Reprinted from PHARMACEUTICAL ENGINEERING®
The Official Magazine of ISPE
November/December 2010, Vol. 30 No. 6
www.ISPE.org

This article discusses risks and mitigation strategies that need to be considered between healthcare companies and outsourced IT suppliers.

IT Outsourcing and Offshoring: Recognizing and Managing Risk

by Arthur D. Perez, PhD and Glenn Morton

Introduction

Hardware is less expensive although we are using more if it. The power of the internet has led to the rise of third party data centers that can serve many client companies so well that users are not even aware that the equipment and staff are no longer in the basement of their building.

Software is more powerful, and we are more reliant on it. Software suppliers have recognized the needs of healthcare companies, so there are now frequently multiple commercially available applications to perform functions where once the lack of choice meant that user companies had to develop their own software. As a result, healthcare companies may be able to employ a smaller staff of software developers. At the same time, this means that they may not have the resources to do occasional software development to meet unique needs or to gain a market edge.

These conditions have led to a proliferation of contracts between healthcare companies and outsourced IT suppliers for both infrastructure management and software development. This article discusses many of the risks and mitigation strategies that need to be considered when engaging such partners. Some of these risks are unique to our industry, and some are generic to any company looking for an IT services partner. GAMP® 5[1] includes an appendix describing some outsourcing issues, and this article focuses on risks that need to be managed prior to and during an engagement.

IT service has increasingly been seen in the past decade as a commodity, and as companies search for ways to focus business energy and resources on core activities, they often turn to outsource partners, both domestic and foreign, as a way of reducing costs and effort on non-core activities. The burden on regulated industries such as healthcare increases the challenge to getting this right.

Why Outsource?

The biggest driver, which is probably greatest for smaller firms, is the difficulty in funding and supporting staff with the expertise for management and execution of IT tasks. Even large firms with hundreds of IT staff cannot match the economies of scale achievable by a huge IT services company. Such providers are able to consolidate computing resources and staff functions to a degree that no healthcare company can hope to match. They may be able to manage a 10-fold larger data center for only double the cost of that at a large pharmaceutical firm.

In addition, the large global IT service companies can leverage the cost benefits of conducting operations in countries with low labor costs, an option not available to firms whose data centers are located in Europe or North America. India, for example, while having labor costs a fraction of those in Europe and North America, actually has a larger, better educated labor pool of IT professionals than do those regions. In theory, leveraging these economies should eventually lead to improved service.

Outsourcing also provides the healthcare company with greater flexibility to execute projects. Doing a major global SAP upgrade? Add 50 ABAP programmers for a year. Closing a manufacturing site? Reduce the support to the appropriate level.

Disadvantages to Outsourcing/Offshoring IT Services

As with any outsourced activity, control is surrendered. There is also a considerable reduction in transparency into how activities are executed.

These factors require a degree of trust that some regulated companies may find difficult to grant.

Finding the right service level in contract negotiations can be tricky. If requirements are too great, the savings are reduced. If too little, the IT Department risks the wrath of users, possibly requiring bringing in additional resources at increased cost, resulting in unhappy users and reduced savings. If the outsourced partner decides to change internal business practices, this also can have a large effect on the regulated company, possibly introducing increased risk and unanticipated expense.

The bottom line is that lower apparent cost can be a very seductive lure into an outsourcing arrangement. Failure to completely understand and evaluate the client firm's needs vis à vis the contracted firm's capabilities can easily erase anticipated cost reduction.

It's All about the Data

As recently as 15 years ago, electronic data was reasonably secure simply by virtue of the fact that it was fairly isolated. Data from manufacturing, quality control results, clinical studies, and various other critical information generally resided on a hard disk in the corporate data center and was inaccessible to non-employees or anyone outside the company network. This is clearly no longer the case.

Today, information is shared within the company across multiple sites, and some of it may be transmitted over public infrastructure (most company WANs involve the internet). Contract employees may have access to the company network via their own PCs. The proliferation of media like USB flash drives means that even if they don't have direct access, they may have indirect access through full time employees, who may share data in unapproved ways. The bottom line is that there are a number of pathways for company data to find its way onto a contractor's laptop, where the company has no effective control over it.

Companies also may share data with other companies who provide services, e.g., a trucking company that needs distribution data or a Clinical Research Organization. Outsourced IT service providers may have company data on their own servers. This is complicated enough with domestic partners, but becomes even more so with off-shore partners who are bound by different national laws. Nowhere is the difference in national laws more apparent than the highly critical and highly visible problem of protection of Personally Identifiable Information (PII). This clearly affects healthcare companies who must handle clinical study records, employee records, etc.

