



NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

Good Practice Guide

Outsourcing: Security Governance Framework for IT Managed Service Provision

Issued 2 August 2006

Abstract

This paper provides a guide for Critical National Infrastructure organisations on managing information security when part, or all, of the organisation's IT provision has been outsourced to a Managed Service Provider. It provides a framework for managing information security throughout the contract lifecycle and also contains a number of illustrative contractual clauses that organisations may wish to refer to when drafting IT outsourcing contractual requirements.

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, NISCC accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

**National Infrastructure
Security Co-Ordination Centre**
PO Box 832
London
SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

KEY POINTS	4
INTRODUCTION.....	5
THE PURPOSE OF THIS DOCUMENT	5
READERSHIP.....	5
DOCUMENT HISTORY	5
WHY YOU SHOULD READ THIS DOCUMENT	7
STRATEGIC BUSINESS CONTEXT.....	9
ROLES AND RESPONSIBILITIES	13
KEY CUSTOMER ROLES AND SECURITY RESPONSIBILITIES	13
KEY SUPPLIER ROLES AND SECURITY RESPONSIBILITIES	14
RISK ASSESSMENT.....	16
MANAGING SECURITY DURING THE OUTSOURCING PROCESS.....	18
SUPPLIER CAPABILITY AND COMPETENCE.....	18
COMMUNICATING THE SECURITY REQUIREMENT – AND SUBSEQUENT SECURITY MANAGEMENT AND ASSURANCE	19
SECURITY DURING THE TRANSITION	22
ONGOING SECURITY MANAGEMENT.....	22
FORCE MAJEURE.....	23
ASSURANCE AND CONFORMANCE.....	24
SECURITY IN THE CONTRACT LIFECYCLE.....	26
CHANGE MANAGEMENT	32
INCIDENT MANAGEMENT	33
TERMINATION	35
FURTHER ADVICE.....	35
APPENDIX A - ILLUSTRATIVE CONTRACT CLAUSES	36
RESPONSIBILITIES, RISK, COMPLIANCE AND COMPETENCE.....	36
COMMUNICATION OF SECURITY REQUIREMENTS OPTION 1 – DETAILED CONTROLS SPECIFICATION	40
COMMUNICATION OF SECURITY REQUIREMENTS OPTION 2 – CONTROL OBJECTIVE BASED SPECIFICATION/ASSURANCE.....	41
COMMUNICATION OF SECURITY REQUIREMENTS OPTION 3 – ISO27001 ISMS	42
ASSURANCE AND CONFORMANCE.....	42
APPENDIX B – GLOSSARY OF KEY TERMS.....	45

Key points

- This document is a guide to managing security when outsourcing to a managed IT service provider, whether for a new project or system, or an existing project or system.
- The document is specifically aimed at non-technical people.
- There are a number of potential security pitfalls when outsourcing which can be avoided.
- Security can be managed effectively using an Information Security Management System (ISMS) and still enable delivery of outsourcing benefits.
- Customer organisation management remain accountable and responsible for ensuring security risk management.
- Key responsibilities need to be defined.
- Outsourcing suppliers should remain responsible for security within their subcontractors.
- Risks should be assessed and compliance requirements understood.
- Supplier capability needs to be established.
- Security requirements need to be communicated contractually.
- Security need to be managed continuously.
- Assurance should be gained that security is effective.
- Security steps exist throughout the project lifecycle.
- Security needs to be managed during change – and changes have security implications.
- Suppliers should be obliged to report and manage incidents.
- Security needs to be managed during contract termination.

