U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

HITECH & The Cloud: Control and Accessibility of Data Downstream

David Holtzman, OCR (Moderator)

James Koenig, Privacy Leader; Health Information Privacy & Security Practice Co-Leader, PricewaterhouseCoopers

Ted LeSueur, Director Product Security, McKesson Corp.

NIST/OCR HIPAA Security Assurance Conference

May 21, 2013

Panel introductions

David Holtzman (moderator)
HHS Office for Civil Rights
David.Holtzman@HHS.GO V
202-205-1619

James Koenig
Leader, Privacy & Data Protection Practice; and
Co-Leader, Health Information Privacy & Security Practice
james.h.koenig@us.pwc.com
610-246-4426

Ted A. LeSueur, CISSP, CHP, CSCS, MSCIS
Director, Product Security
Information Security and Risk Management
McKesson Corporation
Ted.LeSueur@McKesson.com
480-663-4196

Session Overview

- Introduce the HIPAA Privacy and Security Rule requirements for business associates
- Challenges organizations face in establishing and managing business relationships with cloud service providers
- Industry trends to manage risk and compliance
- Post-contract audit of cloud service providers to assure compliance with regulatory requirements and contractual agreements

David Holtzman, OCR (Moderator)

Business Associates Requirements Established in Omnibus Final Rule

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule
  - Liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule
  - Criminal and civil liabilities for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of a BA are now defined as a BA
  - BA liability flows to all subcontractors

Applying New Requirements

- Cloud service provider is a business associate if the data is maintained in the performance of its function
  - Even if the agreement with the covered entity does not contemplate any access or access only on a random or incidental basis.
  - The test is persistence of custody, not the degree (if any) of access.
- Downstream entities that work at the direction of or on behalf of a business associate and handle PHI are required to comply with the applicable Privacy and Security Rule provisions, just like the “primary” business associate and are subject to the same liability for failure to do so.

General Rules

- Ensure confidentiality, integrity, and availability of ePHI
- Flexible approach
- Addressable and required standards
  - Addressable ≠ Optional
  - Addressable measures are required if “reasonable and appropriate”
- Review and modify security measures as needed

Security Rule: Key Areas

- Implement security management process
  - risk analysis, mitigation & evaluation process
- Train workforce on safeguarding PHI
- Have contingency plans in place
  - disaster recovery and emergency mode operation
  - create and maintain retrievable exact copies of data
- Policy/procedure for system activity review & audit
- Physical safeguards for components & devices
- Have business associate agreements with CEs and subcontractors

Security Rule:
Key Technical Safeguards

- Implement reasonable and appropriate safeguards to ensure the CIA of data on systems that create, transmit or store PHI
  - Encryption at rest
  - Encryption during transmission
  - Automatic logoff
  - Strong authentication
- Properly configure wireless network access

James Koenig, Privacy Practice Leader; Health Information Privacy & Security Practice Co-Leader, PricewaterhouseCoopers

Trends around Vendors & Cloud in Healthcare

- **New Health Care Delivery Models & Technologies Drive Use of Vendors.** More third parties are needed and entrusted with personal information/PHI as (i) new healthcare delivery models (e.g., EHRs, HIEs, ACOs, telemedicine) and (ii) new technologies (e.g., cloud computing, mobile devices, interactive and social media) are being increasingly used.

