

Morgan Lewis

Key Developments in Outsourcing – 2009



July 15, 2009

Introduction

informed

Agenda

time	topic
12:00 – 12:05 pm	Introduction
12:05 – 12:30 pm	Trends 2009 – Hear from an Industry Expert
12:30 – 12:50 pm	What's Hot in General Privacy
12:50 – 1:10 pm	Changes to HIPAA and the Handling of Health Information
1:10 – 1:30 pm	The Aftermath of Satyam – How Companies Are Mitigating Risks Relating to the Financial Viability of Their Providers
1:30 – 1:55 pm	The Evolving Outsourcing Contract – Where Customers Are Focusing
1:55 – 2:00 pm	Questions

Participants



Barbara Melby

Morgan Lewis

Phone: 215.963.5053

Email: bmelby@morganlewis.com



W. Reece Hirsch

Morgan Lewis

Phone: 415.442.1422

Email: rhirsch@morganlewis.com



Michael L. Pillion

Morgan Lewis

Phone: 215.963.5554

Email: mpillion@morganlewis.com



Gregory T. Parks

Morgan Lewis

Phone: 215.963.5170

Email: gparks@morganlewis.com



Jessica R. Bernanke

Morgan Lewis

Phone: 202.739.5447

Email: jbernanke@morganlewis.com



Thomas L. Hall

EquaTerra

Phone: 214.866.0101

Email: thomas.hall@equaterra.com

Outsourcing Trends - 2009

informed

State of the Industry

- **Unrest in the Customer's Marketplace**
 - business prospects
 - access to capital/budgets
 - uncertainty
- **Competition in the Service Provider's Marketplace**
 - globalization realized
 - rise of Indian providers
- **Maturation of Technology, Systems, and Dialogue**
 - cloud computing
 - ERP software systems
 - standardization of business processes
 - terms and conditions (audit, taxes, f/x, data)

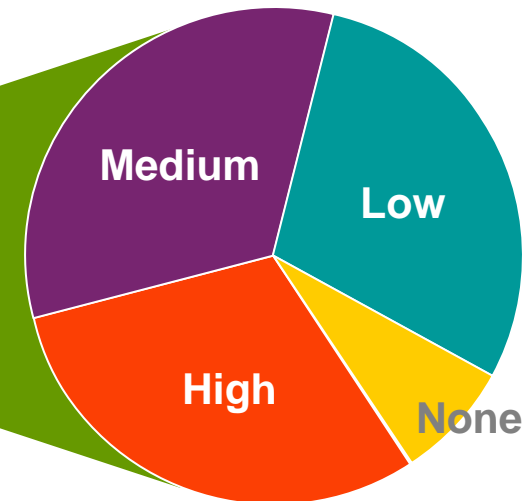
Trends in BPO

Foundation: Adoption of Shared Services

- **Over 80% of Large Companies Have Adopted Shared Services**

- **Of these, nearly two-thirds are operating in a model that is multifunctional and globally integrated**

Level Integrated Across Functions, Geographies, & Business Units



Source: Corporate Executive Board

Trends in BPO

- **Shared Services – driving approach to BPO**
 - migration to and from customer captives
 - geographic scope of solutions, relationships
- **Lessons learned from early adopter full-service HRO**
 - Right-sizing HRO solutions to customers (one size does not fit all)
 - allocation of services among retained organization and outsourcing providers
 - expiration of surviving agreements from early adoption; volume and nature of transactions
- **Allocation of services**
 - between retained organization and providers
 - among providers; best in class
- **Best in class**
 - issue management
 - end-to-end service levels (performance assurance)

Trends in ITO

- **Hardening of Technology**
 - cloud computing
 - storage technology
- **Hardening of Service Provider solutions and standardization of offerings**
 - evolution from lift 'n shift
 - rebidding
 - transformational solutions
 - standardization of offerings
 - provider's service level tiers
 - shared service centers
 - onshore/offshore work allocation and blend
- **Ascension of Indian providers**
 - expanded the field for alternatives
 - breadth of contracting terms and issues

General Trends

- Transformational solutions
 - ERP upgrades/steady-state outsourced service delivery
 - server consolidation, virtualization; clouds
 - migration through captive to outsourced services

General Trends (continued)

- Transformational solutions

- ERP upgrades/steady-state outsourced service delivery
- server consolidation, virtualization; clouds
- migration through captive to outsourced services

For Example



- Global server consolidation, virtualization
 - major ERP upgrade
 - application rationalization
 - geographic/business line waves of consolidation
- Transformation hurdles
 - ERP implementation
 - business line requirements and limitations
 - corporate activity (divestitures)

General Trends (continued)

- **Transformational solutions**
 - ERP upgrades/steady-state outsourced service delivery
 - Server consolidation, virtualization; clouds
 - migration through captive to outsourced services
- **Model for outsourcing transaction**
 - competitive/comparative/collaborative
 - restructuring/rebidding
 - red apples, green apples, and oranges
 - timing of issue management and risk allocation
 - solution development (e.g., security)
- **Transaction costs**
 - struggle between low cost transaction vs. value assurance
 - golf and golfers
 - financing transition costs (whose bank?)

