

# Risky business?

## Evaluating and managing risk on outsourcing

**Mike Rebeiro and Radford Goodman of Norton Rose LLP** review some of the key risks on outsourcing, and how businesses can address and manage such risks.

The accounting fraud at Satyam Computer Services (Satyam), where Satyam's chairman admitted that its accounts had been overstated by some \$1 billion, was India's biggest ever corporate scandal, and shook the confidence both of investors and of companies outsourcing their services (customers) in the offshore outsourcing sector as a whole.

The affair has brought into sharp focus the wider risks of outsourcing, particularly in relation to supplier performance, and forced many businesses to examine the integrity of their outsourcing arrangements. Outsourcing deals where customers have taken an unrealistic approach to risk are more likely to end in renegotiation or termination than those with a more balanced approach to the apportionment of risk and reward.

This article reviews some of the risks inherent in outsourcing transactions and considers how businesses undertaking an outsourcing can evaluate, apportion, price and manage such risks.

### EVALUATING RISK

There are many types of risk which should be addressed in any outsourcing arrangement. For the customer, these generally include: service failure; project delay; business disruption; regulatory risk; breach of security; data loss; damage to reputation; employee liabilities (for example, under the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246)); sup-

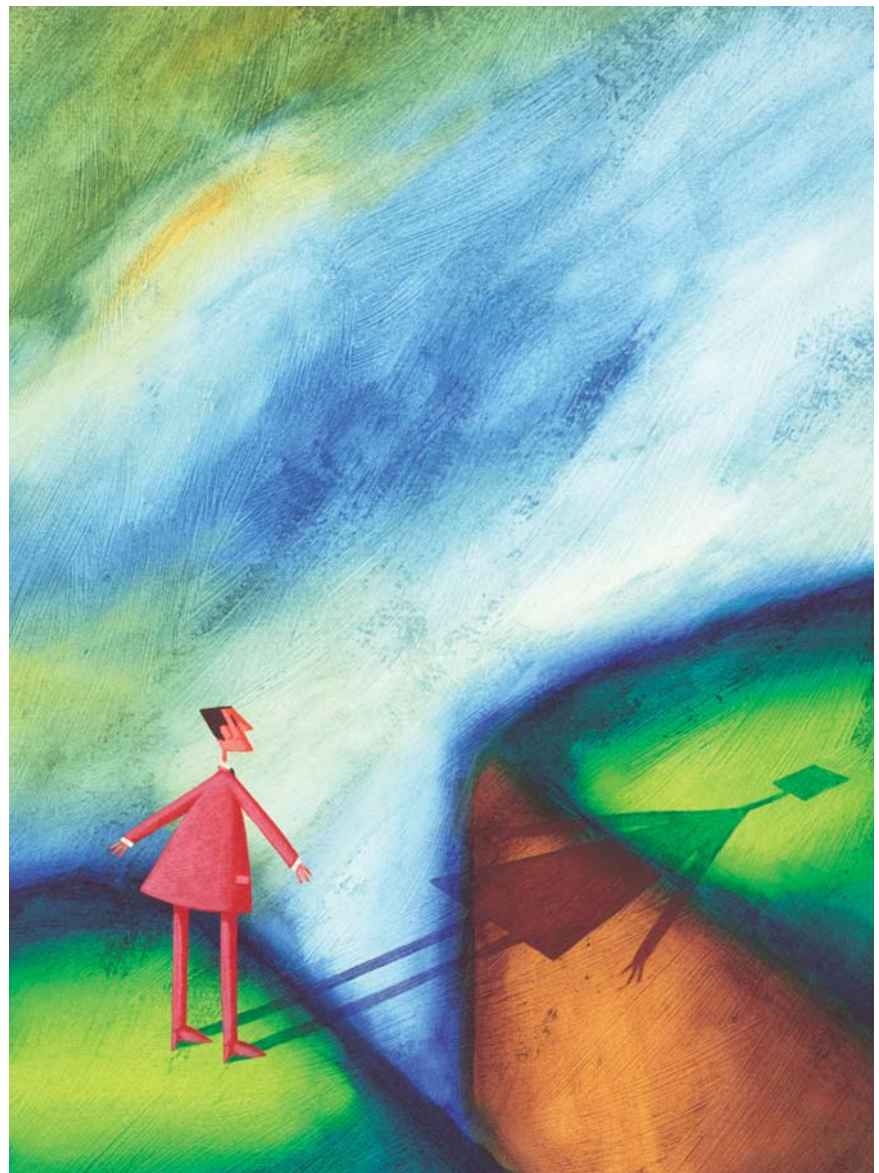


Illustration: Getty Images

plier insolvency; damage to business relationships; damage to property; and loss of revenue (for background on em-

ployee liabilities, see feature article "Outsourcing: the commercial issues", [www.practicallaw.com/1-201-8559](http://www.practicallaw.com/1-201-8559)).

