li>▶ Institutionalize review mechanisms and perform periodic assessments</li><li>▶ Update risk classifications</li></ul>

---

# Industry Approaches to Vendor Assessments

---



# Regulatory environment

- ▶ Privacy and data protection and breach disclosure requirements
  - ▶ Federal
  - ▶ State
- ▶ EU Privacy Directive/US Safe Harbor
- ▶ **Companies retain responsibility for protecting that data even when they cede custody of that data to external parties.**
- ▶ Typically utilize contract, business partner agreement and/or SLAs to enforce requirements

Pertinent Regulations	
Gramm-Leach-Bliley Act	California 1386 & 1950 (Security Procedures and Notification)
Sarbanes-Oxley Act (SOX)	California SB 27 (Third Party Direct Marketing)
Health Insurance Portability and Accountability Act (HIPAA)	Individual State Security Breach Acts
Payment Card Industry (PCI) Data Security Standards	Others still pending...

---

# Defining vendor assessment requirements

---

- ▶ Company Policies
- ▶ Vendor Contracts
- ▶ Industry guidelines:
  - ▶ Sector Specific Guidelines (NERC- Interim Security Guidelines)
  - ▶ Legal/Regulatory Requirements (Sarbanes Oxley, GLBA, HIPAA, FISMA)
  - ▶ Security Checklists (BSA, NIST, OECD)
  - ▶ Board Governance Guidelines (NACD, IIA, CIAO)
  - ▶ Guidelines for Senior Managers (ISA, eSAC, ICC, NIST, TechNet)
  - ▶ General Management Guidelines (CERT, NSA)
  - ▶ Risk management Models (SEI- Octave, NIST 800-30)
  - ▶ Configuration/Patching Guides (DISA, NIST, NSA, SANS, CIS)
  - ▶ Comprehensive Models (ISO 21827- SSE-CMM, SSE-CMM)
  - ▶ Controls Based Models (BS 7799, ISO 17799, CobiT, FISCAM-GAO, SysTrust/WebTrust- AICPA, NIST 800-series, FFIEC, BITS Framework)
  - ▶ General Control Models (CoCo- CICA, COSO-Treadway)
  - ▶ Principles Based Models (OECD, GAPP-NIST 800-18, GAISP, Basel II)

# Representative areas

---

## ▶ **Procedural controls**

- ▶ Records management and retention
- ▶ Policies and procedures
- ▶ Security awareness and training
- ▶ Background checks
- ▶ Confidentiality agreements
- ▶ Business continuity
- ▶ Incident response
- ▶ Change control
- ▶ Systems auditing

## ▶ **Physical controls**

- ▶ Security guards
- ▶ Asset accounting and inventory
- ▶ Physical access barriers
- ▶ Confidential disposal
- ▶ Backup and offsite storage
- ▶ Fire suppression