General Trends (continued)

- **Rebidding: shifting issue prioritization**
 - HR transfers vs. SP cooperation
 - socialization of service levels, solution differences
 - governance during transition
 - knowledge retention
- **Transitions**
 - failure rates
 - level of documentation
 - governance

What's Hot in General Privacy

informed

General Privacy Overview

- **Good News** – there is no all-encompassing data privacy statute in the United States
- **Bad News** – there is no all-encompassing data privacy statute in the United States:

Attorney General Enforcement
FTC Act
FCRA
CAN-SPAM
COPPA
Breach Notification Laws
Data Disposal Laws
Gramm-Leach-Bliley
MA Data Security Laws
Red Flags Rule
FACTA

EU “Safe Harbor” Rules
Consumer Class Actions
PCI and DSS Credit Card Rules
Document Retention Requirements
HIPAA
CA Online Privacy Act
Stored Communications Act/ECPA
Do-Not-Call Lists
Telephone Consumer Protection Act
Video Privacy Protection Act
Wire-Tapping Liability

Invasion of Privacy Torts
Data Encryption Laws
Identity Theft Assistance
E-Sign
Computer Fraud and Abuse Act
Communications Decency Act
Spyware Laws
RFID Statutes
FDCPA
Driver’s Privacy Act
Social Security Number Laws
Regulation Z

Data Breach Notification – Federal Law?

- 45 states now have data breach notification laws.
- Generally apply to “owners” of data.
- Laws vary on:
 - Triggering elements
 - Notification requirements – timing, recipients, method
 - Law enforcement involvement
 - Exceptions for encryption, decreased risk
- Federal legislation warranted.
- Has been introduced for last five years, seems more likely now.
- Will generally provide universal regulation.

Mandatory Encryption

- New laws in MA and NV expressly require encryption of “personal information” when it moves.
- Extension of laws in many states requiring “reasonable precautions,” but now more specifics.
- MA rules effective January 1, 2010.
- Requires a “Comprehensive Written Information Security Plan.”
- HR and IT function challenges.
- Retail – compliance with PCI/DSS will generally cover.
- Some likelihood of federal preemption.

But – Federal Preemption in Question

- California has many laws that go beyond scope of corresponding federal law:
 - Unsolicited email advertisements
 - Financial Privacy Act
- Federal law **should** preempt
- Ninth Circuit has held otherwise; Supreme Court so far unwilling to overrule
- Most recent (last week) was Financial Privacy Act
- So, a need to focus on the state-specific laws in California

Red Flags Rule

- Part of FACTA/FCRA
- Applies to (1) financial institutions; and (2) creditors, but with broad definitions. For outsourcers, imposed by contract.
- “Covered account” – personal, family household, or risk of i.d. theft.
- FTC approach – broad application, narrow requirements.
- Identity theft protection program to detect “red flags.”
- Address changes.
- **Enforcement delayed to August 1, 2009. New guidance available.**

Data Privacy Class Actions

- Data privacy and security are increasing focus of plaintiffs' class action lawyers
- Generally following highly publicized data breach
- Lawsuits are weak on damages
 - Identity theft monitoring not like medical monitoring
 - Damages present individualized issues
- Typically rely on negligence theories
- View data privacy, security issues, and crisis management through that lens

Increased FTC Enforcement

- With new administration, increased FTC enforcement was anticipated.
- So far, has not materialized. But, hiring dozens of new lawyers.
- Probably more focus on:
 - General privacy protection, FTC Act
 - Red Flags
 - COPPA
 - CAN-SPAM
 - FCRA
- Also anticipated data privacy law and breach notification law.
- Broad interpretation of own authority, minimal requirements, and focus on “bad actors.”
- Can generally negotiate a consent decree if you act quickly.

HIPAA

informed

Amended HIPAA Privacy and Security

- Amendments to HIPAA Privacy and Security Rules are in The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of The American Recovery & Reinvestment Act of 2009 (ARRA).
- Effective Date: February 18, 2010, except as otherwise noted.

Major Changes in HITECH Act

- Today we will address:
 - Expanded obligations of Business Associates (BAs).
 - Affirmative notification of breach requirements.
 - Increased enforcement and penalties.
- Additional changes include:
 - Guidance on “Minimum Necessary” standard.
 - Prohibition on sale of PHI, and restrictions on marketing.
 - Increased individual rights with respect to certain PHI (applicable to providers).
 - Limited application to Personal Health Records (PHR) Vendors.

Business Associates

- HITECH Act responded to concerns that a wide variety of organizations maintain and transmit PHI, but are not regulated by HIPAA.
- HITECH Act is a game changer with respect to the legal obligations of BAs and this is likely to have a significant impact upon outsourcing arrangements.
- Prior to HITECH Act, BAs were not directly regulated under HIPAA.
 - Subject to privacy and security restrictions pursuant to required BA agreements.
 - Only contractual remedies were available to covered entities for breach of the BA agreement.
 - Unless the BA also happened to be a covered entity, in which case a breach of a BA agreement could result in sanctions.