In assessing risk, it is essential to identify those particular risks which are associated with the outsourcing project and to decide what level of risk is acceptable (see box “*Risk evaluation: best practice*”). Customers must also gauge the probability of identified risks occurring and assess what their impact would be on their business, as even if a risk is highly probable, its effect on the business may be negligible.

Keeping track of risks identified and the measures taken to mitigate them can be difficult, particularly where the pace of negotiations accelerates towards the end of the procurement exercise. For this reason, it is vital that the parties maintain and update a risk register so that each risk can be managed as negotiations progress (see box “*Risk register*”).

### Sector-specific risk evaluation

While suppliers often adopt similar approaches to the risks they face (for example, non-payment, recovery of costs, damage to their reputation), an analysis of customer views across industry sectors shows that customers do not all attach the same degree of importance to a particular type of risk.

**Banking and insurance.** Insurance companies and banks operate in a similar business and regulatory environment, and so have a similar approach to risk. In these sectors, customers rank security, regulatory issues and reputational damage as the highest risks. Insurance companies rate data loss as another primary risk, while banks also focus on loss of revenue.

Both sectors need to be able to demonstrate to their regulators that any contractual arrangement for the provision of outsourced services minimises operational risk (see box “*Regulatory framework for banking and insurance outsourcing*”). This is especially so in the banking sector, where the effective management of risk has a direct impact on capital adequacy requirements under the Basel II capital framework (for background on these sectors, see feature article “*Outsourcing: sector-specific issues*”, [www.practicallaw.com/0-201-9998](http://www.practicallaw.com/0-201-9998)).

## Risk evaluation: best practice

Companies outsourcing their services should bear the following points in mind when embarking on an evaluation of the risks inherent in any particular outsourcing:

- With the help of advisers, identify risks at the outset of the contract, before the invitation to tender is issued. This is best achieved using a written risk register (see box “*Risk register*”).
- Once identified, evaluate the risks as to the likelihood of the risk arising and the damage caused if the risk materialises.
- Consider allocating a risk manager to the project team.
- Once the contract has been executed, treat risk reporting as an integral part of project governance.

Security issues are closely tied to regulatory risk: witness the Financial Services Authority’s imposition of substantial fines on banks and insurance firms which have lost client data. For example, in 2007, Nationwide Building Society was fined £980,000 over security breaches following the theft of a laptop ([www.practicallaw.com/8-242-0104](http://www.practicallaw.com/8-242-0104)) and Norwich Union was fined £1.26 million for security lapses which lead to its customers being subject to identity fraud.

**Professional services.** While not subject to the same extensive regulatory regime as the financial services sector, professional services firms are required to deliver to their own clients a discreet, secure and timely service. A failure to do so could lead to irreparable damage to their reputation.

Businesses in the professional services sector rank data loss, breach of security, reputational damage and damage to business relationships as primary risks. As with firms in the financial services sector, the risks faced by professional services firms need to be minimised from the outset, starting with a thorough due diligence process. After that, they need the outsourcing contract drafted to ensure that operational risks are minimised, and effective project governance to ensure that any issues are picked up, and dealt with, promptly.

Professional services firms are specialists in understanding and evaluating insolvency risk and have a sophisticated approach to mitigating risk in this area. As a consequence, supplier insolvency is not a risk which tends to rank as highly as other risks.

**Communications, media and technology.** The communications, media and technology (CMT) sector has a client base which demands an uninterrupted delivery of services. The impact of failure to deliver is therefore more immediately felt, so that a CMT business’s failure to deliver consistently and on time will be particularly damaging to its reputation. CMT customers also tend to be more focused on relationships with consumers rather than with other businesses.

**Transport.** The main risks to transport companies’ businesses are failure to process orders and reservations, and failure to transport clients and goods safely and on time. As a result, this sector tends to rate service failure, project delay, reputational damage and business disruption as its primary risks. Limiting risks arising from these issues is best done by maintaining a positive relationship with the supplier, coupled with an effective service level agreement which details objective and quantifiable criteria expected from suppliers, and remedies for failure to meet service levels that will adversely affect the customer’s business.