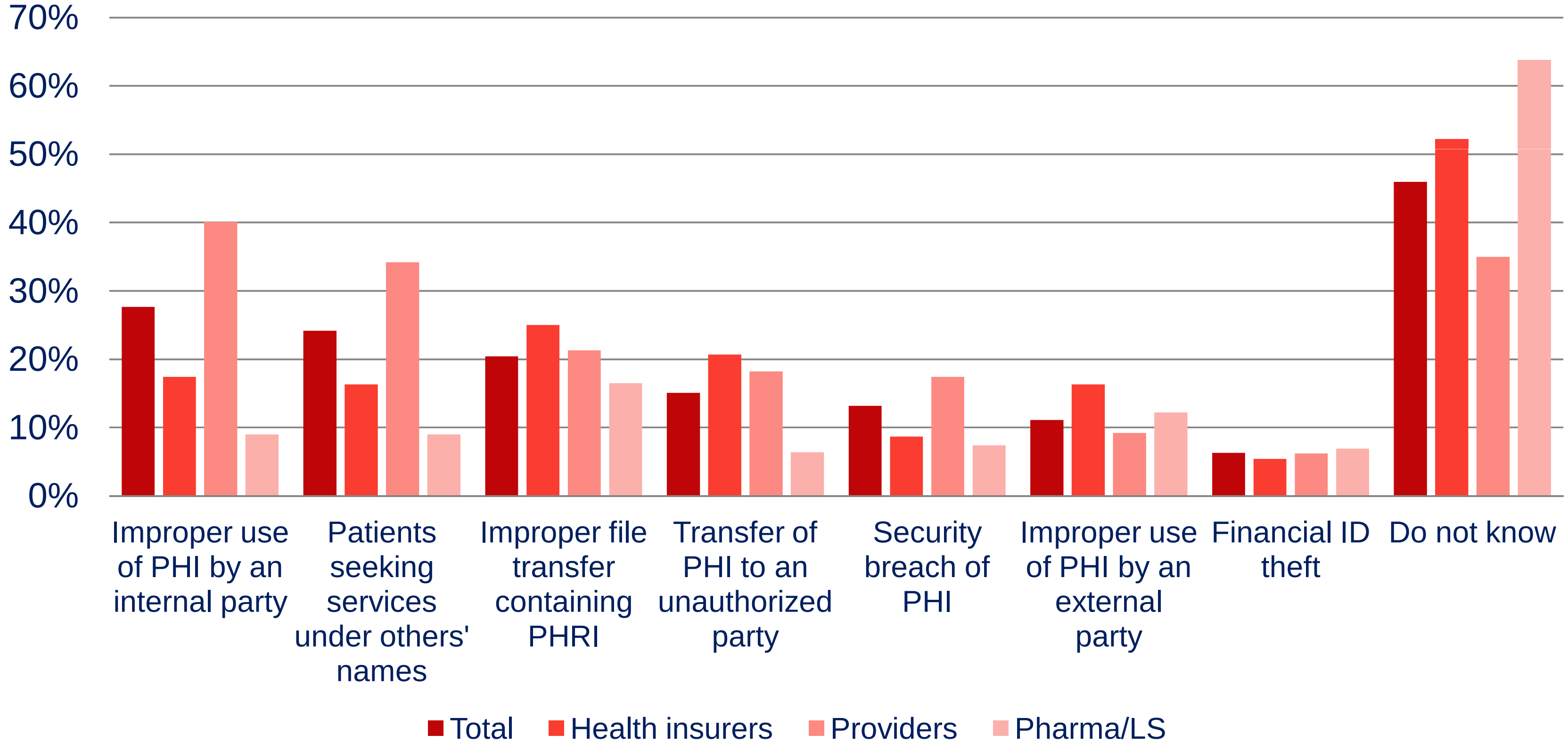
- **The Drive to the Cloud Varies by Health Sector.**
  - **Providers** – Implementing cloud EHRs, ePrescribing and IT help service desks
  - **Payors** - Placing outcomes-based research/analytics applications in cloud
  - **Pharma/LS** – Consolidating systems, electronic data capture, safety
  - **HR** – Implementing cloud HR consolidated systems, including benefits

- **Conduit Rule and Other requirements beyond HIPAA**
  - **Historically, cloud providers may have relied on Conduit Exception.** Under Final Rule, exception only includes courier services that transport information (persistent vs. transient opportunity to access)
  - **Massachusetts CMR 201** Requires Vendor Diligence
  - **FTC** Vendor Fraudulent Use of Data (Lack of Vendor Diligence) – Vendor privacy/security policy must be "in sync" with that of contracting company.

54% of healthcare organizations have experienced a privacy/security issue in the last two years

Of the 11 million people affected by data breaches 2009-2011, 55% were affected by breaches involving business associates

Within the last two years, have you experienced any of the following? Please select all that apply.