Introduction

The purpose of this document

1. This document intends to be a guide to managing security when outsourcing to a managed IT services provider in a way which efficiently and effectively manages the security risks throughout the life of the contract, and provides assurance that the security risks are managed. In particular, this document is intended to be used when the security risks to be managed are quite considerable, for example in UK Government and Critical National Infrastructure areas. In these cases, business impact of security failure could be material and threats to security may be elevated, for instance when suppliers opt to use offshoring within the service delivery approach.
2. It is not intended to replace established information security standards issued by industry bodies, standards organisations or regulators; instead, this document aims to provide a framework for applying those standards effectively when outsourcing. Likewise, the document does not aim to address all aspects of IT management or procurement, but only those directly related to security management in outsourcing.
3. This document should be consulted from the very start of any process to outsource IT systems.
4. The example contractual clauses included in this document, as appendix A, are for illustrative purposes and do not constitute professional legal advice. They should not be regarded as a substitute for detailed advice in specific cases.

Readership

5. This document aims to provide helpful advice to a wide variety of people, including:
 - Senior business and IT managers with overall responsibility for outsourcing an IT function
 - Procurement specialists involved in the outsourcing procurement cycle
 - Security professionals (both general and IT) involved in outsourcing
 - Accreditors and assurance professionals of customers whose assets may be part of the Managed Service

Document history

6. This document was created to meet a set of requirements prepared in 2005 by the National Infrastructure Security Co-ordination Centre (NISCC) in conjunction with the Managed Service Information Exchange (MSPIE).

7. Readers should check that they are using the latest version by visiting the NISCC website. Feedback is encouraged and should be submitted to NISCC via email - feedback@nisc.gov.uk

Why you should read this document

8. Managing security in outsourcing is a complex area to manage successfully which cannot be dealt with in a simplistic way. There are a number of pitfalls to be avoided; the significant ones are detailed below.

- The customer is unaware of the security risks involved, in terms of the business impact of compromise of the information/systems, the threats to the information/systems, and their current vulnerabilities.
- Project sponsors and service managers from the outsourcing organisation do not consider themselves accountable for security.
- Customers do not make suppliers aware of the security risks relating to the business areas and IT systems being outsourced.
- Customers assume that suppliers will implement best-practice security, when in fact suppliers may only implement what they have been contracted (and paid) to do.
- Customers assume that security is often inferred as part of functionality requirements, when in fact the requirement for security needs to be explicitly specified.
- Contracts aim to over-simplify security requirements into contract clauses, such that the resulting security measures may be ineffective in countering the risk.
- Contracts fail to invoke security requirements, meaning that the supplier is not obliged to implement and operate required security measures.
- Customers specify draft, imprecise or inconsistent policies or security standards to be complied with, or refer incorrectly to standards or codes of practice which allow considerable variance in interpretation.
- Customers inadvertently sign up to levels of security which were in place at the time of transitioning, as identified by a supplier's operational review, and are surprised by scope-changes relating to security later on.
- Customers try to micro-manage and specify security requirements with such detail that the supplier has little room for innovation or flexibility, constraining their ability to deliver other outsourcing benefits such as economies of scale or cost-savings.
- Customers inadvertently continue to manage security at the detailed level, even though the intent was that the work should be outsourced, thereby duplicating effort and confusing accountabilities.

- Customer management tacitly permit reductions in security, functionality or service level if they are not measured or accountable for them.
- Supplier commercial directors and service delivery managers do not consider themselves to be accountable for security as a key part of the customer contract.
- Suppliers fail to allocate sufficient skilled, experienced and qualified resources to security management.
- Suppliers cut back on security processes which are not explicitly contracted for, in order to meet cost-savings targets or increase contract margin performance, and as a result security patch management, intrusion detection, monitoring, and secure system design and build processes do not happen.
- Suppliers will seek any opportunity to reduce costs and increase margin, including sub-contracting of services or offshoring of services unless the contract prohibits it.
- Suppliers may resist customer attempts to gain visibility of security processes, or to commission assurance reviews or audits of security.
- Supplier-provided assurance often fails to meet customer requirements.
- Suppliers deal with post-contract requirements for security improvement as material scope extensions, sometimes considerably increasing charges (often inflated commercially by considerable scope-change margins) to the customer.
- Suppliers may resist requirements to change security measures once contracts are signed if they consider that such changes are commercially unattractive to them.

