

Emerging Challenge: Risk Management in an Outsourced World

By Karen Wilson, JD, CCEP

Executive Summary

Accounting fraud at outsourcing giant Satyam and terrorist attacks in Mumbai and Jakarta should resonate with risk managers in any organization that outsources or is thinking about it. While it's unlikely these events have tarnished outsourcing permanently or outsourcing providers as a whole, they emphasize the need to have a disciplined risk management and governance framework to select a provider and manage the relationship over the long term. Even without the red flags, companies who outsource are well-advised to examine their risk management standards and adjust them to account for the decision to turn over control of mission-critical functions to another party who delivers services from a foreign country.

For hundreds of U.S. companies, investments in outsourcing and offshoring are more important than ever to achieve strategic and financial goals. Outsourcing can simplify modernization, shift risks, and give buyers access to integrated system solutions. A growing reliance on outsourcing to deliver core business processes and knowledge-based services also increases risks and alters their scope and impact. Outsourcers are in control of key business operations and interface directly with clients and their employees and customers, very often from offshore sites.

On the eve of reform legislation and at a social and economic tipping point, healthcare services in America are poised for fundamental change. Payers and providers undergoing this transformation are expected to look to outsourcing as a way to upgrade IT capabilities quickly and offload back office operations and costs. Outsourcing also facilitates around-the-clock clinical support from locations like India where low-cost medical professionals read radiology reports and review CT scans for U.S. providers and patients.

Until now, healthcare has lagged other industries in adopting outsourcing as

part of an overall management strategy. This is changing, but before making the move or recommitting to outsourcing, healthcare organizations should undertake a comprehensive review of the risks, including performance, reputation, security, legal, financial, and competitive factors associated with offshore outsourcing. This assessment is more complicated because clinical and administrative processes alike are candidates for outsourcing and their risk profiles are different. A risk common to all outsourcing relationships and considered a leading cause of their failure is the lack of effective oversight and governance. Outsourcing governance is critical to manage the provider in ways that advance the objectives of the outsourcing initiative through its lifecycle. Without good governance, there's a greater chance an outsourcing strategy will be considered a failure because it did not deliver expected results.

Despite its challenges, outsourcing's time has come in the healthcare industry. Risk

managers, auditors and others focused on risk have an essential role promoting a dialogue focused as much on risk and relationship management as it is on cost savings. Outsourcing is an opportunity for healthcare organizations to take a reasoned approach to risk and advance the principles of enterprise risk management in doing so. Intelligent risk management and sound governance practices won't guarantee the venture's success, but they will greatly improve the odds that an outsourcing strategy was the right decision for a healthcare organization.

The State of Outsourcing *"There is a profound and impassioned stigma associated with outsourcing."*

The International Institute for Outsourcing Management, January, 2009

The state of outsourcing in 2009 is generally good, with the trend to outsource remaining steady in the current recession. In 2008, the IT and Business Process Outsourcing (BPO) segments generated \$600 billion in contract signings, and the Everest Institute projects that annual contract value for finance and accounting deals will grow at a 20% rate annually for the foreseeable future.

Some believe the global economic crisis will encourage protectionism and reduce demand for offshore services, at least temporarily, especially as wage gaps narrow and geopolitical dynamics evolve. If this is correct, providers who have relied on wage arbitrage as

"There is a profound and impassioned stigma associated with outsourcing."

their primary value proposition will feel the effects. To compete, they will either become commodity providers of low value services or change their business model from one based on standardization and cheap labor to one based on productivity, efficiency, and quality. It also compels clients, especially those receiving financial assistance from government agencies, to improve how they select and manage outsourcers and offshore operations. These developments contribute significantly to the success of an outsourcing strategy and can actually increase its use over the long term.

The most successful outsourced functions are those with rules-based, repeatable actions that can be wholly or partially performed by technology integrated in a streamlined workflow requiring fewer resources, less time, or both. Jobs like data entry and payroll processing were commonly outsourced in the early years. Today, a range of business processes are candidates for outsourcing, including information technology, claims processing, human resources, supply chain management, logistics, customer care, facilities management, procurement, transcription, billing, coding, and collection services. Since the late 1990s, the Internet has allowed companies to outsource higher-value services traditionally performed in-house, such as financial reporting, accounting, auditing, legal and engineering support, and tax preparation. If this practice continues, it could change assumptions about outsourcers as being low-cost providers because highly-educated workers no matter where in the world they are change risk profiles and drive up costs.