Finally, there is the case of the business partners of business partners. The trucking company mentioned above may contract out their IT services so that an unwary healthcare company's data may be residing on equipment belonging to a firm they have never heard of.

Three Principal Risks to Data

There are three points of concern regarding data that must be protected when considering engaging an outsourced partner:

1. **Integrity:** the data is what it is and it needs to remain that way. For example, audit trails must remain intact, precision and accuracy must be preserved, and of course

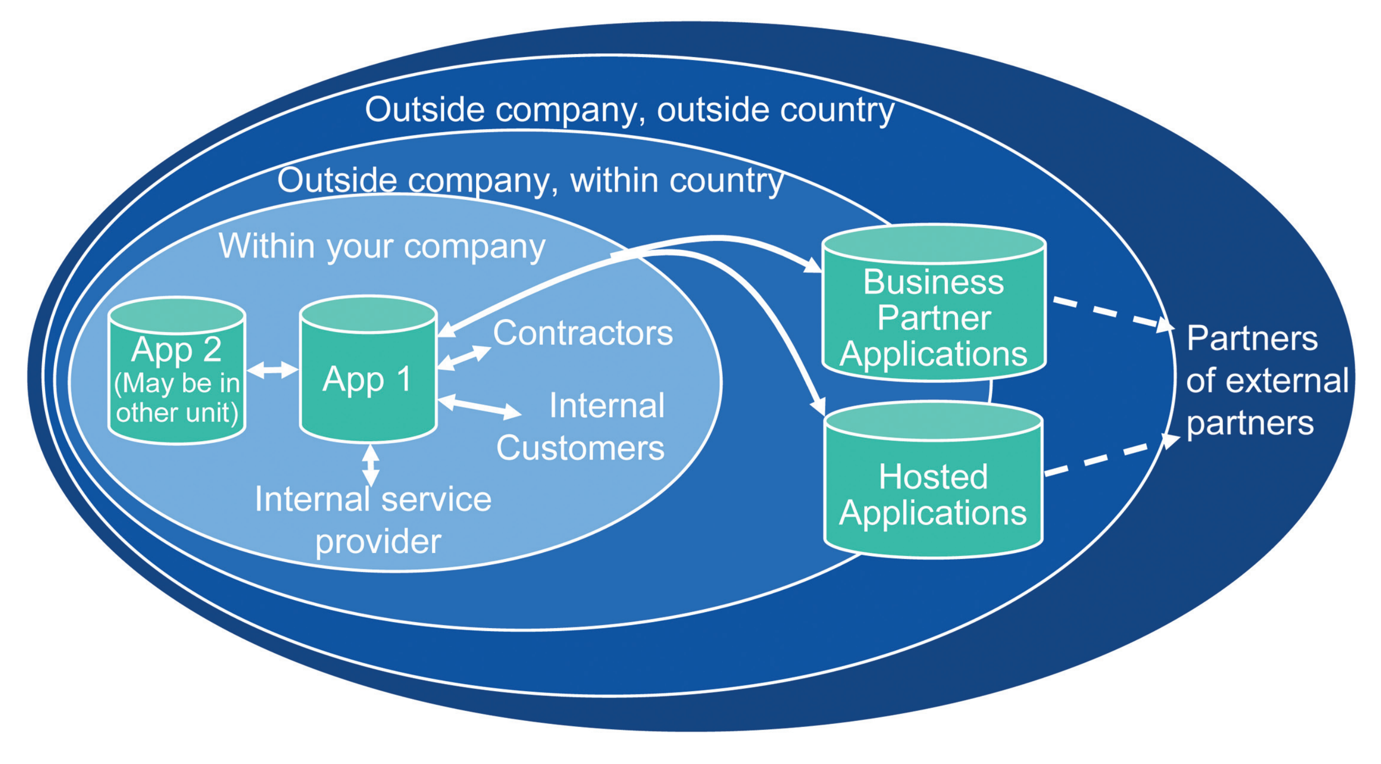
Outside company, outside country
Outside company, within country
Within your company
App 2
(May be in other unit)
App 1
Contractors
Internal Customers
Internal service provider
Business Partner Applications
Hosted Applications
Partners of external partners

Figure 1. It's all about the data: who has it, who can access it, and how is it protected?

records must not be lost or deleted until their retention period is over.

2. **Availability:** the data needs to be available when it is needed, where it is needed, and only to those with a legitimate need for it.
3. **Confidentiality:** some data are exceptionally sensitive and it is essential that it is protected from unwarranted exposure. This includes Intellectual Property (IP), PII, privileged attorney-client communications, and a range of other business information.

Five Risk Areas

Understanding that these are the issues of focus, there are five areas where risk needs to be evaluated.