Strategic business context

9. Outsourcing is driven by a business or commercial strategy to achieve a number of aims, in pursuit of the strategic goals of an organisation. These aims may include:

- Cost savings
- Accounting or balance sheet improvements
- Increased agility and flexibility
- More attractive financing or funding options
- Speed of exploitation of new technologies or capabilities to deliver competitive edge
- Elimination of non-core activities
- Rapid implementation of a major change in strategy or approach which could not be done in-house for cultural, resource or capability reasons
- The need for new or increased capability which had never been implemented and operated in-house

10. Many organisations are subject to a number of compliance, regulatory, legal or operational risk management regulations, including corporate governance requirements.

11. The areas being outsourced remain the governance, compliance and risk management responsibility of the customer organisation and their management, and the customer should ensure that:

- Risks and compliance requirements are understood by themselves and by the supplier
- Security requirements are clearly articulated
- Risks are managed appropriately;
- Assurance is gained from the supplier that risks are managed
- Incidents are reported, investigated, and corrective actions taken

12. The processes which combine to achieve these objectives form an Information Security Management System (ISMS) for the outsourced services.

13. When suppliers sub-contract work, they should repeat the outsourcing security management process with their sub-contractors, such that the ISMS covers the entirety of the information and systems outsourced by the customer.

14. The process can be described by the diagram below:

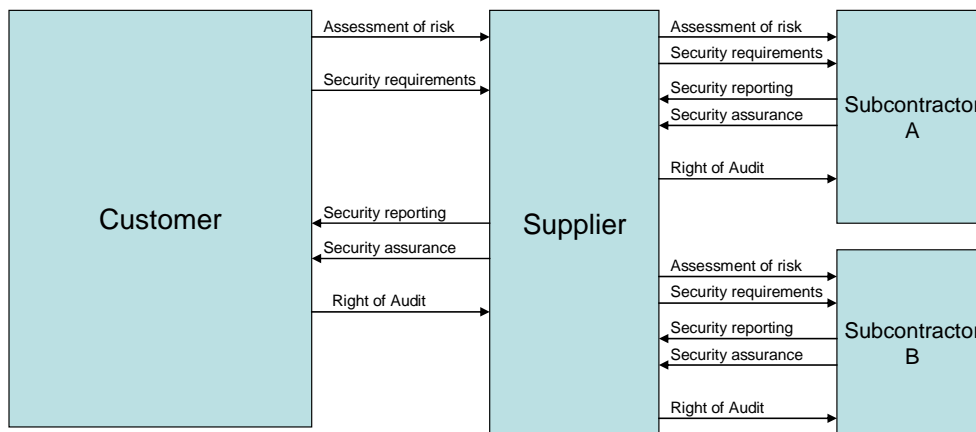


Figure 1: Overall information security management process

15. It is particularly important that customer management ensure that the benefits of outsourcing can be realised once the costs and constraints of security are taken into account. It may be found that the business to be outsourced is so sensitive and security threats so great that any savings from outsourcing are offset by the supplier's security costs in the outsourced operation, combined with the customer's costs of managing the supplier and gaining assurance from a security perspective.

16. Many large outsourcing suppliers are very competent at security provided the customer contracts for it. To allow economies of scale to be exploited resulting in higher levels of service and cost savings for the customer, the supplier must be able to use 'leveraged' delivery infrastructure whilst managing customer security risks and providing assurance.

17. Maintaining continuity of security management during the entire outsourcing transition process is key to management of risk.

18. It is particularly important that suppliers must be able to meet the requirements of the contract (including management of security) whilst still making a commercial profit.