**Industrial.** Industrial customers tend to view service performance failure as the main threat to their business. If they are not able to run their manufacturing or other facilities, this will have an immediate impact on their business: they will suffer a loss of production, with a corresponding downturn in revenue and profit. Unlike all the other sectors, they do not rank reputational damage and regulatory issues as key risks. Industrial customers are less heavily regulated, and it is less likely that one event would cause catastrophic damage to their reputation. However, industrial customers do regard supplier insolvency as a high risk which reflects the nature of the supply chain specific to this sector.

### APPORTIONING RISK

Having ascertained what risks the customer faces, the parties must agree during negotiations who will be liable if a risk materialises and damage is suffered as a result. Questions around the type and level of liability to be accepted by suppliers or customers are ultimately commercial questions that cannot be divorced from the issues of risk and price management.

Customers in different industry sectors are prepared to accept different levels of risk (*see above*). In addition, customers and suppliers have different views on the apportionment of risk; in some cases, customers are prepared to take a greater responsibility for the management of more types of risk than suppliers would otherwise believe.

Customers must consider how risks can be minimised and whether they or the supplier are best placed to manage them, through appropriate contractual provisions and operational processes (*see "Risk management strategies" below*). Customers need to be realistic in their approach to risk: there are some risks that should not simply be allotted to the supplier (for example, where the risk is within the customer's control, such as the risk of infringing a third party's intellectual property rights in respect of materials provided by the customer, or loss of data where the customer retains responsibility for its stor-

## Risk register

A risk register is an invaluable tool which allows both companies outsourcing their services (customers) and suppliers to identify risks and the strategies required to mitigate them. The risk register should allow each party to:

- Identify and work through the risks presented by an outsourcing project in some detail.
- Consider and record desired risk allocations before contracts are drafted.
- Consider and record both contractual and operational mitigation strategies against each risk.
- Record negotiation positions on each risk, together with the status (for example, in red, amber and green) of the risk, with the objective of downgrading the status of high severity risks throughout the procurement process by ensuring that such risks are properly managed.

More sophisticated risk registers operate electronically and produce reports on the position adopted against each risk, which may be presented to senior management. These registers may also create links from the recorded risk to the relevant clause in the draft contract, which facilitates easy access to the document and any changes which need to be made.

A risk register allows customers to take a more informed view as to how risk should be managed and the value of including or omitting certain contractual provisions. It may also help the project team to develop a more balanced long-term contractual relationship between customers and suppliers.

age and back up) (*see box "Risk allocation: checklist"*).

### PRICING RISK

Suppliers operate sophisticated models for pricing risk. Asking them to accept an unbalanced proportion of risk will have a direct impact on the level of charges. For example, imposing five different contractual remedies to manage a single risk where one remedy would suffice will inevitably lead to an increase in the price imposed by the supplier. Likewise, the transfer to the supplier of those risks which would be better managed by the customer will also increase the price.

Having a good supplier understanding of legal and operational risk is therefore important to pricing contracts; suppliers need to have an overview of relevant risks, the likelihood of the risk materialising and the resulting damage before they can attribute a proper cost to carrying such risk. This must be borne in mind when customers run tender

processes, and customers must consider how risks can be minimised and whether they are best placed to manage such risk. They can also ask suppliers to bid against different risk profiles during the tender process to obtain a clearer idea of how different risk apportionment will be priced (*for background on the tender process, see feature article "Outsourcing: the commercial issues", [www.practicallaw.com/1-201-8559](http://www.practicallaw.com/1-201-8559)*).

### RISK MANAGEMENT STRATEGIES

Risk cannot be eliminated, but it can be properly managed. Customers have a variety of risk management tools available to them, and need to consider which are the most appropriate. Over-reliance on one risk management tool is unhelpful: spreading such tools can lead to the avoidance of technical and business problems or their resolution at an early stage, saving both time and money. However, it is only by working together with the supplier that risk can be managed effectively (*see box "Risk management strategies: checklist"*).

## Regulatory framework for banking and insurance outsourcing

There are various regulatory requirements which banking or insurance companies should bear in mind when considering outsourcing:

**Notification.** Banks and insurance companies must notify the Financial Services Authority (FSA) of proposed outsourcing arrangements and significant changes to outsourcing arrangements (15.3.1R and 15.3.8G(1)(e), *Supervision (SUP)*, *FSA Handbook*).

**Systems and controls.** If a bank is outsourcing critical functions, it must take reasonable steps to avoid undue operational risk. It must also not outsource important operational factors in such a way as to impair materially the quality of its internal control and the FSA's ability to monitor the bank's compliance with its obligations under the regulatory system (8.1.1R, *Senior Management Arrangements, Systems and Controls (SYSC)*, *FSA Handbook*). Banks must also exercise due skill, care and diligence when entering into, managing or terminating any arrangements for the outsourcing of critical or important functions (SYSC 8.1.7R), and ensure compliance with a number of specific conditions set out in SYSC 8.1.8R.