Business Associates and the Security Rule

- Security Rule Obligations – Under HITECH Act, BAs must comply with the HIPAA Security Rule’s administrative, technical, and physical safeguard requirements.
 - Essentially the same compliance obligations as a covered entity.
 - Newly strengthened HIPAA civil and criminal sanctions apply.
- Effective Date: February 18, 2010.

Business Associates and the Security Rule

- **New BA obligations will include:**
 - Implementing written policies and procedures that address each Security Rule standard.
 - Implementing a security awareness and training program for workforce members.
 - Designating a security official.
 - Conducting a security risk analysis, coupled with a security management process.
- **Covered entities have often attempted to effectively “pass through” Security Rule standards to outsourcing companies.**
 - HITECH Act provides further support for rigorous security due diligence of outsourcing vendors.

Business Associates and the Security Rule

- Large BA organizations, such as outsourcing companies, are likely to already have implemented a comprehensive security compliance program.
 - However, program still may not be fully aligned with Security Rule requirements.
- Smaller BAs, particularly those that are not exclusively dedicated to the healthcare industry, may have a lot of work to do.
- The good news – the Security Rule represents a flexible standard that is consistent with prudent risk management practices.

Business Associates and the Privacy Rule

- Different than approach under Security Rule.
- Requires a BA to only use or disclose PHI consistent with obligations under a BA agreement with a covered entity.
 - Provisions of BA agreement dictated by Privacy Rule.
- Violation of a BA agreement will be a violation of HIPAA (and subject to new, enhanced sanctions).

Business Associates and the Privacy Rule

- The additional privacy requirements of the HITECH Act that are applicable to covered entities will also apply to BAs (Section 13404(a) of ARRA).
- Seems to refer to new privacy requirements relating to:
 - Access to electronic health records (EHRs)
 - Accounting of disclosures from EHRs
 - New “minimum necessary rule” standards
 - HITECH’s limitations on marketing
 - Prohibition on sale of EHRs and PHI
- It appears that each of these new requirements must be reflected in the BA agreement.
- Will a general incorporation by reference work or should each requirement be specifically addressed in the BA agreement?

Business Associates and Security Breaches

- BAs must notify covered entities of any breach of which they become aware.
- BA is not required to notify individuals.
- BA agreements will be required to include a confusing array of breach notification provisions:
 - Notice of unauthorized uses and disclosures of PHI (Privacy Rule)
 - Notice of “Security Incidents” (Security Rule)
 - Notice of “Breaches” (HITECH Act)

Organizations Transmitting PHI

- Clarifies that organizations that provide data transmission of PHI for covered entities and that require routine access to PHI are BAs.
- Doesn't really modify existing BA rules.
- Specifies that health information exchange organizations, regional health information organizations, e-prescribing gateways, and PHR vendors who provide PHRs as part of a CE's PHR all **may** be BAs.
- Seems to emphasize that the exception for "conduits" is not that broad.

Amendment of Business Associate Agreements

- Additional privacy and security requirements imposed upon BAs must be incorporated into the BA agreement.
- Potentially very burdensome given the number of BA agreements entered into by most HIPAA-covered entities.
- New BA obligations are imposed by force of law, not contract; so, are BA agreement amendments really necessary?
- Susan McAndrew of HHS Office for Civil Rights (OCR) has stated that OCR is working on a proposed rule over the summer that will be issued later this year.
 - A model of a BA agreement on the OCR website is expected to be updated at some point.

Amendment of Business Associate Agreements

- What should you do if you are entering into an outsourcing agreement that will have a term that runs through February 2010?
 - Incorporate provisions now that are likely to meet HITECH Act requirements?
 - Execute an amendment prior to February adding HITECH Act provisions?
- One consideration favoring early amendment:
 - New security breach obligations imposed on BAs will become effective by September 18, 2009 (or sooner, depending on when HHS issues final regulations on the subject).

Affirmative Notification Obligation

- **Pre-HITECH Act Rule:**
 - No affirmative obligation to notify individuals or HHS of a breach of HIPAA Privacy or Security Rules.
 - But, covered entities' obligation to mitigate any harm caused by a breach may have included notification of breach.

Affirmative Notification Obligation

- Under HITECH Act, if security of “Unsecured PHI” is “breached,” covered entity must provide notice without unreasonable delay and within 60 days after “discovery” of breach:
 - **To the impacted individuals.**
 - **To the media:** If breach involves more than 500 individuals in a state or jurisdiction.
 - **To HHS:** If breach involves more than 500 individuals, immediate notice to HHS; if less than 500 impacted individuals, covered entity logs breach and provides annual log to HHS.
- If BA discovers breach, it must notify the covered entity, but it may be possible to delegate notification obligations to BA.

Notice of Breach – Content

- **Notice of Breach must include:**

- Brief description of breach, including dates.
- Description of types of Unsecured PHI involved.
- Steps impacted individual should take to protect against potential harm.
- Brief description of steps covered entity has taken to investigate incident, mitigate harm, and protect against further breaches.
- Contact information.