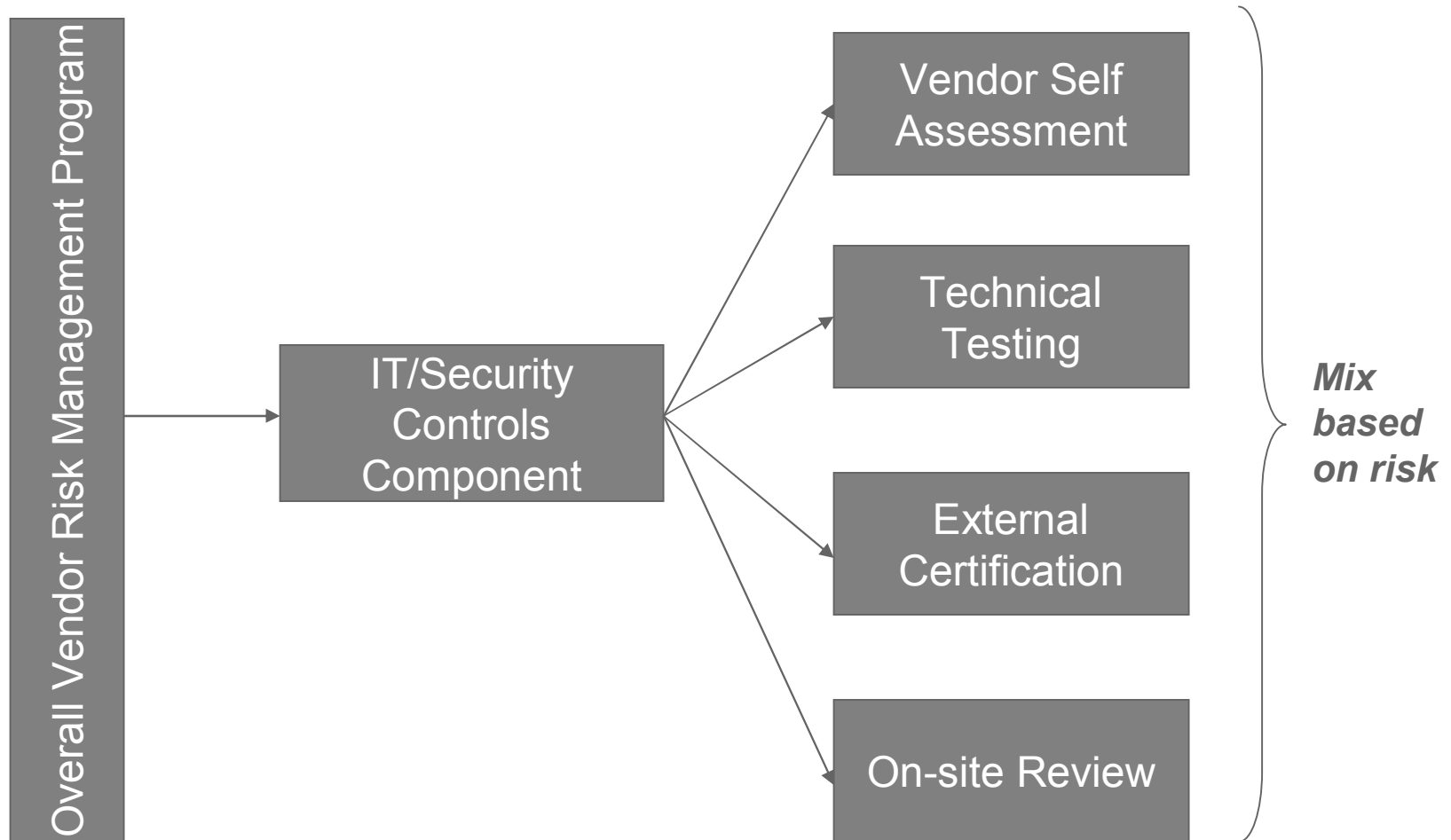
## ▶ **Privacy controls**

- ▶ Acceptable use
- ▶ Information classification
- ▶ Third party access
- ▶ User access
- ▶ Privacy policy

## ▶ **Technical controls**

- ▶ Network documentation
- ▶ Firewall/router/server configuration and patch management
- ▶ Antivirus
- ▶ Encryption
- ▶ Logging and monitoring
- ▶ Intrusion detection
- ▶ Access management
- ▶ Content filtering
- ▶ Audit trails
- ▶ Remote access
- ▶ Wireless
- ▶ Vulnerability testing
- ▶ Logon banners

# Typical approach to vendor assessments



---

# Vendor self assessment

---

- ▶ Typical scope: Vendor completes a questionnaire (sometimes online) that describes security policies and controls
- ▶ Advantages:
  - ▶ Efficient process once questionnaire established
- ▶ Disadvantage:
  - ▶ Relies on representations made by vendor (not validated)
  - ▶ Interpretation of questions and responses may be required

---

# Technical testing

---

- ▶ Typical scope: Vendor is subjected to technical attack and penetration testing by company or independent tester
- ▶ Advantages:
  - ▶ Provides validation that technical controls are in place
  - ▶ Can be a test of incident response process
- ▶ Disadvantages:
  - ▶ Skill and time required to perform testing
  - ▶ Point in time result
  - ▶ Needs follow up to ensure remediation performed
  - ▶ Limited to scope of technical test (e.g., internet addressable devices)

---

# External certification - SAS70

---

- ▶ Typical scope: Vendor engages CPA to perform service organization audit
  - ▶ Type I: Design only
  - ▶ Type II: Design and operating effectiveness
- ▶ Advantages:
  - ▶ Independent attestation
- ▶ Disadvantages:
  - ▶ Control objectives/coverage may not be relevant

AICPA Trust services provides an alternative to SAS 70 reporting

---

# External certification - FISAP

---

- ▶ Typical scope: Standardized program developed within financial services industry. Vendor engages assessment firm to perform agreed upon procedures (AUPs)
- ▶ Advantages:
  - ▶ Results are reported
- ▶ Disadvantages:

---

# External certification - ISO27001

---

- ▶ Typical scope: Vendor engages an accredited testing organization to perform an ISO27001 certification
- ▶ Advantages:
  - ▶ Internationally recognized security certification – limited but growing acceptance in US
- ▶ Disadvantages:
  - ▶ Need to define area of applicability
  - ▶ Skills and time required by vendor