Where a bank outsources critical or important functions, it remains fully responsible for discharging all of its regulatory obligations and must comply with a number of conditions set out in SYSC 8.1.6R. It must have a written contract in place with the supplier which clearly allocates the rights and obligations of each party (SYSC 8.1.9R). It must also make available to the FSA on request all information necessary to enable the FSA to supervise the arrangements' regulatory compliance.

The outsourcing rules applicable to insurance companies are located mainly in SYSC 13 and 14.

### Due diligence

Selecting the most appropriate supplier for the project can reduce risk substantially. It is incumbent on a customer to devise a due diligence process that will properly test and evaluate potential suppliers. A successful due diligence exercise should not be just a paper exercise: it should involve visiting potential suppliers, testing technology and speaking to other customers of the supplier. It is also important for customers to consider soft issues such as cultural fit.

Since the Satyam scandal, the financial aspects of due diligence are under greater focus to ensure that the prospective supplier is solvent, and will have the resources to remain solvent during the term of the contract. Supplier responses should be challenged and not accepted at face value. Concerns may be resolved by the supplier's parent company guaranteeing performance and/or financial

compensation (see "Third party guarantees" below). Moreover, in the current market, some customers are also carrying out due diligence on the key supplier personnel who will be involved in the outsourcing project. A project manager who has "misrepresented" his qualifications may demonstrate a lack of integrity which could be fatal to a project.

### Contract

The outsourcing contract itself is generally regarded as the most effective risk mitigation tool. However, in practice, industry has become over-reliant on standard form documents and provisions which do not bear any resemblance to the specific risks at hand. It is not possible to have a "one size fits all" outsourcing contract. While it may appear trite to say that the draftsman needs to have a full understanding of the project-specific risks and that the contract should be drafted with those risks in

mind, this is very often not the case in practice.

Too often, senior management and other members of the procurement team leave the negotiation of liability and termination provisions to lawyers, without input from the business. Moreover, one cannot look at these clauses in isolation from the rest of the contract or the business: only the business can assess what effect a breach will have, what loss will be suffered, and if (and how) such a breach can be remedied.

### Key performance indicators and service level agreements

It is essential to set the standard of the services performed by the supplier. Key performance indicators (KPIs) and service level agreements (SLAs) are terms which are often used interchangeably, but are usually distinguished by the type of remedy which applies if there is a failure to meet the KPI or SLA. For instance, breach of an SLA may trigger the requirement for a meeting or a report, while breach of a KPI may trigger a service credit (a deduction from the contract price payable by the customer in response to the supplier's failure to meet a service level). Persistent failure to meet an SLA may mean it is promoted to being a KPI, while a persistent failure to meet a KPI may trigger a termination event.

KPIs and SLAs need to be identified at the business case planning stage and should be included in the invitation to tender (ITT). Suppliers can then be scored against their ability to achieve KPIs and SLAs. Customers should be careful that they do not include unnecessary KPIs and SLAs in the ITT as this may have an adverse impact on charges (see "Pricing risk" above).

**Service credits.** Claiming service credits is often viewed as a last resort; in reality, many customers doubt whether they offer any substantive remedy from a business perspective. Moreover, their inclusion in the contract will increase price. While it is self-evident that suppliers do not wish to lose revenue through service credits, the requirement that the supplier make a payment to the customer

## Risk allocation: checklist

When deciding how to allocate risk, customers should:

- Before engaging in a tender process, clearly identify the risks associated with the project. Consider the risks arising at each stage of the tender, contract negotiation and delivery.
- Maintain a risk register throughout the project, identifying how risk can be mitigated as the project continues (see “Risk register”).
- Consider whether risk can be best managed by the customer or supplier; take a realistic view of risk allocation.
- Not focus on a deal-breaking position on risk, if the overall risk profile of the arrangement is low.
- Focus on risk which is real and important to the business. Where risk is not important, take a realistic and commercial view in negotiations.
- Remember that risk will be priced into the contract.

can be more effective than just setting off the service credit incurred against the amount payable by the customer. No project manager on the supplier side wants to write a cheque that might require authorisation from his line manager and prompt a difficult discussion about why the contract is not maximising revenue.

However, a well-structured service credit regime, which focuses solely on those areas of risk which have a real and detrimental effect on a customer’s business, could help in managing a supplier’s performance. The threat of having to pay credits in itself should encourage good behaviour, but only where the service credits are material: where they are

not, the costs of managing their application could outweigh their benefit.