For some, outsourcing is a handy way to unload expensive, poorly-managed operations that sap resources and distract attention from the core business. In outsourcing parlance, this is known as 'my mess for less' and is usually a reliable predictor of failure. When structured and managed properly, however, outsourcing offers tangible value and real strategic advantages for an industry under the gun to change quickly and dramatically.

Healthcare Outsourcing—Why Now?

"It's axiomatic that outsourcing needs to be part of the equation hospitals and other

institutions consider. To meet the burgeoning needs piling up at the door of every healthcare institution in America, these organizations need to look beyond their own four walls for solutions."

Affiliated Computer Services, Inc., 2008

Just as many industries have embraced the benefits of outsourcing, healthcare organizations are recognizing its potential in both clinical and administrative areas. Historically, the healthcare industry has been slow to realize outsourcing's advantages or view it as part of a business strategy. Outsourcing challenges traditional relationships between patients and physicians. Nonetheless, healthcare institutions increasingly are choosing outsourced solutions, in particular IT, human relations, and coding and billing on the administrative side and transcription services and CT/MRI scan review on the clinical side.

Hastening the move to outsourcing is healthcare reform legislation, which was being debated in Congress at the time this article was written. Regardless of the law's final form, it will result in new healthcare standards that make cost reductions, particularly back office, and integrated technology solutions more urgent than ever. Healthcare organizations will be forced to upgrade their clinical and IT capabilities and administrative processes to stay competitive and remain eligible to participate in government-funded programs.

Another driver for outsourcing is the decline in profits that physicians and providers are experiencing as they treat more patients and make less money. This is due to skyrocketing costs, managed care models, and changing entitlement programs. The time and cost to process claims and byzantine authorization requirements create a vicious cycle that turns providers into creditors and diverts resources from the mission of delivering healthcare services. In extreme cases, it can threaten the provider's very existence.

A major challenge addressable by outsourcing is the growing burden of regulatory compliance. Healthcare is one of the most heavily regulated industries in the U.S. Laws and regulations change frequently and can be difficult to interpret and apply. Adding to this, outsourcing complicates compliance and can trigger legal requirements that didn't exist before. Together, they create a perfect storm of legal compliance headaches for providers and payers already struggling with anti-fraud, conflicts of interest, and privacy imperatives.

Oversight Requirements

Changes in the outsourcing industry itself have made attention to regulatory risk more important. Buyers are outsourcing more knowledge-based functions with complex regulatory requirements embedded. They expect the provider's systems and policies to be compliant with Sarbanes-Oxley, Payment Card Industry