Source: PwC Health Research Institute privacy and security survey, 2011

Cloud Computing – Is It Just a Business Associate or a Special Case

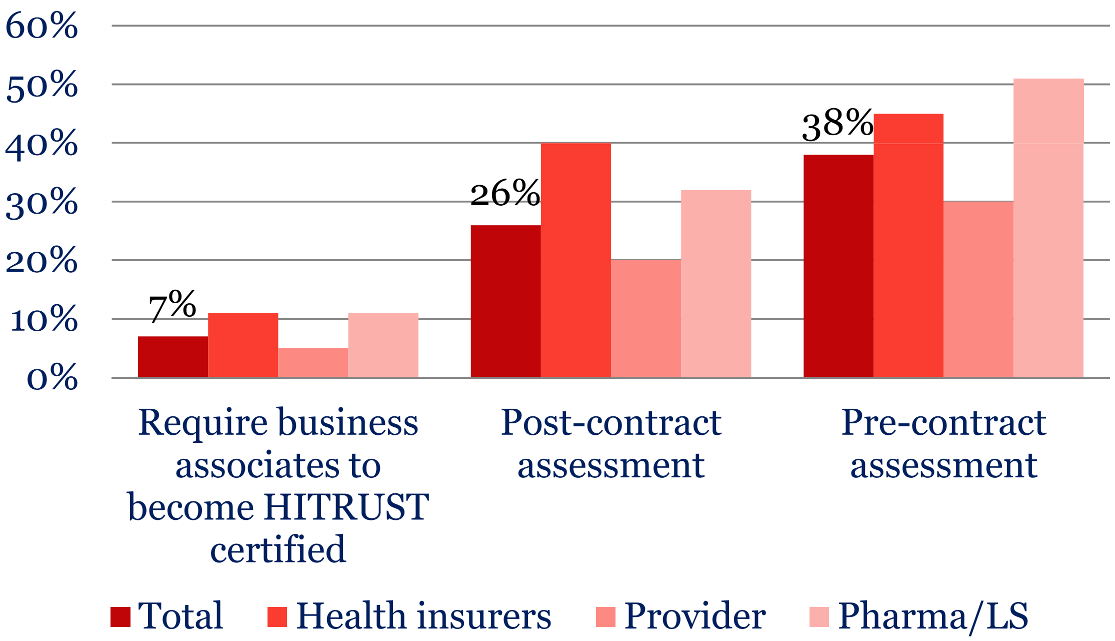
- **The Differences Are Cloudy.** Cloud is a subset of Business Associate oversight/compliance, yet it has special issues, heightened risks and complexities
  - **Where is the PHI?** Location / geography of data
  - **How do I minimize breach risk?** Incident response plan
  - **How do I prevent breach notifications?** Encryption at rest and transit
  - **How do I minimize breach risk and prevent notifications?** Incident Response plan, rights to forensics and encryption
  - **Who can access my PHI?** Access controls to prevent unauthorized access
  - **Who accessed or modified my PHI?** Audit logging and monitoring
  - **How can I prevent "domino" destruction or "neighbor peeping"?** Segregation of data
  - **How is PHI disposed at end of contract.** Retention and destruction
  - **How to prevent threat of knowledgeable insiders?** Internal security (e.g. employee background checks, training and physical and logical access)
- **Approaches Are Hard to Forecast.** Heath care organizations are addressing in various ways

Given risks, organizations are increasing assessing/ monitoring business associates' practices; still low, but changes based on Final Omnibus HIPAA Rule

Industry trend around vendor management:

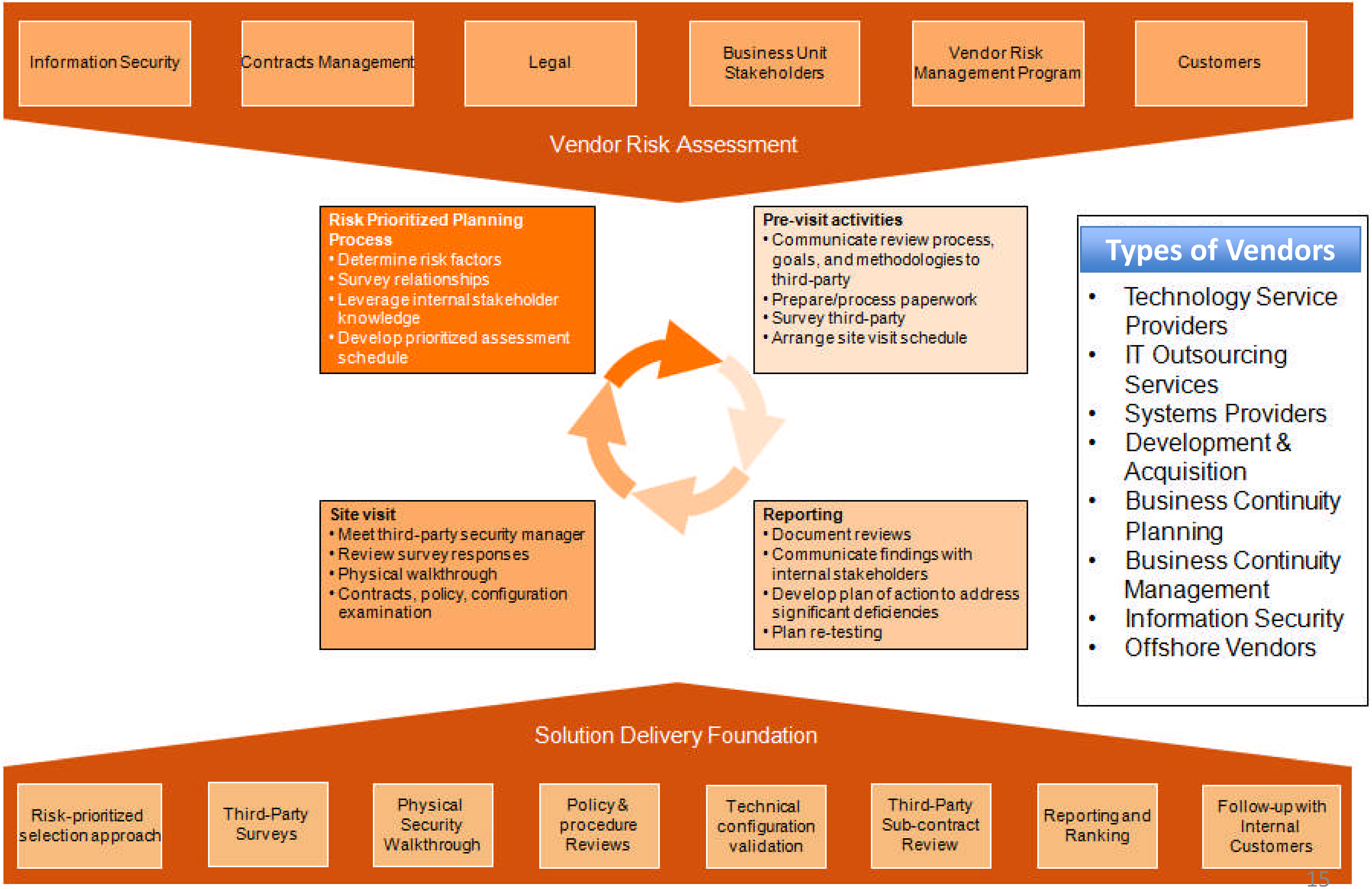
1. *Adding Pre-Contract Risk/Controls Assessments*
2. *Enhancing Contractual Safeguards/BAAs*
3. *Adding/Enhancing Post-Contract Audits*

How do you ensure that a business associate (partner/vendor) can be trusted with protected health information? Please select all that apply.



Source: PwC Health Research Institute privacy and security survey, 2011

Sample - Vendor Risk Assessment Approach



Information Security

Contracts Management

Legal

Business Unit Stakeholders

Vendor Risk Management Program

Customers

Vendor Risk Assessment

Risk Prioritized Planning Process
- Determine risk factors
- Survey relationships
- Leverage internal stakeholder knowledge
- Develop prioritized assessment schedule

Pre-visit activities
- Communicate review process, goals, and methodologies to third-party
- Prepare/process paperwork
- Survey third-party
- Arrange site visit schedule

Site visit
- Meet third-party security manager
- Review survey responses
- Physical walkthrough
- Contracts, policy, configuration examination

Reporting
- Document reviews
- Communicate findings with internal stakeholders
- Develop plan of action to address significant deficiencies
- Plan re-testing