**Liquidated damages.** Liquidated damages are a determined sum which the parties agree will be payable on the specified default of one party. Under English law, they must be a genuine pre-estimate of a customer’s loss (*Dunlop Pneumatic Tyre Co Ltd v New Garage and Motor Co Ltd* [1915] AC 79).

In outsourcing contracts, liquidated damages are used most commonly as an incentive for timely performance; if a project (such as the implementation of a service or a computer system) runs late, liquidated damages will become payable for the period of the delay. If a delay in the project would lead to severe problems, liquidated damages may be a tool to mitigate such risk.

It is not possible to simplify the process by simply guessing the likely loss and including this figure: if the estimate is not genuine, the court will classify it as a penalty and it will not be enforceable. While this does not mean an estimate of loss has to be precise, it does require customers to make a genuine attempt to forecast the loss that might occur. Customers should also retain the basis on which they made their estimate in case this is needed as evidence to rebut the supplier’s claim that the liquidated damages are in fact a penalty and therefore unenforceable.

Some customers regard liquidated damages as being useful, not because they represent adequate compensation but because customers feel it is the most effective way of ensuring that a supplier delivers on time. However, their inclusion may represent the customer’s sole remedy for delay, as suppliers will resist the inclusion of other remedies and sanctions if liquidated damages are included. It might also drive contract costs higher as suppliers build the costs of paying out liquidated damages into their price. Because of this and the difficulties in pre-estimating loss, there is an increasing disillusionment with the effectiveness of liquidated damages as a risk mitigation tool.

## Risk management strategies: checklist

When considering risk management strategies, customers should:

- Once risks have been identified, consider how these can be managed and which risk management tools are most appropriate. Risk analysis can be shared with the supplier.
- Conduct thorough due diligence on their sourcing partner’s financial, legal and, most importantly, operational status.
- Not underestimate the importance of good project management. Ensure good governance and project management is in place with the right skill sets for the role.
- Limit financial commitments by using appropriate payment plans tied to performance and delivery.
- Ensure a contract is in place which is properly aligned with the underlying business plan but also reflects an appropriate sharing of risk.
- Focus on those risk tools which they regard as effective for their business, and not waste time, money and resources negotiating around tools which will not be used.

**Audit rights.** The right to audit entitles the customer to carry out its own investigations as to the supplier’s compliance with the terms of the outsourcing contract. It may also extend to other matters, such as the supplier’s compliance with relevant regulations or the supplier’s solvency.

The effectiveness of audit rights is determined by the limitations the supplier places on access to information. In many cases, suppliers will restrict the extent to which customers can carry out investigations by withholding information which they deem to be confidential, such

## Audit rights: case studies

In an outsourcing within the financial services sector, audit rights were used extensively following a loss of data by the supplier. The customer was able to exercise its right to audit the supplier's processes and systems, to identify how the data was lost and to satisfy itself that the breach was a one-off and not part of a systemic failure to keep data secure.

In an outsourcing in the communications, media and technology sector, the customer had concerns regarding the amounts it was being charged. The customer and supplier had agreed to charge for the supplier's services on a cost plus basis (meaning the customer was charged for the costs of providing the outsourced services plus a profit margin). The audit revealed extensive overcharging for services, including charges for costs incurred by the supplier for its other customers. Following the audit, the supplier agreed to repay the amount overcharged and contributed to the cost of the audit.

as information which relates to its other customers or its profit margins. The cost of an audit can also be prohibitive; many customers do not have sufficient resources to carry out their own audit and the costs of hiring the services of a professional audit team can outweigh the benefit the customer expects it will derive from the audit.

As such, audit rights are often not ranked as highly as other risk management tools. However, given the requirement of many financial services regulators to include extensive audit rights in outsourcing contracts, greater emphasis is placed on audit rights and their implementation in the financial services sector (see *"Banking and insurance" above*). Equally, in sectors such as professional services, where the customer may have the ability and resources to carry out its own audit, there is often a greater appetite to secure audit rights than in other industry sectors (see box *"Audit rights: case studies"*).

**Change control.** No business environment remains static, and without the ability to make changes, the outsourcing arrangements risk becoming obsolete. The contract should therefore contain a mechanism for managing contractual and operational change. However, the process of change and attendant risks are rarely given sufficient focus in the negotiation of large-scale contracts. This can often result in unanticipated costs being incurred once the outsourcing has

gone live and, accordingly, a general dissatisfaction with the outsourcing arrangements.

