

INFORMATION SECURITY: HOW TO OUTSOURCE AND MAKE USE OF EXTERNAL SERVICES

[Introduction](#)

[Requirements](#)

[Selecting an outsourcing provider](#)

[Contract content](#)

[Implementation and operation](#)

[Contract termination](#)

[Other issues](#)

[Conclusions](#)

[Further help and advice](#)

This section is intended to provide guidance on outsourcing IT-based services. Some of the information contained here is particularly detailed and complex and may not, therefore, be relevant for all companies. We have, however, tried to ensure that there is advice for all organisations, irrespective of their size or experience.

Introduction

Outsourcing is often seen as a practice performed by large companies, about 66% of which wish to either make cost savings or concentrate on their core business. For example, a manufacturing company could use a third-party organisation to run its IT systems, this service being governed by an outsourcing contract. Small and medium enterprises (SMEs) are beginning to anticipate benefits from outsourcing, and many already use such facilities.

Some services have always been outsourced, e.g. most companies outsource the provision of web based services to an Internet Service Provider (ISP). This document is intended to act as a guide for companies which are considering outsourcing their IT-based services.

In such circumstances, cost savings are possible (in theory at least) in that a client (i.e. you) does not need to recruit specialists and/or retain expensive non-core skills. Outsourcing service providers can exhibit economies of scale, both through manpower and skills as well as hardware and network infrastructure. Other savings can be made if the operation is relocated to a cheaper environment. There is currently a tendency to relocate to India and other low-cost countries. India has an articulate, educated, English-speaking workforce, which costs very much less than the UK-based equivalent.

The theory is sound, but there are issues that cannot be ignored and security is one of them. Many outsourcing deals have failed, resulting in acrimony, loss and even bankruptcy (for both clients and outsourcing providers). If you fail to understand your own requirements for outsourcing, so will any service provider you ask to run a part of your operation. This is the root cause of most outsourcing failures with security being one of the prime areas of potential misunderstanding.

What has been learned from previous outsourcing work is that whilst the responsibility for implementing security controls may be delegated, the accountability for such security cannot be outsourced. The contract has to be managed with the client organisation retaining ultimate responsibility. The implementation of control via a contract is different from implementation via a chain of internal command and, as such, requires a different approach. This notwithstanding, your organisation remains accountable and ultimately responsible for the security of the assets being outsourced. After all, it's your company which will suffer the impact and consequences if something goes wrong.

Outsourcing is a complex issue and information security is only one of a number of areas for consideration when investigating the possibility of outsourcing. There are significant Human Resources (HR) risks. For example, many staff will become concerned about job security. This will have an impact on productivity. Some may even actively seek to thwart any plans for outsourcing.

The following sections outline a 'road map' for successfully implementing an outsourcing contract.

Requirements

Your requirements are the most important guide you will have to outsourcing any part of your business operation. These therefore have to be made intelligible to your chosen service provider and set out in a clear, unambiguous and mutually beneficial contract.

Many outsourcing providers make the mistake of trying to 'shoe-horn' an operation into their generic offering. This may have the advantage of reducing your costs, but could result in loss of service capability.

One of the best ways to set out your requirements is to assemble a team from across the organisation. Each person will have different responsibilities, but members should include appropriately empowered representatives from each of the following key business areas:

- Human Resources
- Information Technology
- Information Security
- Legal.

The team should be a decision-making body but also provide a channel through which issues can be passed to the most senior decision-makers. The team should analyse each business process that will be affected by the proposed outsourcing and establish the various risks that could impact on it.

Examples of such risks include:

- exposure of a company's sensitive and critical information to another party
- exposure of personal information
- relocation of IT equipment from a known, safe environment to an unknown environment
- no direct control over the recruitment process.

The risks need to be identified and evaluated to determine what controls are required to manage them. In the case of outsourcing, most of these take the form of a statement in a contract. They also form part of the client requirements. Note that not all requirements are directly related to information security. Many, if not most, are more concerned with service levels and cost. However, all these requirements have to be collated into a meaningful form that can be used as the basis for an Invitation To Tender (ITT). They can also be used to assemble a Request For Information (RFI), usually sent to identified prospective service providers prior to the full ITT being issued.

The ITT should include a clear set of requirements. Some people recommend that these should be set out in a formal requirements specification at this stage. How far to go in setting requirements depends very much on the nature and scale of the process or processes that are to be outsourced.

Security requirements

Security requirements normally include the following:

- the information security policy to be used (normally directly based on the client's own policy and standards)
- roles and responsibilities (both client and outsourcing provider)
- mandatory practices, e.g. access control processes, back-up and recovery
- the various service levels for providing confidentiality, information quality and recovery from incidents
- rights of inspection and audit.

ISO/IEC 27002 contains a clause dealing with security requirements in outsourcing contracts. In addition, ISO/IEC 20000 (previously BS 15000) has some useful advice on IT service management (for more information please visit www.bsi-global.com).

Selecting an outsourcing provider

Selection is best managed as follows. The first stage is to identify potential service providers. This can be done through a mixture of research (web searches, advice from Chambers of Commerce and through recommendation) and active RFIs. You should seek out those providers who seem best placed to meet your initial requirements and then select a shortlist. The chosen service providers should then receive a full set of your requirements, set out in an ITT.

Outsourcing providers will normally respond with a proposal and after discussions with the outsource team, a suitable provider can be chosen and contracts drawn up.

Contract content

The box below outlines the types of issues that need to be considered as part of the security requirements. They are set out here because these requirements often overlap with other areas within an organisation (such as HR and facilities management) and need to be discussed within the internal outsourcing team. The statements could eventually form the basis of the agreed contract.