---

# On-site assessment

---

- ▶ Typical scope: Company conducts an onsite assessment of vendor utilizing their own audit program/checklist
- ▶ Advantage:
  - ▶ Provides higher degree of comfort to the company
  - ▶ Program can be linked directly with company policies and vendor contractual requirements
- ▶ Disadvantages:
  - ▶ Skill and time required by company

---

# Case study



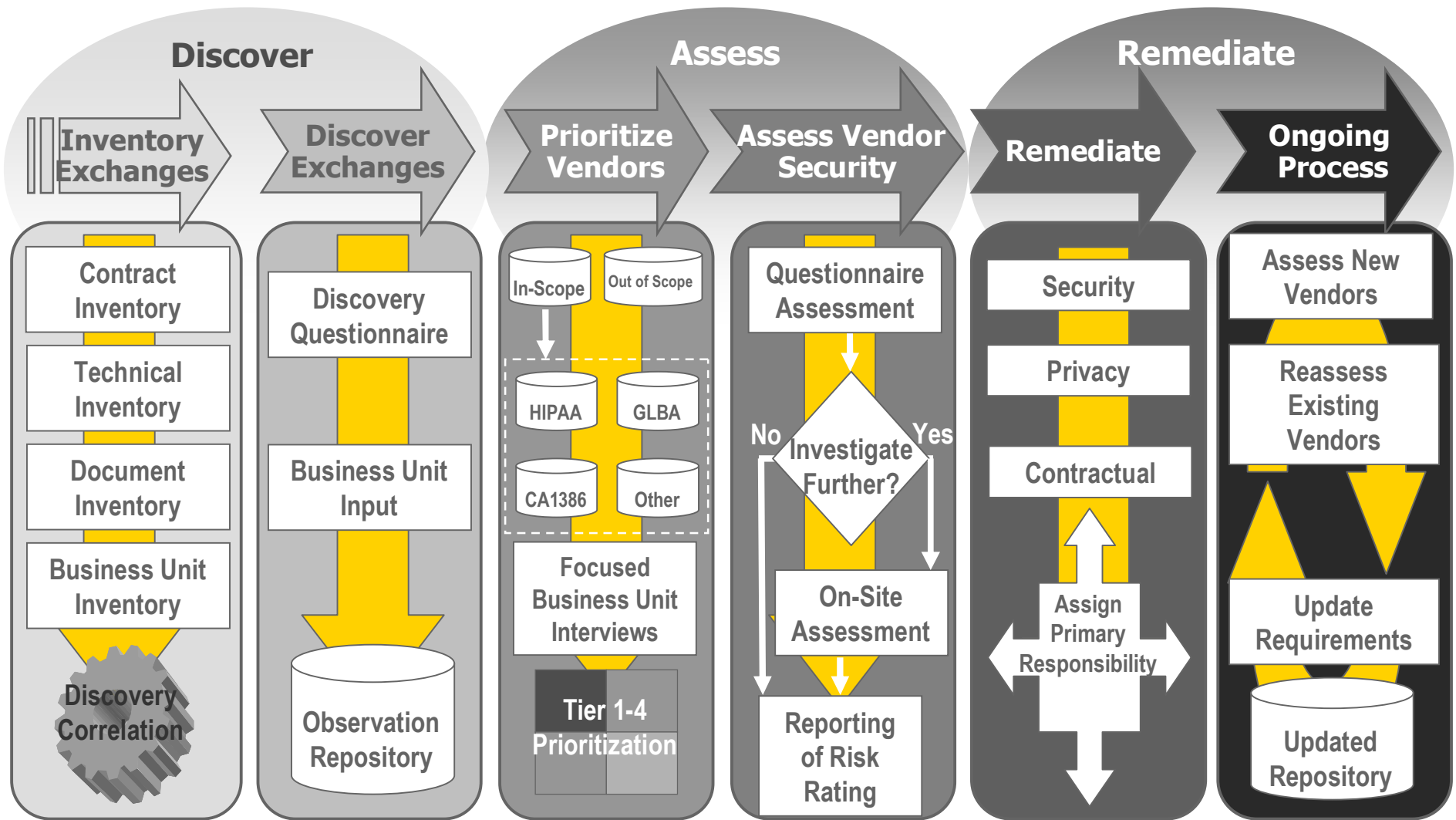
---

# Background

---

- ▶ **Business scenario:**
  - ▶ Large financial institution wanted to improve vendor risk management around data protection\
- ▶ **Initial observations:**
  - Lack of formal documentation for many vendors exchanges
  - Same vendor, multiple exchanges, different controls
  - Business owners difficult to identify
  - Lack of consistent process to assess and monitor vendors
  - Vendors not addressing remediation action plans
  - Some “out of band” communications (e.g., e-mail)
  - “Procuring without Procurement”
  - Lack of timely remediation follow up