19. The ISMS of the outsourced operation (i.e., the ISMS of the prime contractor, as well as sub-contractors and sub-sub-contractors which by definition are the prime contractors responsibility) and its scope definition within the contract should embrace not only 'traditional' IT security aspects surrounding the service, but also wider areas which have a far greater bearing on the security risk relating to the customers information and systems. These wider areas are normally taken for granted when IT services are in-house, and include:

- Management of political and security risks relating to the local environment which affect security and continuity of information, systems and services
- Management of security of physical and electronic documents and other information relating to the services provided to the customer, including protective marking of materials and protective-marking specific handling procedures
- Management of physical security of facilities from which services are delivered
- Management of personnel security within the outsourcing operation
- Management of security investigations within the outsourcing operation
- Management of security of information relating to any aspect of the contract within the service provider's organization (and their sub-contractors and sub-sub-contractors)

20. In particular, the ISMS must additionally embrace management of security on leveraged supplier infrastructure, such as

- Remote and shared systems management facilities
- Utility computing, storage and backup/archive services
- Business continuity planning and disaster recovery arrangements
- Shared networks and network security systems
- Shared hosting facilities
- Privileged access and entitlement management systems and processes, as outsourcing suppliers often need to employ large central teams of subject-area specialists (such as systems administrators), often requiring privileged access to be potentially available to a far wider group of people than for in-house operation.

21. Security management of shared and infrastructural aspects must be sufficient for the risks related to the most sensitive information and systems dependent on them and the greatest threat faced by them. Customers must ensure that this is represented in contractually binding risk assessments, controls specifications and other contractual aspects.

22. The elements of managing security when outsourcing are shown in the following diagram. These elements are explained in detail in the remaining sections of this document.

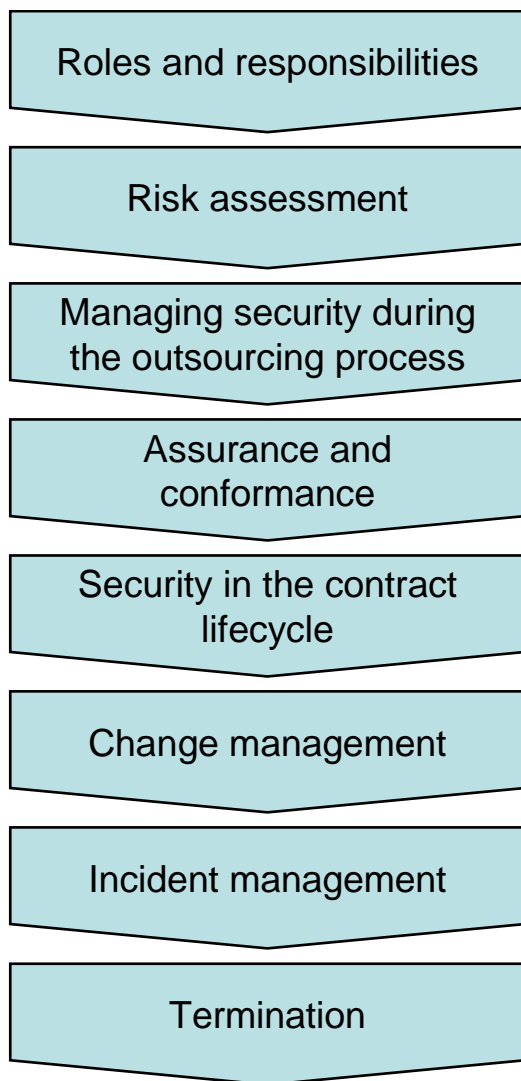


Figure 2: Overall security management elements

Roles and responsibilities

23. When outsourcing, there are a number of particularly key responsibilities to be established, initially at the customer organisation, subsequently in supplier organisations when bidding for the contract, and finally within the organisation of the successful bidder. Contracts should establish key security roles and responsibilities within customer and supplier organisations. In the following table, the adjective “outsourcing” refers to the customer organisation.