- Governance
- Country
- Company
- Contract
- Nature of Contracted Work

The remainder of this article will examine these risk areas in detail.

Risk #1: Governance

Governance is essential to ensure that the contracting healthcare company has some visibility into all activity and related risks, adherence to the contact terms, and to identify changes to the services to support business needs. There are a variety of approaches to achieving that, ranging from close supervision and reporting to reliance on auditing. The approach will depend heavily on the degree of trust between the parties. Ideally, the contracting company should be confident that the partner adheres to standard processes, makes optimum use of available resources and tools, and manages risks appropriately, including notification of the client when critical incidents occur. Effective governance also will play a very large role in the identification, mitigation, and control of risks in the other four areas.

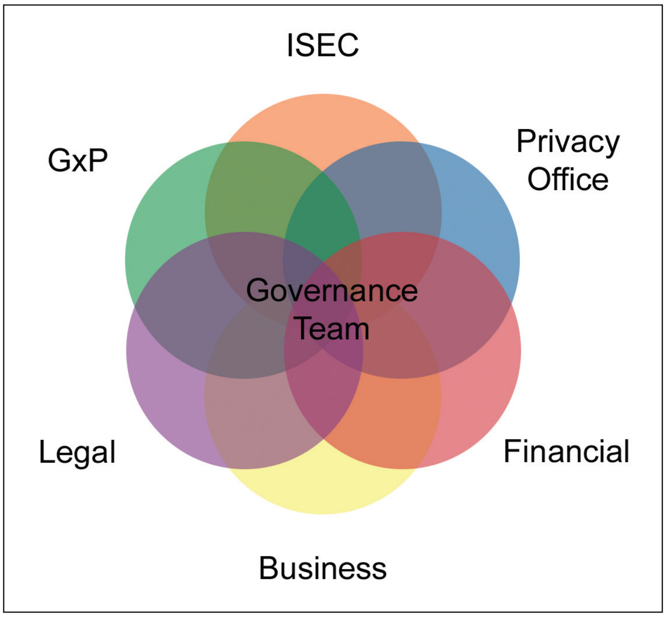

Figure 2. Governance includes wide scope of responsibilities.

Governance scope must include all divisions and geographic locations and cover IT, information protection, and related activity initiated in business units. Governance practices must include participation from all relevant/interested parties, documentation of activities, and reporting of results - *Figure 2*. To be effective, the governance team must have full understanding of laws and regulations in all affected jurisdictions.

Risk #2: Country

Legal/Regulatory

It is important to understand how national laws may affect the manner in which engaging an outsourced partner should be approached. In general, as Figure 3 illustrates, in the absence of strong national laws protecting corporate information, the contracting healthcare company will probably need to introduce some risk mitigation. Stronger laws generally provide more protection and will mean less mitigation is needed.

Specific laws and regulations that need to be considered obviously include GxP regulations, which are fortunately fairly uniform around the world. Protection of Intellectual Property (IP), on the other hand, is not uniform. In some nations, IP is not patentable. If there is an information breach, this could cost the company millions or even billions. Another consideration relates to compulsory licensing. Could the government of the nation where the data resides force the business partner to release information for use by a local low-cost manufacturer?

Data privacy laws vary greatly between nations. EU laws are generally more protective than US laws, while India is less protective than the US. Even within the USA, the requirements of state laws concerning data privacy differ substantially. It is imperative that the company understands what data is involved and what the laws are concerning that data in both the country where the data is stored or manipulated and in all of the jurisdictions where the people it concerns reside. If adequate controls cannot be established, in order to comply with the pertinent law, it might be necessary to keep a database with PII internal to the healthcare company rather than outsource its management.

Financial regulations, such as the US Sarbanes-Oxley law, may introduce additional risk. For example, if a control requires limited access to data, and an IT service supplier wants its entire UNIX Support staff of 70 to have admin rights on the servers with the financial applications, there is obviously a disconnect related to understanding of the controls required to comply with US law that needs resolution.

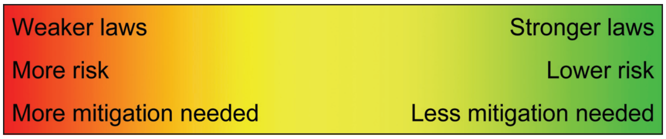

Figure 3. Laws that protect your data generally mean you'll need less risk mitigation.

Finally, rules regarding e-discovery in support of legal suits need to be understood. For example, US law is quite clear regarding protection of information falling under attorney client privilege. This right may not exist in other countries. Therefore, the corporate legal department should be involved in structuring any outsourcing agreements.

Any of the above factors could influence mitigation actions ranging from encryption of sensitive data to a decision not to store or use certain data in some countries.