# Approach



# Risk tiers used to determine vendor approach

		Data Classification	
		Highly Sensitive	Sensitive
Data Volume	High	<b>Tier 1</b> Assessment questionnaire and on-site security assessment	<b>Tier 3</b> Assessment questionnaire only unless significant issues are noted
	Low	<b>Tier 2</b> Assessment questionnaire <i>may</i> be followed by on-site assessment	<b>Tier 4</b> Document in exchange database only

# Vendor questionnaires and on-site assessments

## ▶ Vendor questionnaire

- ▶ On-site work plan mapped to NSA IAM and ISO17799 Standards
- ▶ General questions include information about the type and quantity of systems storing, processing, and transmitting of data to third parties
- ▶ Assessment questions focus around management, operational and technical controls protecting data
- ▶ Focus of the questionnaire assessment is on policies and procedures. Assurance received is the equivalent of obtaining a process narrative without doing any testing

## ▶ On-site assessment

- ▶ On-site assessment focused on actual application of technical controls for systems that store, transmit and process data; leverages the work performed in the vendor questionnaire
- ▶ Develop Data Flow Diagram to illustrate current state vendor exchanges
- ▶ Compare stated policies and procedures to actual production controls (or lack thereof)
- ▶ Gain understanding of all storage, processing and transmission points by creating data flow diagram during walkthrough
- ▶ Conduct a physical walkthrough of data center and office environment security

---

# On-site assessment topics

---

- ▶ Privacy Controls – Interview key personnel who have access to PHI/PII data. Evaluate the level of awareness and compliance to policy, contractual and regulatory requirements.
- ▶ Data Flow – Map each point of transmission, storage, and processing of privacy data from the point it enters the vendor to the point it is deleted or relayed to another party. Include any “ad-hoc” reporting and retention of reporting data.
- ▶ Physical Evaluation – Determine if the physical layout of the data center and office premises support effective privacy and security controls.
- ▶ Procedural Controls – Determine if procedural controls outlines in the questionnaire are in fact followed on systems containing privacy data.
- ▶ Technical Controls – Verify that the technical controls identified in the questionnaire are actually applied on the systems storing, transmitting or processing data. This includes:
  - ▶ Password controls
  - ▶ Patching
  - ▶ Hardening
  - ▶ Account management
  - ▶ Monitoring
  - ▶ Encryption of data

---

# Remediation approaches

---

- ▶ Various remediation techniques employed:
  - ▶ Communication to vendors should state identified gaps and track remediation against those gaps – follow-up communication should confirm gap closure
  - ▶ Excessive data elements may be transmitted to vendor
    - ✓ Remove or mask unneeded data elements before transmission to vendor (i.e. only last four digits of SSN)
  - ▶ Consider compensating security controls for company
    - ✓ Additional monitoring on VPN link with vendor
    - ✓ Additional controls over company's site that the vendor accesses
  - ▶ Specify security standards in contract with vendor/use as leverage during next contract renewal

# Lessons learned

---

- Few third parties protect data as you do
- Closely review SAS 70
- Include 'right to audit' in contract
- Trust but verify
- Off-shoring adds complexity
- Track vendor remediation
- On-going process; dynamic vendor list
- Involve Business units, Procurement & Legal
- Data exchanges not restricted to minimum data elements needed
- Include security posture as part of vendor selection criteria
- Data sent to previously unknown 4th parties
- The need for a continuous maintenance process to keep up with the changes



---

# Summary



---

# Summary

---

- ▶ Organizations will increasingly rely on external parties to execute certain business processes
- ▶ Whether driven by cost, technology or skills, organization will need to draw on solutions at both large and small vendors and maintain a multitude of relationships
- ▶ In order to ensure that your data is secure outside the enterprise, vendor risk management needs to be a robust process executed with consistency across your organization

---

## For more information

---

- ▶ “Governance of Outsourcing”, IT Governance Institute
- ▶ “GTAG-Information Technology Outsourcing”, Institute of Internal Auditors
- ▶ “Outsourcing Technology Services”, FFIEC Examination Handbook
- ▶ Financial Industry Shared Assessment Program ([www.bitsinfo.org/fisap](http://www.bitsinfo.org/fisap))

---

---

# Questions?

---

Graeme Payne  
Ernst & Young LLP  
Technology & Security Risk Services  
Phone: 404-817-4921  
E-mail: [Graeme.Payne@ey.com](mailto:Graeme.Payne@ey.com)