Solution Delivery Foundation

Risk-prioritized selection approach

Third-Party Surveys

Physical Security Walkthrough

Policy & procedure Reviews

Technical configuration validation

Third-Party Sub-contract Review

Reporting and Ranking

Follow-up with Internal Customers

Types of Vendors

- Technology Service Providers
- IT Outsourcing Services
- Systems Providers
- Development & Acquisition
- Business Continuity Planning
- Business Continuity Management
- Information Security
- Offshore Vendors

Framework Used Depends on Type of Cloud and Goals

Three types of cloud architectures under NIST SP 800-145:

- **Infrastructure as a Service (IAAS)**
  - Hardware and Network controlled by provider
  - OS, Application, etc controlled by end-user
  - Allows nearly instantaneous deployment of servers
- **Platform as a Service (PAAS)**
  - Hardware, Network, OS and Database controlled by provider
  - Application code "plugged in" by end-user and run in remote environment
  - Lack of control/flexibility makes this less popular
- **Software as a Service (SAAS)**
  - Hardware, Network, OS, DB, Application controlled by provider centrally
  - End-user access applications through a web browser
  - Reduces deployment times, removes critical data from mobile computers

Assessment/Audit Standards

- SAS 70, SOC 1 , SOC 2
- AICPA GAPP
- HITRUST
- National Institute for Standards and Technology (NIST) SP 800-53 rev. 4 – Privacy & security controls
- NIST SP 800-66 – HIPAA
- NIST SP 144-146 Cloud
- ISO / IEC 27001
- CSA Cloud Controls Matrix
- FedRAMP

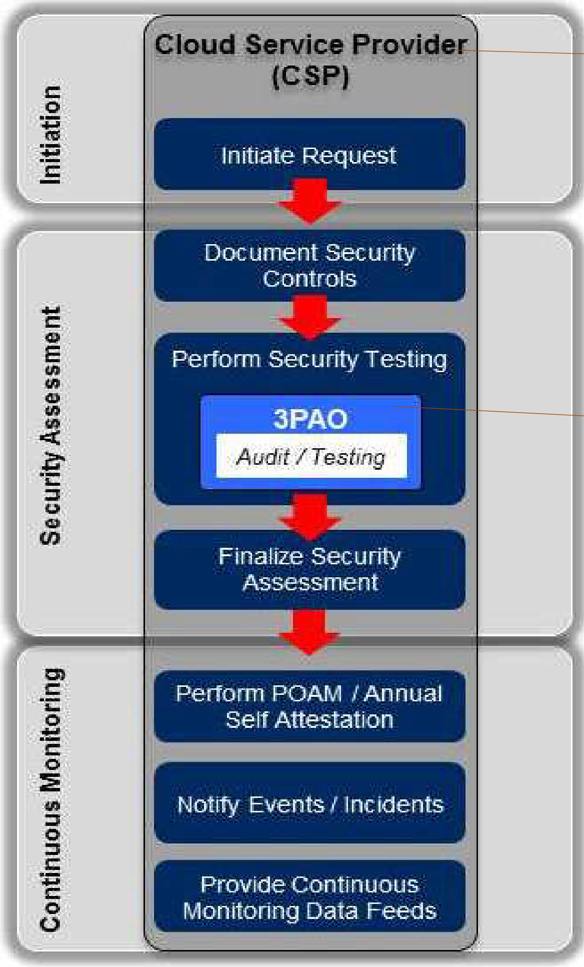
Encryption Standards:

- NIST SP 800-111 for data at rest
- Federal Information Processing Standard (FIPS) 140-2, NIST SP 800-52, SP 800-77 and SP 800-113 for data in motion

FedRAMP – A new standard to consider

Federal Risk and Authorization Management Program (FedRAMP) is a government program that provides an approach to security assessment, authorization, and continuous monitoring for cloud products/services.

- FedRAMP includes security controls and corresponding enhancements based on NIST SP 800-53 that federal agencies and Cloud Service Providers (CSPs) must implement.
- The FedRAMP process and standards can be leveraged for a multitude of known security controls and to provide assurances of the security controls of cloud service providers.