Definition of “Unsecured PHI”

- **“Unsecured PHI”** is PHI not secured through use of a technology or methodology identified by HHS as rendering the information unusable, unreadable, or indecipherable to unauthorized persons.
- **Notification obligations are only triggered by breach of “Unsecured PHI.”**

Definition of “Unsecured PHI”

- HHS guidance will identify the technologies and methodologies that “secure” PHI:
 - Identified technologies and methodologies are intended to be exhaustive, not illustrative.
 - Use of the HHS-identified technologies and methodologies is not required, but such use will act as a “safe harbor.”

Definition of “Unsecured PHI”

- On April 17, 2009, HHS started the process of defining “Unsecured PHI.” It issued initial guidance identifying two acceptable methods for securing PHI:
 - Encryption (electronic PHI at rest, in use and in transmission).
 - Destruction (electronic and hardcopy PHI).
- HITECH Act directs HHS to issue final interim regulations defining “Unsecured PHI” by no later than August 16, 2009.
- Notice obligations will apply to breaches discovered on or after 30 days following the date regulations issue.

Increased Enforcement Mechanisms

- **Periodic Audits.**
Effective Feb. 2010.
- **“Willful Neglect.”**
 - Audit required if preliminary investigation of complaint indicates “willful neglect,” and HHS is required to impose a penalty for violations due to willful neglect.
 - Effective Feb. 2011 (regs. expected in Aug. 2010).
- **State Attorneys General.**
Authorized to bring a civil action for HIPAA violations to enjoin violations and seek limited damages on behalf of residents. Effective immediately.
- **Mechanism for Individual Recovery.**
Regs. to issue by Feb. 2012, and effective on or after date of regulations.
- **Annual Reports to Congress.**

Increased Tiered Penalties

- **Increased Tiered Penalties:**
 - Tier 1: If person is not aware of the violation (and would not have known with reasonable diligence), penalty is at least \$100/violation, not to exceed \$25,000 for all violations of the same requirement in the same year.
 - Tier 2: If violation is due to “reasonable cause” (but not willful neglect), penalty is at least \$1,000/violation, not to exceed \$100,000 for all violations of the same requirement in the same year.
 - Tier 3: If violation is due to willful neglect and is corrected in 30 days, penalty is at least \$10,000/violation, not to exceed \$250,000 for all violations of the same requirement in the same year.
 - Tier 4: If violation is due to willful neglect and is not corrected in 30 days, penalty is at least \$50,000/violation, not to exceed \$1.5 million for all violations of the same requirement in the same year.
- **Effective Date:** Increased penalty amounts apply immediately. “Willful neglect” provisions not applicable until February 2011.

Lessons from the Satyam Fraud

informed

The Satyam Fraud

- What Happened?

- Satyam was India's fourth largest IT services company after TCS, Infosys, and Wipro.
- On January 7, 2009, Satyam's chairman admitted to massive accounting fraud.
- Fictitious cash balance of more than \$1 billion (94% of the cash that Satyam had listed as assets in its most recent financial disclosures). Satyam had significantly inflated its revenues, operating margin, and accrued interest, and significantly understated its liabilities.
- Stock price crashes.
- Indian government took over the company to prevent damage to India's outsourcing industry.
- Employees left to competitors. Issue: possible degradation in quality of services.

The Satyam Fraud

- What Happened?

- Customers reviewed contract options and some terminated (e.g., State Farm)
- Sale to Tech Mahindra, a joint venture between the BT Group and the Indian conglomerate Mahindra & Mahindra (\$1.2 billion acquisition of 31% of the company, with an option to purchase an additional 20% at market price at a later date)
- The two founders, the CFO, and four other employees face criminal charges, as do two PricewaterhouseCoopers former partners
- Lawsuits have been filed against PricewaterhouseCoopers by Satyam investors claiming that the fraud should have been found
- Satyam is recovering – has regained half of its lost value and is now seventh largest Indian IT firm

Review Your Contract

- Customers Need to Review Their Outsourcing Contracts
 - Not just those with Indian IT vendors
- What Rights and Remedies Are Available?
- What Protections Are in Place?

Termination for Cause vs. Convenience

- Termination for Cause
 - Typically no termination fees
- Termination for Convenience
 - Typically a termination fee and wind-down costs
- Termination for Material Breach – Rarely a “clean” right
 - Contributory causes by customer
- Solution – Include some rights to terminate for clear “causes” on the part of vendor

Cause – Vendor’s or Guarantor’s Financial or Regulatory Issues

- Do the Applicable Contract Provisions Cover the Correct Entity?
 - Affiliates? Guarantor?
- Vendor’s or Guarantor’s Bankruptcy
 - Generally not enforceable under U.S. law
 - We understand that generally enforceable under Indian law

Cause – Vendor’s or Guarantor’s Financial or Regulatory Issues

- **Governmental or Regulatory Action or Investigation**
 - E.g., “Vendor [or Guarantor] becomes the subject of any action or investigation by any governmental authority or regulatory agency which (A) in Customer’s judgment could render Vendor unable to provide any of the Services in accordance with the requirements of this Agreement [or Guarantor unable to fulfill its obligations under the Guaranty], or (B) involves material fraud or financial irregularities by or on behalf of Vendor [or Guarantor] or any illegal activities by or on behalf of Vendor [or Guarantor].”

