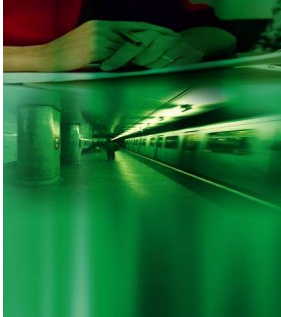


## A Review of IT Services for a Major Metro Client

### Introduction and background to the assignment



A major Metro industry client had engaged a leading IT services supplier to provide IT infrastructure support around the clock. However, within a few months of the contract starting, our Metro client managers were dismayed to find that the IT contractor was not meeting the requirements of the service specification, with consequent potential impact on 400 wide ranging systems.

While the IT contractor was generally complying with the requirements during office hours, there was particular concern about a perceived drop in standards at other times, on a 24/7 basis.

Our client therefore commissioned Touchstone Renard to conduct a professional and comprehensive audit and assessment of the IT contractor's performance, focusing on the areas of support where a detrimental outcome could cause increased risk to the operational railway.

Phil Austin, Managing Director of Touchstone Renard, says: 'As has often been the case, the combination of technical and inter personal skills and significant experience in the Metro sector was key to the success of the consultants deployed on the assignment.'

### Our task

We were required to carry out the assignment over a relatively short timescale, having regard to the urgency of a situation in which the services were potentially falling short of the specified standards. Broadly, our task was to investigate and analyse the performance of the IT contractor, taking account of the concerns of our client's managers, before reaching conclusions as to the nature and level of any consequent risks, and making recommendations for a remedial action plan.

Our client requested us to work to the UK government's Risk Analysis and Management Method (RAMM), which asserts that risk is dependent upon the relevant asset values, the threats and the vulnerabilities, from which a recommended set of counter measures can be produced.

Unfortunately, the timescales involved could not accommodate this methodology, so we adopted the US National Institute of Standards and Technology Risk Management Guide for Information Technology Systems.

This provided a structured methodology to determine the extent of potential threats and the associated risks within our client's IT infrastructure. We took the view that the output of this process would help to identify appropriate controls and counter measures for reducing or eliminating risk which could be translated into mandatory controls.

### How we went about it

In discussion with senior managers, we identified the areas of our client's business on which to concentrate. The selected areas were those which were considered to be the Business Critical Groups, namely:



- The customer support centre
- Depots
- Line control rooms
- The network control centre
- The power control room
- Signal control centres
- The track access control system
- The travel information centre
- The IT network

We identified the specific 'Business Critical' areas within these groups as being: Finance; Safety; Operations; Reputation; and Security.

The flow chart which we prepared for the selected methodology demonstrated the stages through which it was essential to proceed and the outputs for each stage:

- Step 1: Identifying the systems for investigation
- Step 2: Identifying threats and producing a 'threat statement'
- Step 3: Identifying and listing vulnerabilities
- Step 4: Analysing and listing current and planned controls
- Step 5: Determining likelihood of threats arising and producing a 'likelihood rating'
- Step 6: Undertaking an impact analysis and producing an impact rating
- Step 7: Assessing the adequacy of planned/current controls & producing an assessment of risk and associated risks
- Step 8: Making control recommendations

As independent consultants, it was our responsibility to interview our client's managers to understand the nature of their concerns but also to identify evidence to corroborate or disprove their perceptions.

The areas investigated were business critical, although they did not relate to the direct control of trains. It was fair to say, however, that if any of the relevant services were not performing properly, a critical situation could result.

### **What we achieved and our thoughts on the assignment**

Following completion of the various stages, we were able to present our client with a report containing the relevant outputs, detailing the evidence and setting out a comprehensive set of recommendations to ensure future compliance by the IT contractor with the required standards of performance and improved working arrangements.

Although we did discover evidence for many of our client's concerns, a key factor impacting on the views of managers was their perceived lack of control over the arrangement with the IT contractor. The contract for IT services had been entered into between the contractor and our client's parent organisation, at group level, leaving our client's managers in a situation in which they felt remote and powerless. We realised that it was going to be important to all concerned, moving forward, to bring about a situation in which our client's managers could benefit from direct communication with the IT contractor, without being impeded by an additional layer of management.

Such was the level of performance in certain areas; we recommended that the issues be raised with the contractor's board and that processes be put in place within the contractor's organisation to achieve a higher level of commitment to our client's business.

We also considered that our client's people would benefit from a range of improved internal systems and training.

It is always essential to receive feedback following any assignment and our client's senior managers were kind enough to tell us that they were highly satisfied with the work of the Touchstone Renard team, taking on the assignment at short notice and ensuring delivery within the specified timescales.