Other Country Risks

When evaluating an offshore partner, other factors not related to the data should be considered:

- Is the legal system generally regarded to be efficient and independent of politics?
- Is the tax policy clear or is it possible that the contracting company could be hit with a large and unanticipated tax increase? Is one partner counting on a tax break that may suddenly disappear, leaving the contracting company with a large unanticipated expense, or a partner who can no longer afford to operate?
- Are there dangerous macroeconomic factors? Is the local currency unstable or does the country have an unsustainable dependence on foreign aid? Is the balance of payments a threat to government stability?
- Is there a danger to security in the form of potential for war, insurrection, terrorism, or violent crime?
- Is the government politically stable? Could it turn unfriendly?
- If the government is friendly and stable, is it effective? Could there be problems with corruption or conflicting vested interests?
- Does the country have a stable infrastructure (electric power, phone, internet, roads, etc.) capable of meeting business needs? Is it unusually vulnerable to disaster?
- Does the labor market meet business needs? Is there a plentiful supply of workers with the needed skills? Are workers generally happy or unhappy? Are there national laws preventing layoffs? Does the country's legal infrastructure enable effective pre-employment background checks?

Mitigating Country Risks

Strategies for addressing country-specific risks primarily involve a very deep effort at due diligence. When evaluating offshore partners, the healthcare company's strategic sourcing department must be involved. It is also strongly recommended to involve the Legal Department, possibly including outside counsel with knowledge of the country in question. There are consulting firms that specialize in evaluating risks like this, and engaging such a firm may be beneficial. Industry research sources and careful perusal of news reports also can contribute to the decision process. When negotiating the contract, some protections designed to mitigate country risks can be included. For example, requiring approval before allowing data access by contractor staff in another country will offer the ability to assess whether the new country's IP and data privacy laws are adequate, and to intervene if they are not.

This ultimate decision when evaluating country risk often comes down to "Do we want to do business here?" However, there may be some other levels of mitigation that will allow the engagement, such as restricting the type of work that can be done at a particular location or adding additional data protection like encryption.

Risk #3: Company

Not all potential partners are created equal. Some companies are better run, some are more stable, and some very good ones are hungry and looking to make a deal that will get them the work. Unfortunately, some are also poorly run or don't take compliance seriously, or both.

When evaluating an outsourcing partner, it is important first and foremost to understand how stable the company is. If a firm is contemplating moving its data center operations to an outsourced facility, those doing the planning had better be reasonably sure that their partner is not going to declare bankruptcy, dismiss the staff, and sell off all of the servers. This will involve thorough due diligence work prior to commitment, plus continual monitoring of the financial stability of the company. Corporate leadership at the partner should be evaluated for stability and effectiveness as well. A company that has had three CEOs over a two-year period may have some very fundamental problems.

Many of the large IT service companies have operations at multiple sites and some of these may be offshore. Chances are that the partner company will want to maximize the use of lower cost offshore resources, which brings country risk into play. Data privacy can be a major concern in such cases. In general, it is advisable to have a contract prohibition against moving data to a different location without permission, which should not be granted without first evaluating all of the risks associated with such a move.

Even within one nation, it is possible that the service provider may not follow the same processes at different sites. Another site issue may be related to location. Is the site vulnerable to natural disaster? Chances are the healthcare company would rather not have its main data center at the foot of an active volcano or on the banks of a river that floods every spring.

The experience of the partner company is relevant, especially in light of the need to comply with GxP and other regulations and data privacy requirements. Companies that have never worked in a regulated environment may claim that they'll do what is needed and compliance will not be an issue, but experience has shown that the amount and rigor of documentation that is expected almost always come as a surprise to inexperienced partners. It can take years for them to accept and settle in to the requirements, and this is exacerbated by the fact that they are not operating under the watchful eye of GxP SMEs as is the case within healthcare companies. In this regard, the healthcare companies need to be wary of inexperienced firms that seem to be offering bargain basement prices. It may be that they don't realize what they are getting into, or worse, it may be that they don't take the requirements seriously because they are not directly exposed to liability for failure to comply.

There are several risks related to staff at the partner company. The contracting healthcare company needs to recognize that it is their sensitive data at risk, and that their partner's employees should meet the same minimum standards as their own employees. Background checks should be routine, at least within the capabilities of the national infrastructure. Employee turnover rate is an important concern. In some developing economies, turnover is remarkably high even in skilled jobs, as high as 30%. This means that staff will always be on the steep part of the learning curve and employee efficiency will be low. The resulting lack of continuity is likely to negatively impact the quality of compliance documentation, too. Finally, staff should be trained in the required regulations and should understand the contracting company's business requirements. This training should be provided by the partner.