Customers must consider from the outset the likely causes of change, and agree with the supplier how any change will be implemented and at what, and whose, cost. However, it is unrealistic for customers to expect that the costs of all changes will be borne by the supplier. Similarly, it is unrealistic for suppliers to view change as a "cash cow". The best change control mechanisms allow change to be delivered at a fair price.

A mechanism in isolation will not solve the inherent risks of change. Both the supplier and the customer must manage change by adhering to the change process. Good governance is key to managing change (see box *"Change control: case study"*).

**Benchmarking.** Benchmarking is the comparison of the supplier's offering against other solutions in the marketplace. It is designed to manage the risk that the supplier's pricing is not the best value for money when compared with that of other suppliers, or that the supplier is providing substandard services to the customer's clients as against other providers of the same service.

In practice, there are mixed views about the merits of benchmarking. For some, benchmarking does not work with outsourcing projects, as it can be difficult to

find a suitable comparator because services are rarely standard. For others, a benchmarking exercise might damage the relationship between the parties, which might lead to a decline in the supplier's standard of performance. Nevertheless, some customers are clear advocates for benchmarking, particularly when it has led to an improvement in the supplier's performance.

There are merits in including benchmarking provisions in long-term outsourcing contracts; in particular, a benchmarking regime is very useful for measuring value for money. However, its worth will ultimately depend on the associated sanctions where the benchmarking demonstrates that the service offering is not competitive either in price or quality.

**Step-in rights.** A step-in right is the right for a customer to step in and manage the contract in place of the supplier. It is normally exercisable as a precursor to termination for breach. Many customers do not consider step-in rights particularly effective, feeling that if the outsourcing project is not successful, it should be terminated and a new supplier engaged. In addition, customers often do not have the skills required to manage the contracts themselves. While it is unlikely that customers will ever exercise such rights, they are usually included in contracts as a remedy of (almost) last resort. In practice, such rights are likely to be of less value where the supplier is offshore, as:

- The costs of step-in may be prohibitive due to geographical restrictions.
- It may be difficult to manage a business function in a foreign jurisdiction and in a different time zone.
- There may be inherent political, cultural, legal and business risks in the offshore location of which the customer is unaware.

However, step-in rights can be a useful tool where extreme measures are necessary (see box *"Step-in and exit: case study"*). Clearly, step-in will not be a so-

lution in each case. However, in the right circumstances, and with the right skills on the customer's part, step-in can work.

**Exit planning.** Proper exit planning is vital. Nevertheless, exit is too often overlooked in the procurement process. It is all too easy to underestimate the time it will take to transfer the service to an alternative supplier (a process which will take even longer when the supplier is offshore, as it may be difficult to repatriate services quickly and gain access to technology, assets and key personnel). As part of the contracting process, the parties should focus on the implications of termination and mitigating the disruption to business that could occur, and should include a comprehensive exit plan in the contract.

The exit plan for an offshore outsourcing will differ materially from an onshore plan in that:

- On termination, employees will be unlikely under the local laws to transfer to the customer's employment.
- The customer may not be able to engage the supplier's key employees directly, as they may not be eligible for the necessary work visas.
- The customer will probably not wish to buy IT assets located offshore.
- The customer's key assets to be transferred from the supplier will be intellectual capital and know-how (but the customer should place an obligation on the supplier to record and deliver know-how throughout the term, rather than just on exit).
- The customer will be anxious to ensure that it can enforce obligations for the supplier to delete confidential information and know-how post termination, which may prove more difficult in an offshore arrangement.

Once the exit plan has been agreed, it is important that the customer regularly checks the supplier's compliance with its obligations to facilitate exit, as well as

## Change control: case study

Problems arose in an outsourcing in the financial services sector where a supplier was engaged to build an IT system designed to operate the integral parts of a customer's business. As the system was being built, the supplier began making changes to the design based on discussions with the customer at project meetings. However, many of these changes were not authorised by the customer's senior management. Further, in respect of changes which the customer approved in principle, the supplier made the changes without first agreeing the price for the change.

At no stage was the contractual change management process followed by either party. The parties soon became involved in a dispute, with the supplier arguing that, since neither party had adhered to the change control procedure, the customer could not subsequently rely on the supplier's non-compliance to justify withholding payment for change, as the customer had, in effect, waived its rights to deal with change under the procedure. The customer argued that it had not agreed to the change, whether under the procedure or otherwise, and rejected the supplier's submission that the supplier's delays in building the system were justified because of the extra time needed to implement the changes.