Cause – Vendor’s or Guarantor’s Financial or Regulatory Issues

- Downgrade in Credit Rating

- E.g., “a downgrade by one or more of the three leading rating agencies in the [United States at that time (collectively, the “Ratings Agencies”) (which, on the Effective Date, are Standard & Poor’s Ratings Services, Moody’s Investors Service, and Fitch Ratings)] that results in any of Vendor’s [or Guarantor’s] publicly or privately traded securities having a rating below investment grade.”

Cause – Vendor’s or Guarantor’s Financial or Regulatory Issues

- Breach of Specific Financial Covenant

- Customer may terminate this agreement, in whole or in part, if on the final day of any of Vendor’s (Guarantor’s) fiscal quarters Vendor’s (Guarantor’s) tangible net worth is less than \$_____.
- Also include covenant of Vendor to deliver calculation of Vendor’s (Guarantor’s) tangible net worth as of the last day of each fiscal quarter, certified by the chief financial officer of Vendor (Guarantor.)
- Need to define tangible net worth – e.g., consolidated total assets of Vendor (Guarantor) and its direct and indirect wholly owned subsidiaries less (a) all liabilities that should, under GAAP, be classified as liabilities on Vendor’s (Guarantor’s), consolidated balance sheet, and (b) goodwill, intangible items, notes, obligations owing by officers or other affiliates, and reserves not already deducted from assets.

Cause – Vendor’s or Guarantor’s Financial or Regulatory Issues

- **Material Adverse Change Involving Vendor or Guarantor**
 - E.g., “any material adverse change in or effect on the Vendor or Guarantor” but excluding the effect of changes that are (i) generally applicable to the IT services industry, the [Indian] economy or the [Indian] securities markets or (ii) a result of the outbreak of major hostilities, a terrorist attack or the declaration by [India] of a national emergency or war.
 - Less definitive

Cause – Other Rights to Terminate

- Change of Control of Vendor/Guarantor
- Vendor's Breach of Service Level Commitments
- Breach of Workforce Turnover Limitations
- Breach of Key Employee Restrictions

Termination for Convenience (Termination Fee)

- Is There an Option for the Customer to Terminate for Convenience?
- How to Exercise?
- Avoidance of Fight over Whether a Breach Has Occurred

Other Rights and Remedies to Consider

- **Switch Business to Another Vendor**
 - Exclusivity covenant?
 - Deemed termination for convenience upon reduction in service volume?
- **Step in Rights**
 - Customer, or third party on behalf of customer, “steps in” and takes over the services for a period of time when there has been a disruption in services or breach in service level agreement

Key Issues upon Termination or Migration to New Vendor

- Intellectual Property (IP) Rights
 - Does the customer have complete copies of all of the categories of IP?
 - How is this material transmitted, stored, and secured?
 - Is the source code in escrow, if any, up to date?
- Transfer of software ownership rights upon development, rather than delivery or payment
- Be sure that applicable IP rights assignments are in place

Key Issues upon Termination or Migration to New Vendor

- **Customer Data**
 - Data retransfer provisions requiring delivery of customer data on demand or periodic data delivery requirements
 - Vendor's obligations to protect data so that it is not improperly disclosed or transferred in any attempts to salvage vendor or its assets

Key Issues upon Termination or Migration to New Vendor

- **Non solicitation and No-Hire Covenants**
 - Does the contract prevent the customer (or its designee) from soliciting or hiring some or all of vendor's personnel working on the account?
 - Right to hire if only non solicit?
 - Applicable for the duration of the term or only for specified periods of time?
 - Does covenant apply depending upon type of termination (e.g., not applicable if termination for cause)?
 - Immigration law issues

Key Issues upon Termination or Migration to New Vendor

- Termination Assistance (to Customer and Its Designees)
 - Time period
 - Costs
 - No degradation in services
 - Customer right to acquire hardware?
 - Is vendor obligated to work only with customer or must it also work with any new supplier designated by customer?

What's New in Outsourcing Contracts

informed

Customers Are Focusing On...