The same economies of scale that make outsourcing attractive introduce a new risk: segregation of duties. Does it matter if work is being done for a competitor in the next cubicle? Does it matter if the same individual is also doing work for a competitor?

The contract can provide for compensation if an outsourced partner makes a mistake that costs the healthcare company a large amount of money. However, a partner worth $10 million is not going to be able to pay for a data theft that leads the loss of intellectual property worth $100 million. This might influence the kind of work assigned to such a company.

Mitigating Company Risks

The key to recognizing and avoiding or mitigating company-related risks is again applying all due diligence. Do the homework. Research as much about the company as possible. Go to their facility and do a thorough audit. If possible, try to find and talk to both satisfied and unsatisfied customers.

Have the courage not to engage potentially unsatisfactory partners, even if there is substantial pressure to go with the lowest cost partner or to simply "get it done." *Caveat emptor:* realize that if the bargain seems too good to be true, it probably is. Finally, write the contract carefully. It is remarkable how difficult it can be to get a partner to do tasks that they interpret as falling outside of contracted services (see next section).

Risk #4: Contract Risks

One of the biggest enemies of cost savings (and thus a significant financial risk) can be a lack of specificity in the contracted service levels, as well as unclear articulation of *all* of the measures that need to be in place to achieve desired service levels. Due diligence up front will result in a firmer, more realistic price and reduce subsequent "nickel and dime" costs. Excessive nickels and dimes that add up to a significant fraction of total cost of service are a mark of a weak contract.

Several specific risk scenarios need to be directly addressed in the contract. These scenarios should detail expectations for actions if they arise, and it may be advisable to include penalty clauses if expectations are unmet or the healthcare company suffers damage. Of course the prospective partner is very likely to resist penalty language in the contract so it is imperative to understand just how much trust should be allowed. In some cases, refusal to accept penalty clauses might be sufficient to disqualify a supplier.

Some of the risks that should be addressed include those below, but there may be others:

- **Protection of Intellectual Property (IP):** measures need to be defined as to how it is kept safe, including whether it needs to be segregated from other data. It is advisable to have specific agreements on who has access and under what circumstances, as well as how it is granted and managed.
- **Breach Notification:** in the event of exposure or loss of information, the healthcare company needs to know about it right away. The contract should stipulate what constitutes a breach and how quickly it must be reported. It also should define the responsibilities of both parties for investigation and mitigation activities.
- **Indemnification:** in the event of a data breach or other serious event, the healthcare company will want financial compensation to help defray losses, and the partner company should have the financial capacity to pay.
- **Right to Audit:** the contracting healthcare company must retain the right to audit the partner company in order to verify compliance to the contract. The contract can specify requirements for notification, frequency of general audits, and guidelines for "for cause" audits.
- **Continuity/Disaster Recovery:** the business continuity clauses in the contract need to ensure the continuity of the healthcare company. From this point of view, the business continuity of the partner is of secondary concern. The healthcare company does not want to wait in queue behind two banks, a retailer, and a nail salon to bring its systems back on line. If this means that a provision is needed to temporarily transfer the data and operations elsewhere, that should be specified. One aspect that may be overlooked is the partnership of system owners at the healthcare company with the IT supplier for DR testing. This may require a different working paradigm for DR testing than the service provider wants to have for routine operations. However, disasters are anything but routine, and that must be recognized. Putting it in the contract may avoid problems with this crucial activity.
- **Background Checks:** if the healthcare company requires pre-employment background checks, it is only reasonable that they would want such a precaution for their partner's employees. This should be stipulated, especially if it is a practice not routinely followed.
- **Separateness:** even beyond IP considerations, the healthcare company may want to have its data segregated from that of other firms. For example, if a company outsources its ERP application, is it acceptable to have its data pooled with that of other firms or do they need an isolated database? Another consideration is staff deployment. If it is unac-

ceptable to have employees working on another account simultaneously with that of the healthcare company, the contract should stipulate this.

- **Stability:** consider what happens to data, applications, and even staff if the partner company goes out of business. If applications are running on the partner's hardware, what happens if the company fails? Presumably many of the subject matter experts that the healthcare company relies upon are employed by the partner so their fate is an issue. While it may be difficult to build protections against business failure into the contract, it may be possible to include financial reporting clauses that would provide warning that the partner is on shaky ground. What protection does the healthcare company believe may be required to ensure that its business is not unduly affected if the partner slashes staff as a cost cutting measure?
- **Exit Strategy:** the healthcare company needs to ensure that it can execute a reasonably problem-free disengagement from the partnership if necessary. By the same token, they need to ensure that if the partner decides to terminate the relationship, there are provisions to facilitate a smooth transition back to the company or to a different supplier. Timelines for notification of termination should be in the contract, including supporting the transition of services to another party.