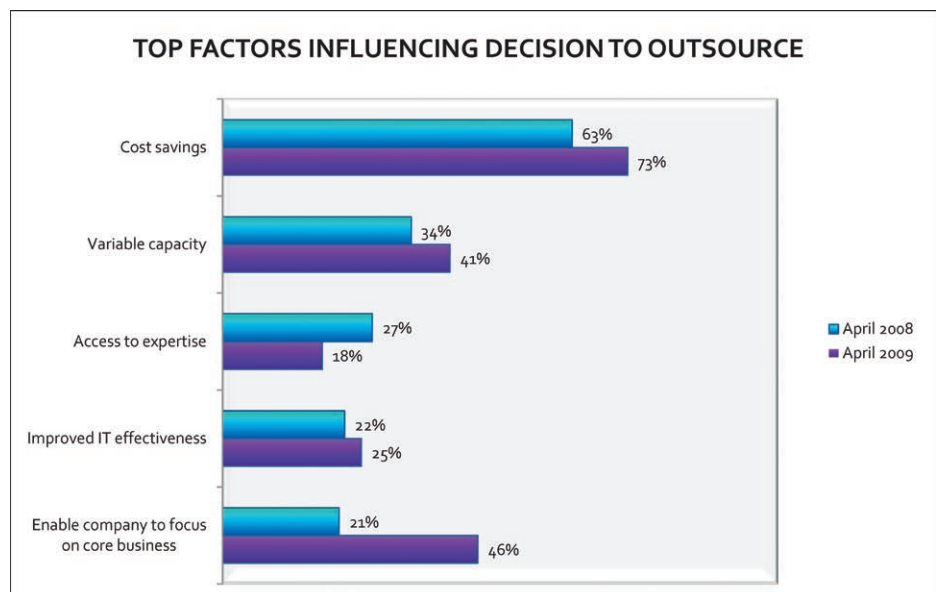


Table 1

Competitive & Strategic Risk	Operations & Performance Risk	Legal & Regulatory Risk	Financial Risk	Security & Privacy Risk	Reputation Risk
<ul style="list-style-type: none"> • Product and service delivery failures • Quality gaps & inconsistency • Conflicting priorities of provider and customer • Customer service degradation • Depleted talent pipeline • Loss of institutional knowledge & skills • Poor morale among remaining personnel • Failure to consider enterprise risks • Disclosure of confidential information • Promised IT improvements do not materialize or are over-hyped, over budget, or both • Inadequate metrics • Reliance on provider's expertise • Questionable or unknown stability of provider • Government-imposed limitations on outsourcing & offshoring • Geopolitical risks • Lack of exit plan 	<ul style="list-style-type: none"> • Non-integrated IT systems • Poorly defined requirements • Transition delays • Excessive changes • Overly optimistic or unachievable financial and operational objectives • Failed handover of employees from buyer to provider • Poor morale, high attrition and layoffs • Culture clashes • Unfamiliar systems, processes, and tools • Unforeseen effects of changes in workflow processes • IT outages • Software infringement claims by client's vendors • Inadequate or untested disaster recovery and backup capabilities • Customer's existing standards and procedures poorly defined and difficult to transition • Customer's business records under provider's control • Lack of consistency, transparency in processes • Inadequate metrics • Provider's use of agents and subcontractors • Poor oversight & governance • Exit barriers 	<ul style="list-style-type: none"> • Provider unfamiliar with industry-specific laws • Provider unfamiliar with foreign laws • Embedded legal risks overlooked or ignored • Provider's lack of compliance resources and know-how • Reliance on provider's policies and standards • Buyer's policies not adapted to outsourcing • Poorly-defined duties • Changes in laws and policies not addressed in the contract • Under-developed foreign IP laws • Software infringement claims by customer's vendors • Vague or non-existent incident management protocols (e.g. data security breach) • Injunctions or other government actions affect operations • Customer's liability to third parties for provider's actions • Provider's representations to regulators on customer's behalf • Customer's business records under provider's control • Lack of "smart" email archive system & retention rules. • Transfers of PI and PHI between the US and foreign jurisdictions and disclosures to third parties 	<ul style="list-style-type: none"> • Aggressive financial models with overly optimistic projections and unrealistic time-frames • Complicates cash flow and financial reporting • Negative effects on SOX compliance • Ill-defined or poorly implemented financial controls • Hidden costs of unforeseen events (fines, penalties, change orders) • Underestimating severance, layoff costs • Miscalculating transition time and costs • Unbudgeted vendor costs, software license assignments • Intangible costs of transition delays, poor production, worker slowdown • Underestimating or disregarding the cost of governance & oversight • Failure to audit invoices and enforce Service Level penalties and favored nations pricing • Unknown exit costs 	<ul style="list-style-type: none"> • Provider unfamiliar with industry-specific standards • Poorly defined physical and IT security standards • Transfers of PI and PHI between the US and foreign jurisdictions and disclosures to third parties • Data security/privacy policies are not adapted to outsourcing • Lack of data inventory showing content and locations of PHI and PI • Failure to implement IT security controls, firewalls, bug fixes • Lack of transparency & uniformity in procedures • IT outages • Provider's PCI compliance • Inadequate or poorly defined data breach response protocols • Unknown or untested disaster recovery capabilities • Unauthorized representations & communications on customer's behalf 	<ul style="list-style-type: none"> • Failures in service delivery that affect patients' health or lives • Provider's bad acts and noncompliance are imputed to the customer • Mismanagement of PHI and PI causes high-profile data security breaches • Negative public and investor perception of outsourcing