Cloud Service Provider (CSP)
Initiation
Initiate Request
Security Assessment
Document Security Controls
Perform Security Testing
3PAO
Audit / Testing
Finalize Security Assessment
Continuous Monitoring
Perform POAM / Annual Self Attestation
Notify Events / Incidents
Provide Continuous Monitoring Data Feeds

FedRAMP process

Two currently authorized CSPs

18 accredited third party assessment organizations currently

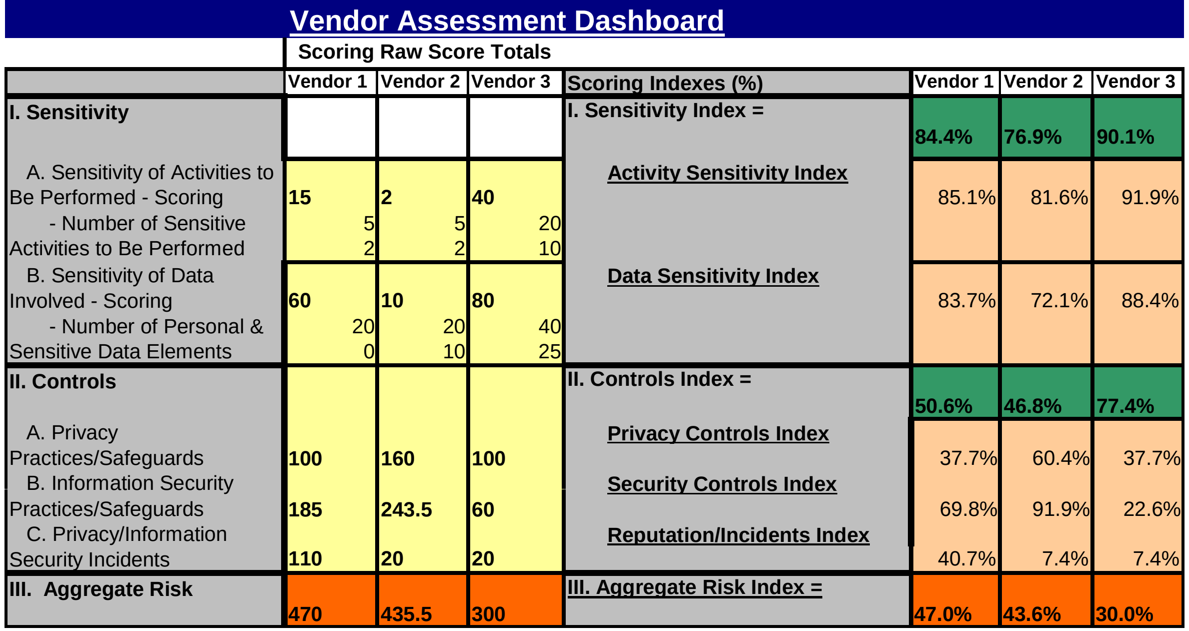
Example - Industry Assessment & Contract Approaches

1. **Develop/Update Standard Contractual Safeguards –** Flexible set of template provisions from which to selectively use as the context and business needs require.
   - Enhanced provisions will integrate (i) the assessment responses as contract representations and warranties and (ii) audit process as ongoing covenant.
   - Trend to increasingly include specific security controls and standards.
2. **Develop/Enhance Short-Form Vendor Pre-Contract Assessment Process or Develop Response Template –** Typically integrated into HIPAA vendor diligence/compliance processes, procurement/contracting or payment process.
   - Most HIPAA vendor assessment processes in industry are solely security focused. The trend in assessments is increasingly broader to also covers privacy, compliance, data handling, record handling, identity theft and reputation.
   - Process typically include risk scoring model correlating risk with vendor maintained safeguards and compliance criteria. See sample reporting/measurement slide.
   - Enhanced assessments (e.g., on-site, SAS70s or other) performed on risk basis.
   - This also creates a Preferred Vendor program concept.
   - Also, companies often entrust with sensitive and regulated information are developing overview statements of their security and privacy programs to be able to quickly answer most routine security and data handling requests.