Mitigation of Risks Related to Contract

Certain parties and activities that should be involved in supplier selection also can be very helpful in developing the most advantageous contract. The Sourcing and Legal Department should certainly be engaged. They will have the most experience with negotiating contracts, and with contract language, which is terribly arcane to most mortals. Consultants also can be very helpful in understanding capabilities of suppliers. Internal subject matter experts need to be very heavily engaged. These SMEs should represent the full range of internal IT customers, plus other authorities like QA. It is too easy to involve only a small team in the process and miss critical requirements of the business. This can manifest in the refusal of the service supplier to do tasks they feel are outside the contract without additional compensation, when chances are that the task would not even have raised eyebrows if added to the requirements list for the contract.

References from other clients, industry research, and an effective Request for Proposal (RFP) process are powerful tools both for deciding whether the right supplier has been chosen and for selecting some of the contract stipulations. Supplier assessment, including a direct audit, also helps highlight supplier weaknesses that should be addressed in the contract.

Risk #5: Nature of the Work

The type of data being handled and what is being done with it have a decided impact on risk. In light of the prevalence of identity theft and the attention of lawmakers to the issue, handling of PII can be a major risk. Included in this category are personnel records, records that include Social Security numbers, contact information, and patient information. The latter includes even such data as disease states, medication, birth date, etc. Different jurisdictions have different interpretations of what is personally identifiable. Ergo when deciding whether such records should be handled by a partner, and what controls are needed, it is imperative to understand the requirements of the jurisdiction where the individuals reside as well as the location where the data may reside and/or be handled.

Other confidential information needs to be considered as well. There are types of business information that have the ability to cause significant company harm if breached, such as merger and acquisition data or documents protected under attorney-client privilege. Perhaps less directly damaging, but still important to competitive advantage would be information on marketing campaigns, sales figures, banking, and of course intellectual property.

Mitigating Risk Due to the Nature of the Work

Several key internal stakeholders should be involved in deciding what work can be done outside the company. This group should include the legal department, information security, the privacy office, Quality Assurance for GxP applications, and of course the business owner. It is important to recognize that the risk analysis and steps taken for mitigation may change over the life of the engagement.

It is a good idea to have predefined criteria for classes of data with strategies defined for each class. For example, for certain sensitive information, risk may be reduced by limiting access to such sensitive data to a small number of the partner's employees or by technical controls such as encryption.

The Risk Equation

Overall risk for a given application or data set can therefore be "quantified" as the sum of four sources of risk, all viewed through a lens of effective governance:

Country Risk
Company Risk
Contract Risk
<u>+ Nature of Work and Data</u>
= Overall Risk

When all of these are considered, there are four potential modes of response. As illustrated in Figure 4, this fits nicely into a 2 × 2 grid plotting risk impact vs. probability. These potential responses are:

- Ignore the risk, allowing the service supplier to manage it as they see fit (while understanding that liability and accountability cannot be outsourced).
- Accept the risk and delegate mitigation to the supplier. Risk mitigation efforts should be monitored and reported.
- Accept the risk and manage mitigation within the healthcare company. Risk mitigation responsibility in this case is considered too critical to leave to the supplier so the solution is developed by the client.