- Privacy
- Flexibility
- Transparency
- Accountability
- Transformation
- Due Diligence
- Financial Terms
- Good Governance

No Surprise – Privacy (and Security)

- **Customers Are Better Informed**
 - Due to focused internal security resources
 - Evolution of how to best comply with EU and state requirements
 - Internal requirements are being passed down to service providers
- **Key Area of Focus - Encryption**
 - Why?
 - Environments to consider
 - Supplier and customer PCs
 - Data in transit
 - Data at rest.
 - Backup tapes
 - May depend on customer's capabilities

No Surprise – Privacy (and Security)

- **Changes to Requirements**
 - Who monitors legal requirements; when does the customer pay?
- **Liability**
 - Security breaches
 - Evolving standards
 - Personal information vs. other information
 - Direct vs. Indirect
 - Cap?
- **Sample Provisions**

Sample Provision

Data Safeguards – Personal Information

[General Requirement] Supplier shall have implemented and shall maintain appropriate operational technical, and organizational measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Supplier shall regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems, and procedures. Supplier periodically shall identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the Personal Information, and ensure that there are safeguards in place to control those risks. Supplier shall monitor all Supplier Personnel for compliance with its security program requirements.

Sample Provision

Data Safeguards – Personal Information

[General Requirement] Supplier acknowledges that the Customer Data may contain Personal Information, the use of and access to which is subject to various privacy laws, including EU Directives, member state, federal and international Laws, and state, federal and national or international government agency orders and decrees to which Customer may be subject (“**Privacy Laws**”), as well as certain restrictions imposed on the Customer Data by the data subjects or other third-party data providers. Supplier agrees to strictly abide by all such restrictions pertaining to the Customer Data, as they are promulgated and applied, currently and in the future, and to implement appropriate mechanisms to comply therewith. Furthermore, Supplier shall in good faith (i) execute any and all agreements that Customer is required to have Supplier execute in order for Customer to comply with any Privacy Laws and (ii) execute, implement or obtain any agreements, documents, notices or consents that are required for Supplier to comply with Privacy Laws. If Supplier’s use (whether directly or indirectly) of the Customer Data is contrary to any Privacy Law or any of the restrictions set forth in this Agreement, Customer shall have the right to terminate this Agreement for cause if such breach has not been cured within **XXX** days of receipt by Supplier of written notice and/or pursue any other legal and equitable remedies. At Customer's request, Supplier shall demonstrate the adequacy and validity of all mechanisms in place to implement compliance with Privacy Laws.

Sample Provisions

Data Safeguards – Personal Information

[Data from Map] Supplier has provided a mapping of where Customer Data (by data type if applicable) is located and from where Supplier shall access or transfer such Customer Data in connection with the performance of the Services. Such mapping is attached as the data flow map in **XXX**. Any changes in such mapping shall be subject to Customer's approval pursuant to the Change Control Procedures.

[Personal Requirement] Supplier shall conduct appropriate background investigations of Supplier Personnel, as provided in Section XXX. No Supplier Personnel shall be given access to the Personal Information until such investigation is complete and the results are acceptable. Additionally, Supplier shall conduct reasonable privacy and information security training, as appropriate, for those Supplier Personnel who Process the Personal Information. Supplier shall require any Supplier Personnel who Processes the Personal Information to sign, and annually affirm in writing, an enforceable confidentiality agreement that includes requirements to keep the Personal Information confidential.

Sample Provision – Liability in Connection with Data Breach Provision

Notwithstanding any other provision of this Agreement, Supplier shall reimburse Customer on demand for reasonable and customary out-of-pocket costs and expenses incurred by the **[Customer Group]** to the extent attributable to any violation of Supplier's duties hereunder with respect to safekeeping of Customer Data or Personal Information of members of the **[Customer Group]** ("**Reasonable and Customary Costs**") consisting of the following **[Customer Group]** external costs and expenses associated with addressing and responding to the violation: (i) preparation and mailing or other transmission of legally required notifications; (ii) preparation and mailing or other transmission of communications to customers, agents, or others required by Law or required or recommended by a Governmental Authority or agreed to by the Parties as a reasonable mechanism for mitigating the breach; (iii) establishment of a call center or other communications procedures in response to such violation (e.g., customer service FAQs, talking points, and training) not to exceed **XXX** days or such longer time required by Law or required or recommended by a Governmental Authority or agreed to by the Parties as a reasonable mechanism for mitigating the breach; (iv) reasonable legal and accounting fees and expenses associated with the **[Customer Group's]** investigation of and response to such event; (v) costs for commercially reasonable credit reporting services not to exceed **XXX** months or such longer time required by Law or required or recommended by a Governmental Authority or agreed to by the Parties as a reasonable mechanism for mitigating the breach; and (vi) all claims for government fines, penalties, and interest imposed by a Governmental Authority.

Flexibility

- With all of the changes in the market, customers are looking for FLEXIBILITY
- Structure
 - Master agreement
 - Ability to handle global scope
 - Ability to handle acquisitions and divestitures
 - Ability to handle downturn in business and growth
 - Consider in context of IP licenses
- Term
 - Trend seems to be shorter term with renewal rights
- Termination
 - Right to descope parts of the services without penalty
- Cooperation in a multisource environment

Sample Provision

Provision of Services to Divested Entities

If Customer relinquishes control of all or part of (i) a business unit or Affiliate or (ii) a particular property or other facility of any member of the **[Customer Group]** after the Effective Date (each such entity, plant, or facility, a “**Divested Entity**”), then upon Customer’s request, Supplier shall continue to provide the Services to such entity after the date such entity becomes a Divested Entity for a period of time requested by Customer, which period shall not exceed **XXX** months at the rates and in accordance with the terms and conditions set forth in this Agreement. If the Divested Entity agrees in writing to abide by the terms and conditions of this Agreement **[and the Divested Entity satisfies Supplier’s reasonable and consistently applied financial viability standards]**, then Customer (and, if applicable, members of the **[Customer Group]**) shall be relieved of any payment or other liability relating to the provision of Services to the Divested Entity. In all instances, Supplier shall provide Termination Assistance Services to the Divested Entity as requested by Customer or the applicable Divested Entity.