Table 2

Legal Risks in Outsourcing Transactions*							
Common Outsourcing Practices	Intellectual Property	Data Privacy & Security	Records Management & E-Discovery	Consumer Protection/ Anti-Fraud	Employment & Labor/ Immigration	International Trade (OFAC, Export-Import, FCPA)	Software Infringement
• Offshore Operations	•	•	•	•	•	•	•
• Foreign Labor	•	•	•	•	•	•	•
• Shared Systems & Software	•	•	•	•	•	•	•
• Common Processes & Tools	•	•	•	•	•	•	•
• Subcontractors & Agents	•	•	•	•	•	•	•

*Does not include industry-specific laws and regulations.

- Direct risk
- Indirect risk

Data Security Standards (PCI), and SAS-70, as well as industry-specific standards like HIPAA, which now extends to outsourcers who were not previously covered as Business Associates. Outsourcers meeting the definition of a bank service company are governed directly by the Bank Service Company Act and are subject to examination and regulation as if they were insured banks.

To design adequate controls for a sourced environment, healthcare organizations need to understand their providers' service model, data flow, and third party contractors. They must know where, how, and by whom services are performed and understand the controls that are in place to provide services in conformance with the law. They should know what policies apply and what happens when they change. They should require protocols and transparency when the provider is responding to data security breaches. High-risk operations should be regularly audited to examine workflow processes, review documentation, and interview employees. Contract administration must have built-in controls to manage invoices, payments, and penalties and track a considerable number of change orders, especially in the build-up to transition. When it's all said and done, healthcare organizations don't outsource their duties to patients and regulators. They are responsible for compliance and the consequences of noncompliance, even if the bad act occurs on the outsourcer's watch.

For Want of a Nail—An Enterprise of Risk

“ERM is designed to enable leaders across the organization to be risk aware, not risk adverse.”

*Director of Enterprise Risk Management
H.J. Heinz, Inc., 2009*

New healthcare programs will affect how patient care is delivered and back office functions are managed. An outsourcing strategy can support this change quite nicely, but not without a commitment to risk management that doesn't vanish the first time financial targets are missed. Enterprise risk management (ERM) is based on an objective understanding of the totality of risks across the enterprise and replaces the practice of managing risks in silos where the full extent of risk to the organization is not understood or appreciated. A holistic view of risk is the best and maybe only way executives can make informed choices about major decisions, like whether to outsource, that preserve and advance stakeholder value. Furthermore, fallout from the financial crisis has many regulatory bodies adopting meaningful changes to risk oversight responsibilities for boards and management, which increases the importance of ERM capabilities.

Outsourcing is well-suited for ERM because its risks are interconnected and span operating units and disciplines. An IT failure touches every department in a hospital, both clinical and administrative. It also increases the potential of peripheral risks like data security breaches and impedes the use of tools like billing systems and email. Risks in isolation may not be overly concerning; the effect of combined risks, however, can be overlooked and devastating. The outsourcer's failure to meet export/import requirements can delay the

delivery of equipment and software critical to support client needs from offshore sites. This affects implementation schedules and delays the client's plans to expand services. The outcome can negatively impact strategy and growth, which may be reflected in investor uncertainty and lower stock values.

Despite the benefits of ERM, companies have been slow to adopt its holistic approach. Deciding whether and what to outsource is a great setting to change this and advance ERM principles at the same time. Auditors, risk managers, lawyers and compliance officers are natural champions of ERM and understand intuitively why it's critical in an outsourcing initiative. They have a comprehensive nose for risk, even if they are specialists, as many are, or work at companies that lack formal ERM processes, as most do today. They have access to audit reports, hotline complaints, insurance claims, litigation and other sources of risk history. Through field audits and investigations, they are familiar with policies, practices, and management in the operations. They talk to executives and the board and can explain outsourcing risks in the context of the organization's overall risk picture. Simply put, it's a great way to add value, contribute to the success of the outsourcing initiative, and advance the interests of ERM.