Ultimately, the parties settled the dispute but not before they had expended significant time, effort and resources in retrospectively validating the legitimacy of changes made, all of which could have been avoided at the outset by managing the change through the change control procedure.

carrying out a final audit on exit to ensure that arrangements have been fully implemented. However, in the event of a supplier failing to comply with its exit obligations, it is unlikely that a court would make an order for specific performance (see box "Step-in and exit: case study").

### Project management

Good project management and governance is vital. A project team comprising representatives both of the supplier and the customer is best placed to monitor the provision of outsourced services on a daily basis, identify any problems early and work together to resolve such problems before serious issues arise. However, the resources and skill required to ensure good governance are often seriously underestimated.

The effectiveness of project management as a risk management tool is wholly dependent on the quality and calibre of the individuals tasked with project management or governance responsibilities. Suppliers often raise concerns that the customer project managers do not have the necessary skills for

supplier management and are not sufficiently knowledgeable about the terms of the contract. The skills required by the retained team are often very different from the actual skill set of most management staff "left behind" in an outsourcing arrangement.

### Operational processes

Customers need to consider carefully what operational processes they can adopt to minimise risk. These will differ from business to business, but may include:

- Allocating risk managers to individual outsourcing projects to evaluate risk on an ongoing basis.
- Comprehensive project governance procedures to identify problems early and escalate them for resolution.
- Regular contract reviews to ensure that the contracts remain fit for purpose.

Whatever the processes adopted, they will only be effective if both customer and supplier are fully engaged in their use.

## Step-in and exit: case study

In an outsourcing where the customer and supplier were in dispute, the supplier threatened to turn off the services, abandon the contract and ignore its exit obligations.

The customer sought an interim injunction for specific performance to force the supplier to continue provision of the services. However, it faced a low prospect of success in securing the injunction, as specific performance will not be ordered if there is uncertainty over the nature of the obligations to be performed or the obligations are complex, as they often are in outsourcing arrangements (*Vertex Data Science Ltd v Powergen Retail Ltd [2006] EWHC 1340 (Comm)*). In that situation, step-in rights provided an alternative solution for the customer.

### Technology

The selection and use of the correct technology may serve to reduce risks. For example, data loss is a common problem: if this is a serious risk then a technical solution is to back up data on a regular basis. Similarly, where security breaches are considered a threat, the customer should ensure that the supplier has state of the art protection systems in place. However, use of the proper technology to address the customer's specific risks will only materialise where the outsourcing solution is properly specified, and the risks have been fully identified.

### Training

All too often, human error is the cause of failure in outsourcing. Loss of customer data by individuals working on unencrypted laptops which are stolen or misplaced is a prime example. Both suppliers and customers need to invest in training their staff, particularly in highly regulated industries such as financial services, where particular emphasis must be placed on compliance (see "Banking and insurance" above).

The procurement team should be properly trained in current best practice to ensure that they secure the same best practice from the supplier (for example, ensuring that the supplier is compliant with the ISO 27001 security management standard, which aims to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system).

Project personnel need to be properly trained in relationship management, to ensure that they properly manage their suppliers and outsourcings. Customers can monitor their supplier to ensure that the necessary training is conducted by carrying out audits such as an annual security audit, requiring the supplier to sign a declaration that staff have completed the required training and to arrange or provide the relevant training to the supplier.

### Insurance

It is possible to insure against many risks. However, this can prove expensive, and for certain risks customers choose to self-insure by setting aside funds which can be called on to cover losses suffered by the business. Further, insurance will only compensate the claiming party in monetary terms. Consequently, if the main risks to the business cannot be adequately compensated by a financial payment (for example, loss of reputation), insurance on its own will not be an adequate risk management tool.

### Dual/multi-sourcing

If the functions outsourced are business critical, customers may consider diversifying and appointing more than one supplier. While there is a noticeable trend towards multi-sourcing, customers now recognise that there are difficulties and risks associated in managing and integrating multiple suppliers, and such integration can be costly.

Unsurprisingly, suppliers tend to prefer a prime contractor model where they ap-

point subcontractors. This is because they feel they are best placed to manage the subcontractors and that customers should not micro-manage these relationships. Of course, there will be an associated cost for the supplier in managing the risks of such arrangements and relationships.

Generally, customers agree with this approach, preferring to deal with just one supplier on the basis that dual and multi-sourcing can create its own risks; if the suppliers and subcontractors do not work together and the project fails, it may be difficult to attribute fault specifically to one party. Nevertheless, where such subcontractors are key, it is prudent to carry out the same level of due diligence on them as the customer would on the prime contractor. This would require co-operation by the supplier, for example, by arranging access to its subcontractor's premises.