Sample Provision Non-Exclusivity

This Agreement shall be nonexclusive and each member of the **[Customer Group]** may in its absolute discretion enter into arrangements with third parties to provide all or part of the Services, subject to **[Reference Pricing Exhibit]**, and any New Services. **[The Customer Group]** reserves the right to perform itself, or retain third parties to perform, any of the Services and any New Services. The Fees shall be equitably reduced to reflect agreed cost savings to Supplier resulting from Supplier's ceasing to provide the Services no longer required to the extent Supplier realizes a cost savings.

Sample Provision

Cooperation with Third Parties

To the extent Customer or any member of the **[Customer Group]** performs any of the Services or any New Services itself, or retains third parties (“**Customer Third-Party Contractors**”) to do so, Supplier shall fully cooperate with the **[Customer Group]** or any Customer Third-Party Contractors in connection with this performance as may be necessary for such performance, including (i) providing system, process, or service-related documentation and access to facilities, systems, processes, and interfaces used to provide the Services; (ii) providing written requirements, standards, and procedures for Customer Systems operations maintained by Supplier so that the enhancements or developments of such third party may be operated by Supplier; (iii) providing such information regarding the operating environment, system constraints, and other operating parameters as a person with reasonable commercial skill and expertise would find reasonably necessary for Customer or a third party to perform the applicable services; and (iv) integration activities to achieve compatibility of systems/products/services and the success of the total solution.

Transparency – It is Time to Lift the Curtain

- A shift away from – “Suppliers are delivering to SLAs so there is no need to micro-manage”
- Personnel projections
 - The data provides visibility and the starting point for a dialogue
- Onshore/offshore ratios
- Succession planning
- Turnover
- Approval on service locations
- Approval on subcontractors
- A view of “financials”
 - Don’t be the last to know

Sample Provision Staffing Plan

Supplier's staffing plan and solution (by name, role, level of experience, and location) as of the **[Effective Date]** shall be attached as **XXX**. On a quarterly basis, Supplier shall furnish its actual staffing against such plan and solution for all of the **[Towers]**.

Sample Provision Turnover

Supplier shall use commercially reasonable efforts to keep the turnover rate of Supplier Personnel performing the Services to a level comparable or better than the industry average for large, well-managed IT services companies. Supplier shall implement and maintain a program designed to retain the Supplier Personnel on the Customer account during the Term. If Customer believes that Supplier's turnover rate of Supplier Personnel performing the Services is excessive, Supplier shall provide data to Customer concerning the turnover rate, discuss the reasons for the turnover rate, submit its proposals for reducing the turnover rate, and agree on a program to reduce the rate at no charge to the **[Customer Group]**. For the purposes of this Agreement, the Parties agree that an annual turnover rate at or over is presumptively excessive, and Supplier shall promptly inform Customer in the event that such a rate is experienced.

Greater Accountability to More Stakeholders – Audit and Compliance

- Greater audit and compliance review than ever before
- Robust compliance provisions
- Get stakeholder review and sign off early
- Seeing a lot of dialogue regarding compliance with internal controls
- SAS 70 – when is it needed?
- Audit assistance – what level is included?
- Laws and outsourcing – what should the customer know about?
 - Offshore laws
 - New U.S. laws
- Understanding import/export responsibility
 - Offshore access may = export
 - Landed resources with access = export

Sample Provision Audit

Supplier shall provide to **[Customer Auditors]** access at all reasonable times and after reasonable notice to any facility or part of a facility at which Supplier is providing the Services, to Supplier Personnel providing the Services, and to data and records relating to the Services for the purposes of performing audits and inspections of the **[Customer Group]** and their businesses to verify the integrity of Customer Data and to examine the systems and infrastructure that process, store, support, and transmit that data. The foregoing audit rights shall include, when applicable, audits of (i) practices and procedures, (ii) systems and infrastructure, (iii) security practices and procedures, (iv) disaster recovery and backup procedures, and (v) other areas necessary to enable Customer to meet applicable Laws.

Sample Provision Audit Cooperation

Supplier shall cooperate with the **[Customer Group]** or their designees in connection with audit functions and with regard to examinations by regulatory authorities.

Supplier shall notify Customer promptly by telephone or by email if a Governmental Authority requests an inspection or makes written or oral inquiries of Supplier regarding any aspect of Customer's activities pursuant to this Agreement or of any Supplier Site. Unless otherwise required by applicable Laws, Supplier shall not allow access to any Governmental Authority relating to such activities without giving Customer the right to have a representative present.