Not all the statements in the box will work in all cases. They are provided as an example to show how they might be worded. It is likely that your own contracts will require ratification by legal experts before issue.

Non-disclosure agreements and technical resumés

The outsourcing provider will name all staff assigned to work on the client account and pass these names to the client. They will all sign a Non-Disclosure Agreement (NDA) supplied by the client prior to starting work on the account.

The technical Curricula Vitae (CVs) of named staff working for the outsourcing provider will be supplied to the client for approval. This approval must be sought and obtained before the members of staff start work on the client account.

If, for emergency reasons, it becomes difficult to implement these practices, outsourcing staff can commence work without taking the above steps providing explicit signed permission is granted from the client outsource contract manager or the client information security manager. The NDA must be signed at the earliest available opportunity thereafter. The CVs must also be supplied as soon as possible.

Staff awareness

All outsourcing staff will be given training in information security as agreed with the client and will be given a pack outlining:

- this agreement
- the client information security policy and standard
- their roles and responsibilities.

All outsourcing staff will be made aware of the potential consequences of a breach of this contract.

Staff vetting

All outsourcing staff named as working on the client account must be subject to checks (preferably as part of the outsourcing provider's recruitment process) prior to being accepted to work on the client account. Screening must include:

- taking up at least two references (one personal, the other relating to previous employment)
- a criminal record check
- proactively checking the accuracy and completeness of CVs
- the positive confirmation of academic and professional qualifications
- a positive identity check (e.g. sight of passport or identity card)
- a credit check

The outsourcing provider will inform the client immediately if they intend to use sub-contractors to fulfil the contract. The client reserves the right to refuse such a service. If any sub-contract is agreed, the sub-contracted body will be required to sign a formal agreement and an addendum to this contract and abide by all the conditions set out therein.

Physical security

The outsourcing provider's staff should access client systems only from specific named premises. These premises should normally be subject to a risk review to determine their security status as part of any risk analysis procedure required by the client. The review should assess the premises against the client's physical security policy.

Implementation and operation

The timing of the handover of an operation to an outsourced service is complex and risky. As many as one-fifth of contracts are terminated during transition due to unexpected problems.

Handover has to be planned and a range of measures, such as acceptance criteria, has to be put in place. If discussions prior to the contract being signed have been sensible and realistic, problems can be reduced.

Security issues are very important at this stage as the complexity and unfamiliarity of such situations can result in security incidents (deliberate or otherwise). Such a situation provides opportunities for fraud, vandalism and theft. Basic security controls have to be monitored and concerns actively investigated. Much of this vigilance will not produce results but the security ethic has to be applied.

To help avoid confusion, a strict timetable should be set up. Everyone should know exactly when responsibilities will transfer. This will reduce some uncertainty and ensure legal responsibility is understood and accepted.

One essential element is a 'get-out' plan (or exit strategy) in case the handover fails. A return to the original service may be a last resort, but should be borne in mind. Remember that the purpose of the process is to support the business.

Operationally, things will take time to settle down. There are some simple routines that can reduce negative security impacts as this happens:

- Keep to formally agreed roles. If informal routines become commonplace, it is possible that they will become contentious issues over time. You have to manage expectations for both the outsourcing provider and the client staff.
- Client staff have to understand that the outsourcing provider's staff will sometimes change. The value of personal relationships needs to be weighed against the provider's requirements for making best use of its own staff.
- Regular, formal meetings need to be held to assess and agree the status of the service. These should be specified in the contract.
- Incident reporting, as well as status reporting, has to be established. Reporting lines and procedures have to be transparent and agreed.
- Change is inevitable, in both requirements and operations. The contract has to be flexible and a workable routine for managing change is essential. Change can come from either the outsourcing provider or the client side and has to be seen as part of the operation. Nothing stands still and this has to be built into the contract and the relationship.

Contract termination

As part of the 'get-out' plan (or exit strategy), there must be mutually agreed provision for contract termination at any stage. Safeguards must, of course, be built in to prevent either party being unfairly penalised through termination, but just as contracts have to be operationally flexible, the terms have to be sensible.

Other issues

It is not the purpose of this document to provide advice outside the domain of information security, but the issue that dominates most outsourcing projects is that of people. Individuals dislike change, especially when they feel powerless, and outsourcing can bring about very fundamental changes.

The key to ensuring as smooth a change as possible is to keep people informed, seek their opinions and take these on board as far as possible. If there are negative impacts (redundancy, relocation, etc.) then HR involvement is essential. This involvement will make the outsourcing process more transparent and acceptable.

Conclusions

- Remember that outsourcing requires a multilateral approach. An internal team approach to gathering requirements is essential.
- You cannot outsource responsibility.
- Garbage in, garbage out (GIGO): if you have a poor system, outsourcing will not make the problem go away. It will merely cause you expense, suffering and loss. Ensure that the system is right first.
- If you take advantage of your outsourcing provider in terms of price, they will respond with an equivalent drop in goodwill and service levels.
- Keep roles and responsibilities clear and concise and stick to them, especially during the early stages of hand-over and operation.
- Keep the people whom the outsourcing will affect involved; understandably they can sometimes feel threatened if they are left out of the process.
- Have a 'get-out' plan (or exit strategy).

Further help and advice

General

BERR Information Security Health Check Tool

<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page

www.berr.gov.uk/sectors/infosec

BERR Information Security Business Advice pages

<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)

<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>

Published by the Department for Business, Enterprise & Regulatory Reform
www.berr.gov.uk

© Crown Copyright. URN 09/645.