Example - Industry Assessment & Contract Approaches (continued)

3. **Enhance Onsite Review and Other Activities Based on Vendor Responses** – Based on vendor profile/services or sensitivity of data involved (data elements), organizations may desire to develop a formal risk-based approach to conduct deeper enhanced reviews in addition to conducting assessments with the survey template. Additional reviews may include, but are not limited to:
   - 1-2 day site visits, interviews and document reviews—based on audit template
   - Enhanced site visits, assessments and framework reviews
   - Audit self-assessment and contract representations and warranties
   - Many companies assess a certain percentage of their vendors
4. **Automate Data Collection & Compliance Reporting Processes** – Implement an application to:
   - Automate information collection,
   - Manage and produce reporting of compliance for internal and regulatory processes and
   - Provide analysis on a single vendor or benchmark standards and compliance requirements across all vendors.

Example - Privacy & Security Vendor Management Quantitative Analysis & Scoring Models

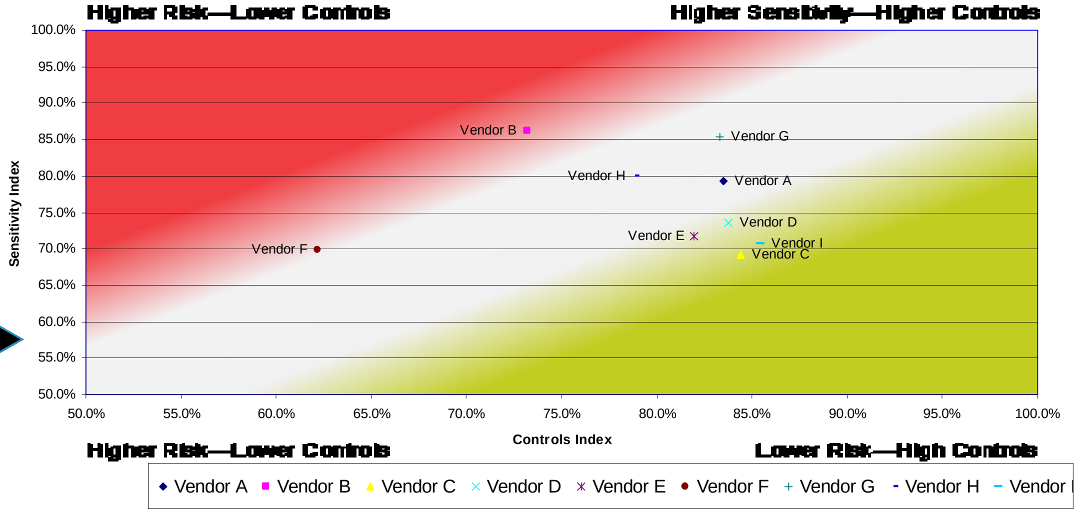


Vendor Assessment Dashboard

	Scoring Raw Score Totals						
	Vendor 1	Vendor 2	Vendor 3	Scoring Indexes (%)	Vendor 1	Vendor 2	Vendor 3
I. Sensitivity				**I. Sensitivity Index =**	**84.4%**	**76.9%**	**90.1%**
A. Sensitivity of Activities to Be Performed - Scoring - Number of Sensitive Activities to Be Performed	**15** 5 2	**2** 5 2	**40** 20 10	**Activity Sensitivity Index**	85.1%	81.6%	91.9%
B. Sensitivity of Data Involved - Scoring - Number of Personal & Sensitive Data Elements	**60** 20 0	**10** 20 10	**80** 40 25	**Data Sensitivity Index**	83.7%	72.1%	88.4%
II. Controls				**II. Controls Index =**	**50.6%**	**46.8%**	**77.4%**
A. Privacy Practices/Safeguards	**100**	**160**	**100**	**Privacy Controls Index**	37.7%	60.4%	37.7%
B. Information Security Practices/Safeguards	**185**	**243.5**	**60**	**Security Controls Index**	69.8%	91.9%	22.6%
C. Privacy/Information Security Incidents	**110**	**20**	**20**	**Reputation/Incidents Index**	40.7%	7.4%	7.4%
III. Aggregate Risk	**470**	**435.5**	**300**	**III. Aggregate Risk Index =**	**47.0%**	**43.6%**	**30.0%**

- Sensitivity Analysis and
- Controls Assessment for Privacy, Security and Reputation

Vendor Privacy & Security Analysis



- Comparative Vendor Analysis
- Review of Proportionality of Risk to Vendor Controls

Ted LeSueur, Director Product Security, McKesson Corp.