There's also an important risk management role through the life of the relationship. Outsourcers are assumed to be world-class experts in the client's regulatory requirements and

business practices. That's a tall order considering most outsourcers have clients in every major industry segment. Outsourcers specialized in healthcare services are plentiful, but specialists or not, expertise and execution must be tested regularly. Internal audit should include outsourcing as a category of risk in annual audit plans. Formal risk assessments should be undertaken periodically, and high-risk activities targeted for examination. The assessments supplement, not replace, monitoring done by the outsourcing governance team and should be conducted in coordination with it. Compliance officers and in-house lawyers are great resources for expert help designing regulatory controls and monitoring practices. In fact, a slice of the organization's compliance program is outsourced along with business processes, so the compliance office and legal department should be eager to contribute.

“ERM is designed to enable leaders across the organization to be risk aware, not risk adverse.”

Audit Focus

Audits should focus on activities with low transparency or those with weak or unknown controls, with a special emphasis on offshore operations. Areas with merged staff, high turnover, or a history of misconduct are good candidates for review. Training, checklists and other aids may be needed to prepare audit staff, including instruction on basic legal requirements of the activity being reviewed. Follow-up should be the responsibility of individuals on the relationship team, who are evaluated on their performance. Outsourcing governance protocols are well-suited for monitoring and reporting status until open items are resolved and audits are closed. Material findings should be reported to management and the board of directors as appropriate.

Another reason audits are important is the growing number of regulations that require monitoring practices to prevent and detect illegal conduct. The USA PATRIOT Act anti-money laundering rules require independent audits to test controls, as do EPA regulations and OIG

standards for healthcare organizations, which mirror the Federal Sentencing Guidelines (FSG). In fact, the FSG Advisory Group adopted the criteria of the Health Care Compliance Association for effective monitoring of a compliance program. The HCCA recommends regular audits reflecting the organization's size, complexity, and risk profile. Audits should be conducted by independent auditors and be part of an audit plan. Major audit findings should be reported to management and the board and corrective actions undertaken and tracked until they are completed.

Collaboration is needed among risk, governance, and relationship teams to identify the highest-risk practices where the likelihood of a violation is high and the impact serious if one occurs. A particularly important risk right now is the outsourcer's ability to locate and

- Readiness to comply with e-discovery requests in litigation and other matters involving client records.
- System capabilities for managing records and email (e.g., document database, email archive).
- Policies and retention schedule(s), including email, used for managing records.
- Backup and disaster recovery policies and practices.
- Location and media of client records.
- Procedures for destroying records, including identity of any vendors used.

If offshore sites and workers are included in the service model, export/import know-how and resources can make the difference between on-time and delayed implementations. Offshore operations are subject to laws of foreign jurisdictions where they are located. Failure to comply with employment, health & safety, immigration, zoning, tax, and other en country regulations can disrupt operations and affect service delivery.

Another area rich with audit potential is the provider's use of subcontractors and vendors. Outsourcers outsource, too, and many times use unsuccessful bidders as subcontractors. Benefits management, HR, and finance and accounting: each

retrieve electronic records and email under its control consistent with new federal discovery rules. For best results, a records management audit should be coordinated with the legal and IT departments and examine the:

Table 3

Ineffective Governance Leads to Lost Value	Effective Governance Leads to Added Value
<ul style="list-style-type: none"> • Disputes about duties • Excessive reliance on contract and executive management • Low trust and lack of communication • Decisions based on incomplete data • Poor execution • Lack of transparency • Need for frequent change orders • Unforeseen risks • Client dissatisfaction 	<ul style="list-style-type: none"> • Collaborative strategic planning • High level of trust and free flow of information • Structured dispute resolution & change control • Easy access to data • Responsiveness & mutual respect • On-time, on-budget projects • Informed risk management • Achievement of outsourcing goals • Customer satisfaction

is subject to a host of standards specific to it like ERISA, SOX, and SAS-70. And these examples don't scratch the surface of regulatory risks in outsourced clinical functions, a many-headed hydra beyond the scope of this article. The point is, there's plenty of risk to manage in an outsourcing arrangement.