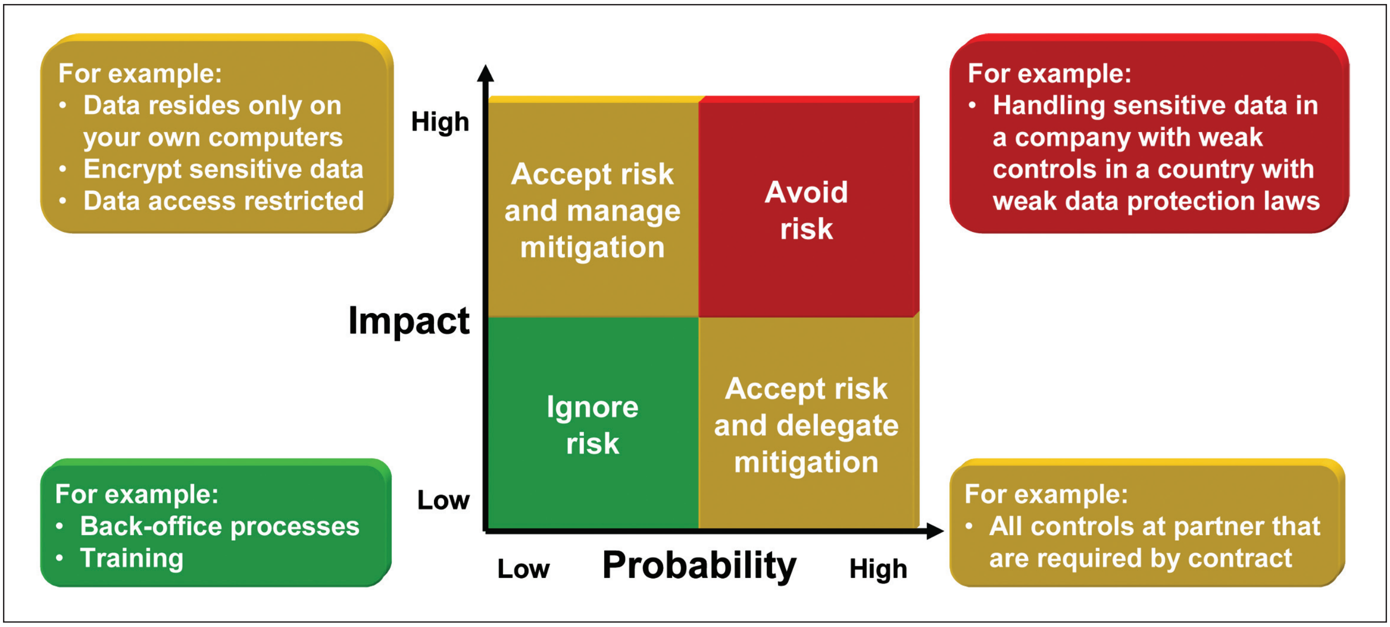
For example:
• Data resides only on your own computers
• Encrypt sensitive data
• Data access restricted
High
Accept risk and manage mitigation
Avoid risk
For example:
• Handling sensitive data in a company with weak controls in a country with weak data protection laws
Impact
Ignore risk
Accept risk and delegate mitigation
For example:
• Back-office processes
• Training
Low
For example:
• All controls at partner that are required by contract
Low
Probability
High

Figure 4. Risk scenarios and possible responses.

- Avoid the risk entirely. Typically this entails retaining and managing the data internally. Another potential route would be to use an alternative supplier where the risks are considered lower, shifting the risk profile from high impact/high probability to high/low or low/high.

Lessons Learned

When navigating the waters of IT outsourcing, several lessons should be taken to heart:

Responsibility and accountability cannot be abdicated. Consultants can add considerable value to the process of selecting suppliers and helping to evaluate them, but in the end the business expects the same service, reliability, and level of risk as they have been getting from local IT, and IT will be held accountable for shortcomings.

Due diligence must be performed. The supplier needs to be audited, both before and during the engagement. Require metrics and reports to demonstrate efficiencies. Monitor the financial health of the service supplier. Use defined change management processes to identify when significant changes occur either at the client or with the provider to ensure the level of risk is still acceptable.

Awareness must be ensured through training and governance. It is fallacy to assume that all local IT staff can be eliminated. In reality, while some staff reduction is possible, new local IT responsibilities will include the governance of the outsourcing effort and the local management of projects involving the supplier. Cutting local IT staff too far will result in a dysfunctional relationship with the service suppliers and unsatisfied customers within the healthcare firm.

The healthcare company should take advantage of every opportunity to reduce risks that are within its control. At the same time, it must be understood that there are some risks that they cannot efficiently or effectively control. These kinds of risks may be better delegated to management by the supplier.

The nature of the work considered for outsourcing needs to be clearly understood, classified, and documented. Depending on risk tolerance, there may be some things that simply should not be done off-shore in some countries or perhaps even outsourced at all. In any case, access should be provided only to that data required for the engagement.

Requirements and expectations should be thoroughly documented. If an activity is important, it should probably be in the contract. However recognize that in a major outsourcing effort, it is unlikely that all needs will be identified in advance so build some flexibility into the contract. If the contract requires maximum effort by the supplier as written, chances are good that when something is discovered that wasn't covered the supplier will be unable to deliver the extra effort needed.

Collaborate with the supplier on solutions. Recognize that they are the experts in the services that they deliver. To maximize the value of the relationship, expect them to be thought leaders, not order takers.

Include close-out and transition considerations. All good things come to an end, and failure to have a defined exit strategy will cause no end of angst when it is time to end the relationship.

Internal Risks

This article deals primarily with risks related to engaging outsourced business partners. However, there are also internal risks that a company will have to address as they transition to an outsourced IT model. Three examples of internal risks traceable to outsourcing are:

- Managing external resources is always time consuming. This will have the potential impact of requiring an adjustment of project management resources, and in some cases, may necessitate some travel to the supplier. Additionally, while IT may cut back on "traditional" staff, some new positions will likely become necessary to manage the interface between business customers and the IT service suppliers. These new positions will require both a grounding in the technical aspects of IT as well as understanding of business priorities and requirements.