Vendor Assurance

- – Overall Vendor Governance
- – The Case for IT Vendor Assurance – Why now?
- – What is IT Vendor Assurance?
- – Benefits to McKesson
- – Key Roles and Accountabilities

Vendor Governance

The IT Vendor Assurance program is aligned, linked and supportive of the Vendor Governance Initiative.

- ✓ The IT Vendor Assurance program is part of the larger Vendor Governance Initiative focused on McKesson’s key strategic vendors designed to:
  - o enhance vendor relationships;
  - o improve vendor governance;
  - o monitor vendor performance against contractual obligations; and
  - o provide a holistic approach to measure vendor performance.
- ✓ The Vendor Governance Initiative will be implemented by tiering vendors into different categories, defining relationship management processes for each tier, developing reporting requirements and metrics; and aligning these processes with McKesson’s defined goals for the vendors.

The case for IT Vendor Assurance
Why now?

Recent trends in outsourcing drives the need for increased vendor assurance

Higher Risk Profiles in Sourcing Arrangement

- Increasing scope and complexity of business activities (i.e. product design, distribution partners, global outsourcing relationships)
- Continuous changes in regulatory requirements and expectations in response to market events
- Increasing risks from technology (e.g. new delivery models such as cloud computing/ SaaS, data vulnerability)

Greater Marketplace 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 considering and managing risk
- Rating agencies require evidence of effective governance, risk management and compliance programs

Strategic consequences exist if McKesson is unable to manage IT vendor risks 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

What is IT Vendor Assurance

- ✓ The IT Vendor Assurance program, creates a risk management framework to provide consistent structure, approach and controls for various IT related risks emanating from McKesson’s reliance upon IT vendors.
- ✓ The objective is to institutionalize the framework to facilitate enhanced evaluation of IT vendor risks and relationships; consistency in reporting; and improved communication of IT risk profiles within each business unit.

Benefits to McKesson

IT Vendor Assurance program provides McKesson:

- ✓ A cross-organizational risk management baseline has been established as a result of surveying and interviewing risk leaders and key stakeholders in each BU to ensure benefit realization
- ✓ A Rapid Risk Rating tool has been developed that supports the BUs in evaluating sourcing risks relative to existing and future sourcing relationships
- ✓ An IT Vendor Assessment Framework has been established to ensure consistency in the management of risk across the enterprise.
- ✓ The implementation of an automated risk assessment and monitoring program that will transition the organization from a reactive to proactive risk management approach (e.g. environmental, strategic/market and operational/execution risks)

By designing a targeted risk classification system with segmented due diligence, McKesson will be able to more effectively match its risk efforts with those vendor relationships that pose the highest potential exposure – with a limited investment of resources.

Key Roles and Accountability

- IT Risk Leaders
  - **Own** BU program and liaison between sourcing teams, CIOs, and IT Vendor Assurance Initiative
  - **Work** to ensure consistency in execution of program and implementing a streamlined IT Vendor Assurance process
  - **Establish** the standard for defining IT vendor risks and integrating within the overall IT vendor selection process.
  - **Monitor and report** on key IT vendor risks and metrics to steering committee

Key Roles and Accountability

- CIOs
  - **Approve** key decisions on IT vendor risk assessment findings, prioritization, and mitigation efforts
  - **Review** key IT vendor risk performance indicators (KRI’s)
  - **Resolve** policy/procedure issues that have been escalated
  - **Approve** key roles, responsibilities, and scope of activities defining the process
  - **Monitor** the refinement of the process function through key performance indicators and standards

Key Roles and Accountability

- IT Vendor Assurance Team
  - **Set** direction and develop framework to implement on IT vendor risk management program
  - I**dentify** key vendor risks, key performance indicators that can be evaluated in partnership with BU risk leaders and CIOs
  - **Create** policy/procedure and training documents
  - Inform BU IT of requirements based on changes in regulatory, market and vendor risks
  - **Support** BU in evaluating IT vendor risks through collaborative partnering and develop an enterprise view of IT vendor risks