



Avoiding a G4S situation

7 ways of managing your risk in outsourcing

July 2012

The media furore over shortages of security staff for the London Olympics has led to much attention being focussed on the supplier, G4S. In this briefing, we look at ways to manage risk in outsourcing deals.

In 2010, G4S was appointed as Official Security Services Provider for the London Olympic Games, initially with a remit to provide 2,000 security staff. In 2011, after a review of security arrangements, it was asked to provide over 8,000 additional staff - a target which it has been unable to meet. As a result, the UK Government has had to draft in thousands of military and police personnel at short notice to bridge the gap.

What lessons can be drawn from this situation? Of course, the wider reputational issues are likely to constrain G4S regardless of the contract terms. But that won't always be the case in other situations, where the supplier may want to play hard-ball, notwithstanding that something has gone wrong. Here are our seven top tips for managing risk in outsourcing situations. The first three assist the customer, but the remainder are applicable to both customer and supplier.

1. Hedging your bets

Multi-sourcing - using several suppliers in parallel - may help to avoid over-reliance on a single supplier. The ability to compare one supplier's performance against others may also allow problems to be detected - and remedied - at an early stage. However, as well as being potentially more expensive, multi-sourcing can make it more difficult to manage the suppliers and ensure consistent quality. In LOCOG's case, the fact that the task is concerned with managing security - where quality control and coordination are key - may have led to a preference for a single supplier.

2. Due diligence

Could better due diligence, in preparation for the 2011 contract variation, have identified that G4S was unlikely to be able to meet its targets? At the time of writing, this is unclear.

Many projects run into difficulties because, at tender stage, suppliers are understandably eager to please and customers do not always have the expertise (or determination) to subject their proposals to sufficiently robust scrutiny. Targeted due diligence is always worthwhile and, in some cases, it can be helpful to seek external input from procurement specialists who can draw on practical experience of similar projects elsewhere.

3. The in-house option

In this case, LOCOG probably had no choice but to outsource, since it possessed neither the staff nor the expertise to handle security itself. But many businesses looking at outsourcing do have a choice.

Before making a decision to outsource, key questions to ask include:

- Is the function too business-critical to outsource? What is at stake if something goes wrong?
- Even if outsourcing is pursued, is it worth maintaining at least some in-house capability?

4. Supervision

In the run-up to implementation, contractual governance and reporting obligations may provide a helpful means of identifying potential problems e.g. delays by either the customer or supplier. If there are no such mechanisms, a counter

party may only become aware of the problem when it is too late to address it. It appears that, in G4S's case, extensive and regular monitoring structures were in place. But of course the monitoring still has to be fit for purpose - so there may be lessons to be learned from the G4S experience.

“Reputation is clearly an issue for G4S – but outside the media spotlight, suppliers may behave differently.”

5. Change control

Changing the contract requirements after signature is another common cause of problems with delivery. In this case, after the original contract was entered into, LOCOG requested that G4S provide substantially increased numbers of security staff. It is important for contracts of this type to allow for variations in order to adapt to changed circumstances - but where the proposed changes are quite significant, both parties may be well advised to re-examine (i) whether the new requirements can be delivered under the existing framework; and (ii) whether the provisions of the contract as a whole remain appropriate.

6. The right remedies

Media and political attention has focussed on whether G4S is subject to "penalties" - even though, as a matter of law, any true "penalty" would be unenforceable. This issue highlights the problems both parties face in agreeing, in the contract, a set of remedies which are both appropriate and mutually acceptable. Options include:

- **Service credits or liquidated damages:** Service credits are fixed payments or rebates due in respect of defined service defaults. These are what most people would call "penalties" (but drafted so as to be legally enforceable). G4S is subject to service credits, but they are capped. In most contracts, a cap of 5-10% of monthly fees applies, so where something has gone badly wrong, service credits are unlikely to provide full recompense for the loss caused.
- **Contractual damages:** Press reports state that LOCOG is entitled to retain or claw back certain sums - and that G4S has accepted that it should pay for the costs of deploying military personnel. But it is unclear whether G4S considers itself contractually obliged to meet those costs or has taken the decision primarily in order to limit reputational damage. And does it accept just the salary and accommodation costs, or also the "marginal" costs of disrupted training programmes etc? This highlights the need to think carefully about whether the framework of financial remedies - particularly liability caps and exclusions - bears a fair relation to the types and amount of loss likely to be incurred if something goes badly wrong.
- **Termination of contract:** This is an option of last resort which can sometimes also be helpful as a threat - but is not a practical option in a G4S-style scenario.

But also keep in mind that performing the contract needs to work for both parties – if one party is pressed too hard, and the contract becomes heavily uneconomic for them, that party may simply walk away. Sometimes the cost of continuing outweighs the cost of court proceedings.

In drawing up the contract, consideration should also be given to non-financial remedies, such as step-in rights. Step-in rights enable the customer to take over management of the service if things go seriously wrong and, if necessary, appoint another provider on an interim basis. However, such rights are only worthwhile if levels of monitoring are sufficient to enable problems to be identified in time.

7. Boilerplate pitfalls

Finally, it is important that both parties ensure that the "boilerplate" wording in the contract doesn't undermine the core substance of the contract they have agreed. For example here, does the "force majeure" exemption from liability cover non-availability of labour (as is often the accepted wording of such clauses)? Similarly, it would be unfortunate if the force majeure clause in a contract for disaster recovery services exempted the provider from liability in the event of a disaster. These issues are buried deep in the small print and are often overlooked.

For further advice on outsourcing contracts, please contact Tom Purton, Richard Brown or Dan Reavill or your usual contact at the firm.

“The contract needs to work for both parties - if one party is pressed too hard, it may simply walk away.”

Travers Smith LLP
10 Snow Hill
London EC1A 2AL
T +44 (0)20 7295 3000
F +44 (0)20 7295 3500



Tom Purton
Head of Commercial, IP and Technology
+44 (0)20 7295 3277
tom.purton@traverssmith.com



Richard Brown
Partner, Commercial, IP and Technology
+44 (0)20 7295 3254
richard.brown@traverssmith.com

www.traverssmith.com



Dan Reavill
Partner, Commercial, IP and Technology
+44 (0)20 7295 3260
dan.reavill@traverssmith.com