Sample Provision Audit Cooperation

Supplier and Customer shall cooperate in resolving any concerns of any Governmental Authority. The escalation path for regulatory issues shall be defined in this Agreement. Supplier shall cooperate with, and participate in, any Customer investigation.

Supplier shall provide use of Supplier Sites and resources for the performance of audits at no charge to the **[Customer Group]** or their auditors.

For the avoidance of doubt, reasonable audit cooperation is part of the Services (including participation from accountants and other Supplier Personnel) and shall not be counted against resource utilization and shall be provided at no charge to the **[Customer Group]**.

Sample Provision Internal Controls

Supplier shall comply with the **[Customer Group's]** then-current key internal controls, including Customer's **[Security Procedures]** (the "**Customer Controls**"). Supplier shall comply with any changes to the Customer Controls as requested or approved by Customer.

In addition to Supplier's other obligations hereunder, and as part of the Services at no cost to Customer, Supplier shall review and respond to quarterly and other inquiries regarding compliance with Customer's internal controls and, as requested by Customer, certify compliance with such controls.

Sample Provision Import/Export

Supplier (a) acknowledges that certain software and technical data to be provided hereunder and certain transactions hereunder may be subject to import and export controls under the Laws of the United States and other countries and (b) shall monitor all such Laws. Supplier shall not import or export or reexport any such items or any direct product thereof or undertake any action in violation of any such Laws. With respect to software or technical data provided by Customer or **[Customer Group]** to Supplier hereunder that is proprietary to Customer (and not licensed from a third party), Customer shall provide specific information reasonably requested by Supplier to permit Supplier to determine the export authorizations and licenses required and shall reasonably assist Supplier with making any required filings and obtaining necessary export authorizations.

Transformation

- Lift and shift vs. new environment
 - New doesn't always mean cutting edge
 - **Before** transformation meant moving infrastructure and environments forward; **now** we are seeing that, **as well as** some customers looking to standardize and move to a leveraged environment
- Seeing more ERP implementations integrated with the outsourcing initiative
- Refocus on change management
- Need to understand payment structures → T&M vs. Milestone payments
- Need to understand → The impact if the transformation doesn't happen or is not successful
 - Consider making transformation benefits a **requirement**
 - With consequences for not achieving
- An example: server consolidation project

Due Diligence

- Customers want to go into deals with their eyes open, and with an understanding of potential financial exposure
 - Enhanced due diligence
 - Limitations on due-diligence adjustments
- Employment Issues
 - Background checks (where is it not allowed?)
 - Drug testing
 - Hiring requirements
 - At the front end
 - Hiring rights
 - At the back end

Due Diligence

- Existing Relationships – More movement from incumbent supplier to next (as opposed to customer personnel to supplier)
 - Due diligence
 - Assess the cost impact
 - Timing
 - Termination fees
 - Assess the impact to your organization

Sample Provision

Termination of Existing Supplier Contracts

Upon the Commencement Date (or the actual transition of service if later and subject to any other rights that Customer may have), the following contracts: _____ (the “**Supplier Terminated Contracts**”) shall terminate and all services provided by Supplier under such Supplier Terminated Contract shall be assumed by Supplier under this Agreement as part of the Services. Customer shall not be responsible for any termination fees, wind-down costs, or other charges or expenses associated with the termination, and Supplier hereby waives any minimum commitment, right to bid (or similar rights), termination notice, or other payment- or termination-related provisions in the Supplier Terminated Contracts.

Financial Terms

- It is all about the pricing (not a new concept)
- Payment due date
 - Cost of \$\$ is real \$\$ - Suppliers are negotiating hard
 - Customers have tough standards to follow
- Inflation risk
 - United States vs. offshore
- Currency risk
- Stale invoices
 - Need invoices because need to be aggressive in budget planning
- Responsibility for taxes

Sample Provision Stale Invoices

Customer shall not pay any invoices issued by Supplier or any third party more than XXX days after the provision of the applicable Services.

Last Words – Good Governance

- The best contract in the world won't mean much without good governance
- State of the industry is evolving → need to be aware
- More regulation and oversight by internal and external groups – accountability to many stakeholders
- Greater need to adapt to change → know what your needs are; know what your contract says
- Good governance means staying informed
 - Customers need to keep an eye on the issues and potential impact
 - Gone are the days of turning over the keys and walking away
 - “Partnership” is key

Questions



informed

Upcoming Webcasts

- October 7, 2009

Re-Negotiating and Re-Sourcing: Pointers for Fixing Deals that Aren't Working and Re-Aligning Your Outsourcing Strategy

- January 13, 2010

Transformational Transactions: Using Technology to Transform Your Business - A Fresh Look at ERP Implementations, Automation Projects and Beyond



worldwide

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston
Irvine London Los Angeles Miami Minneapolis New York Palo Alto Paris
Philadelphia Pittsburgh Princeton San Francisco Tokyo Washington