Governance is the Key

Even the most well-considered ERM strategy is not a substitute for good governance. How clients manage their outsourcing relationships has an enormous impact on value and risk. Experts say that when governance is ignored or shortchanged, the result can be a 30 to 70% decline in expected returns of both parties, making them equally dependent on good governance to achieve desired results. But don't expect an outsourcer's objectives to be aligned naturally with the client's. Outsourcers are in the business of outsourcing for a profit. Buyers want to offload non-core functions and get more for less. Complex services add expense and process and are at odds with outsourcing's traditional value proposition. Shorter-term contracts put pressure on outsourcers to recoup start-up costs quickly, and shortcuts and delays can be signs of misalignment.

Outsourcing governance is more than service level penalties and platitudes like 'we believe in partnering'. Governance is important in outsourcing for the same reasons it's important in corporations—transparency, accountability, oversight, strategy development, and risk management. The simple objective of outsourcing governance is to make sure the outsourcing strategy is aligned with long-term corporate objectives and the relationship is delivering expected benefits to both parties. Without governance practices, the parties waste time arguing about unmet expectations

and ambiguous duties or resort to hyper-technical interpretations of the contract as the court of last resort. This undermines trust and stymies communication about topics like new strategies and tools for advancing business objectives and reaping more value from the relationship.

Organizational models for governance are customized to match the culture and structure of the company. Many believe that placing outsourcing governance functions under a corporate executive like the CFO or CIO promotes transparency and decision-making at appropriately senior levels. Include a requirement in the RFP for the provider's governance model, and be suspicious of those who don't have one or have one that's limited to contract management tasks. Members of governance teams should be full-time and have appropriate experience and training. Avoid the mistake of assigning former process owners to governance roles; they are inherently conflicted and can be counterproductive. Consider evaluating and compensating the governance team based on the value derived from improved strategy, leveraged capabilities, and managed change rather than on flawed financial models and unachievable objectives.

Outsourcing governance starts before ever engaging providers or issuing RFPs. The organization should conduct interdepartmental due diligence of processes, workforce, and costs of operations targeted for outsourcing and test assumptions about how, and how well, they are done today. Typically there are gaps in policies and accountability that must be addressed. Include all stakeholders from the beginning so everyone with an interest has a say in defining objectives and setting financial targets. Proper scoping of outsourced processes is the foundation for decoupling them from the mother ship. Every

interdependency must be considered to reveal hidden costs and transition roadblocks. Detailed financial modeling is critical to an outsourcing strategy but of little use if it ignores or underestimates the totality of risks to the enterprise. A lack of reliable metrics is common, too. If metrics exist, they're usually too narrowly concentrated on quantitative data and must be adapted to a sourcing strategy that emphasizes qualitative measurements as well. It's easy to see why auditors and others focused on risk are so important in setting and managing controls and supporting the governance team through the life of the outsourcing relationship.

Conclusion

Execution, not service penalties or pricing, is the source of most of the value and risk of outsourcing. Thinking about risk using an ERM framework is the only way to navigate the added uncertainty and loss of control that outsourcing creates. Relationship building is crucial to execution the same way an unambiguous contract is crucial to defining duties. For those contemplating outsourcing, informed risk management and a commitment to good governance will set the stage for a long-term relationship based on value, shared goals, and mutual trust. **NP**

Karen D. Wilson, JD, CCEP is a business attorney and compliance professional with 24 years experience practicing law and managing corporate Compliance & Ethics programs. Ms. Wilson was formerly the Senior Vice President & Chief Compliance Officer for a Fortune 500 company where she managed the Office of Legal Compliance that was responsible for the company's global compliance affecting 60,000 employees in 30 countries. In 2008, Karen formed Citadel Compliance Group, LLC. which provides comprehensive services for compliance & ethics programs. She may be reached at information@citadelcompliance.com, or at 972-447-0271.

There is nothing so useless as doing efficiently that which should not be done at all.
~Peter Drucker