- Staff reductions result in the loss of local expertise. Incidents once addressed locally now depend on external resources. Bureaucracy is likely to increase, especially if the support staff is in a different time zone. There is a risk of customer frustration at the amount of extra time and effort required to solve problems, which can encourage the rise of "shadow IT."
- "Shadow IT" is a significant threat. If getting a project done through the IT department becomes onerous due to outsourcing/offshoring, there will be a temptation on the part of business managers to cut out the middle man and develop their own outsourced solutions. This can lead to non-standard infrastructure, unrecognized support requirements or unsupported systems, and increased risk to data integrity, confidentiality, availability, and accessibility.

Conclusion

There are real potential benefits to be realized by outsourcing or off-shoring routine IT activities. However, there are accompanying risks that must be monitored and in some cases mitigated. You cannot go far wrong if you remember this mantra:

It's all about the data.

The bottom line is that the most important asset of a pharmaceutical or biotech company is its information. Placing that information in the hands of a third party service provider automatically assumes a level of risk. How high that risk is depends on country issues relating to legal and political factors, company issues, contract issues, and the nature of the data and the work to be done by the supplier.

Finally, as we are constantly reminded by regulators, whatever is done in the name of the healthcare company is at day's end the responsibility of the client company. Hence, the fifth risk factor, governance of the outsourcing/off-shoring program.

Legal Disclaimer: The opinions expressed in this article are solely those of the authors and not necessarily those of Novartis Pharmaceuticals Corporation ("NPC"). NPC does not guarantee the accuracy or reliability of the information provided herein.

References

1. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems*, International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, p. 305, www.ispe.org.

2. Davison, Dean, *Top 10 Risks of Offshore Outsourcing*, http://searchcio.techtarget.com/news/article/0,289142,sid182_gci950602,00.html, 2004.

3. Westerman, George, and Hunter, Richard, IT Risk: Turning Business Threats into Competitive Advantage, Harvard Business School Press, 2007.

4. Bakalov, Rudy, "Risk Management Strategies for Offshore Application and Systems Development", *Information Systems Control Journal*, Volume 5, 2004, http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=22051&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

About the Authors

Dr. Arthur (Randy) Perez currently holds the position of Executive Expert, IT Quality Assurance for Novartis Pharmaceuticals. His responsibilities at Novartis include a wide range of IT Compliance issues, such as GxP, Sarbanes-Oxley, and data privacy. He serves on several global Novartis teams dealing with computer systems compliance issues, and has authored many of the firm's global GxP compliance policies. During his 27-year tenure at Novartis, he has developed a broad range of experience, working as a chemistry group leader in process research, managing a chemical manufacturing process validation program, and running a QA validation group for pharmaceutical operations. Dr. Perez was a member of the PhRMA Computer Systems Validation Committee from 1995-1999, and was instrumental in the formation of GAMP® Americas when that group started in 2000. From 2002-2008 he served as Chairman of GAMP® Americas and he remains a member of the global GAMP® Council. He initiated and led the Global Information Systems SIG, who wrote a GAMP® Good Practice Guide that was published in 2005, and was part of the core team who developed GAMP® 5, published in 2008. Dr. Perez has been a speaker and a course leader at numerous conferences in the US and Europe, and has been published in industry journals and textbooks. In 2005, he was elected to the ISPE International Board of Directors, where he currently holds the office of Vice Chair. He can be contacted by email: arthur.perez@novartis.com.

Glenn Morton was previously with Bell of Pennsylvania and the Federal Reserve Bank in numerous roles including data center manager, Manager of Quality Assurance, Manager of Systems Programming and Disaster Recovery Planning. Since joining Novartis in 1997, Morton developed and implemented a Global Change Management system and methodology used in over one-hundred countries in all divisions. As Head of Global Disaster Recovery Planning, he created a methodology, database and training material, and executed an implementation plan that captured information for more than 200 IT locations. He was part of the core team responsible for the roll out of Sarbanes-Oxley for more than 50 countries and led the project for the Novartis Pharmaceuticals' U.S. Avian Flu Business Continuity planning effort. Most recently, he has headed Novartis' US IT Risk Management and Compliance organization with responsibilities in GxP and SOX compliance, Information Security, Data Privacy, Application Portfolio Management, and Business Continuity. He can be contacted by email: glenn.morton@novartis.com.

Novartis Pharmaceuticals Corporation, One Health Plaza, East Hanover, New Jersey 07936, USA.