### Third party guarantees

Customers often have concerns about dealing with subsidiaries of corporate groups. In such circumstances, customers may wish the parent company to stand behind its subsidiary and guarantee performance and/or financial compensation. However, the practicalities of enforcing such guarantees mean that the use of parent company guarantees may drive costs up but be ineffective. This is especially so where, having secured a judgment from an English court to enforce a guarantee, there is no reciprocal arrangement with the jurisdiction in which the guarantor is established.

### Insolvency contingency planning

In the light of Satyam, businesses need to focus on insolvency risk, review contractual arrangements and have contingency plans in place, so that damage is minimised if a key supplier ceases to trade.

However, dealing with financially insecure suppliers is sometimes unavoidable. For example, a supplier may have exclusive technology or may only run into difficulties after the contract has been entered into. In such instances, exposure may be minimised by including contractual protections such as:

- Limiting the amount of money paid in advance (if possible, paying in arrears for services, or subject to delivery and acceptance in the case of system development).
- Audit rights.
- Frequent provision of deliverables which the supplier has contracted to provide, such as documents or software, so the customer has the latest version of the technology.
- Where relevant, placing source codes into escrow, with insolvency being a trigger release event.

Customers must draw up a contingency plan which sets out the steps they need to take to secure the services and/or technology if the supplier is no longer able to perform or has become insolvent. This plan should be reviewed and updated throughout the contract term and will be integral to the exit planning process.

If the supplier becomes insolvent, a customer generally has four options available:

- Source the services from a third party (although in many offshore relationships, the ability to switch supplier in the timeframe required will be limited).
- Bring the services back in-house.
- Fund the supplier or the relevant insolvency office holder to continue supplying the services.

## Related information

### Links from [www.practicallaw.com](http://www.practicallaw.com) and the web

This article is at [www.practicallaw.com/3-500-1941](http://www.practicallaw.com/3-500-1941)

### Topics

Outsourcing [www.practicallaw.com/0-202-2707](http://www.practicallaw.com/0-202-2707)

### Practice notes

Outsourcing: overview [www.practicallaw.com/2-202-1226](http://www.practicallaw.com/2-202-1226)

Offshore outsourcing [www.practicallaw.com/6-216-7962](http://www.practicallaw.com/6-216-7962)

Due diligence in outsourcing [www.practicallaw.com/2-381-2359](http://www.practicallaw.com/2-381-2359)

Outsourcing in the financial services sector [www.practicallaw.com/8-212-2982](http://www.practicallaw.com/8-212-2982)

Service levels and service credit schemes in outsourcing [www.practicallaw.com/1-211-9964](http://www.practicallaw.com/1-211-9964)

### Previous articles

Outsourcing: the commercial issues (2006) [www.practicallaw.com/1-201-8559](http://www.practicallaw.com/1-201-8559)

Outsourcing: sector-specific issues (2006) [www.practicallaw.com/0-201-9998](http://www.practicallaw.com/0-201-9998)

Outsourcing: ensuring ongoing competitiveness (2003) [www.practicallaw.com/0-102-2845](http://www.practicallaw.com/0-102-2845)

### External links

"A smart approach to sourcing"

[www.nortonrose.com/knowledge/publications/pdf/file17648.pdf?lang=en-gb](http://www.nortonrose.com/knowledge/publications/pdf/file17648.pdf?lang=en-gb)

For subscription enquiries to PLC web materials please call +44 207 202 1200

- Buy the insolvent business from the relevant insolvency office holder.

The contingency plan may include provisions to facilitate one, or a combination, of these options. It should be noted that a supplier's insolvency may not automatically constitute a breach of contract entitling the customer to terminate; the right to terminate should be expressly included.

*Mike Rebeiro is a partner and head of sourcing and Radford Goodman is a partner in dispute resolution at Norton Rose LLP.*

*Norton Rose LLP recently conducted an international survey of suppliers and customers of outsourced services (see "A smart approach to sourcing", [www.nortonrose.com/knowledge/publications/pdf/file17648.pdf?lang=en-gb](http://www.nortonrose.com/knowledge/publications/pdf/file17648.pdf?lang=en-gb)).*

**PLC IPIT & Communications**

**PRACTICAL LAW COMPANY**



**"It is considered a key reference tool by the team."**

Jane Clavin, Knowledge Services Manager, A&L Goodbody.

**PLC IPIT & Communications** is the essential know-how service for IP, IT & communications lawyers. Never miss an important development and confidently advise your clients on law and its practical implications. [www.practicallaw.com/ipandit](http://www.practicallaw.com/ipandit)