Key customer roles and security responsibilities

Outsourcing Project Sponsor	<p>The senior manager responsible for sponsoring the outsourcing project is ultimately accountable for ensuring that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood; • the acceptable level of residual risk is agreed by the organisation; • security requirements are clearly articulated; • an appropriate security framework is followed; • security risks are managed during the outsourcing lifecycle; and • assurance is gained that security risks are managed and that processes are in place to sustain security risk management.
Outsourcing Project Security Manager	<p>The outsourcing security manager is accountable to the outsourcing project sponsor for operationally ensuring that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood; • the acceptable level of residual risk is agreed by the organisation; • security requirements are clearly articulated; • security risks are managed during the outsourcing lifecycle; and • assurance is gained that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken. <p>The outsourcing project security manager should be professionally qualified and experienced in security management.</p>
Outsourcing Procurement Manager	<p>The outsourcing procurement manager is accountable to the outsourcing project sponsor for ensuring that contracts and schedules effectively:</p> <ul style="list-style-type: none"> • communicate the security risks and compliance requirements; • state the security requirements; • ensure security risks are managed during the outsourcing lifecycle; and • ensure assurance is gained that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken.

Outsourcing Transition and Service Manager	<p>The outsourcing service manager is accountable for ensuring that outsourced services continue to be managed such that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood; • security requirements are clearly articulated; • the acceptable level of residual risk is agreed by the organisation; • security risks are managed during the outsourcing lifecycle; and • assurance is gained that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken.
Accreditor or third party assessor/regulator	<p>The accreditor or customer appointed third party assessor/regulator is responsible for ensuring that:</p> <ul style="list-style-type: none"> • security controls implemented by the supplier correspond to those required in the contract; and • assurance is gained that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated and corrective actions taken.

Key supplier roles and security responsibilities

Senior Commercial Director	<p>The senior commercial director responsible for bidding for and subsequently delivering the outsourcing contract is accountable for ensuring that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood by the supplier organisation; • the acceptable level of residual risk is agreed by the customer; • security risks are managed during the outsourcing lifecycle; • assurance is gained and provided to the customer that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken; and • representations to the customer are complete and true.
Supplier Security Manager	<p>The outsourcing security manager is accountable to the senior commercial director and the supplier transition manager and service manager for operationally ensuring that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood; • the acceptable level of residual risk is agreed by the organisation; • security risks are managed during the outsourcing lifecycle; and • assurance is gained that security risks are managed

	<p>and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken.</p> <p>The outsourcing supplier security manager should be professionally qualified and experienced in security management.</p>
Supplier Transition Manager and Service Manager	<p>The outsourcing transition manager (and subsequently) the service manager is accountable for ensuring that outsourced services continue to be managed such that:</p> <ul style="list-style-type: none"> • security risks and compliance requirements are understood; • the acceptable level of residual risk is agreed by the organisation; • security risks are managed during the outsourcing lifecycle; and • assurance is gained that security risks are managed and that processes are in place to sustain security risk management and ensure incidents are reported, investigated, and corrective actions taken.
Other responsibilities	<p>Other responsibilities relating to security will be defined depending on the nature of the activities being outsourced.</p>

24. Customer contracts with suppliers should ensure that suppliers remain accountable and responsible for all actions of subcontractors contracted by them and are responsible for managing security into all sub-contractors and sub-sub-contractors and providing assurance to the customer in the agreed forms.

Risk assessment

25. Before the decision is taken to commence the outsourcing process, security risks should be assessed. The risk assessment is vital to ensuring that the organisation understands its security requirement, as well as ensuring potential outsourcing suppliers understand the risk they are expected and contracted to manage.

26. In addition, the risk assessment should consider the governance, regulatory, and compliance standards to which the organisation is bound. This may be achieved by drawing up a list of applicable regulations and standards and considering the impact of each of these on the intention to outsource and the controls required to manage the compliance risk.

27. Risk assessment should be carried out using ensuring the six key steps below are covered. The risk assessment should be facilitated by a qualified and experienced information security professional, with input from business, IT, and procurement management. The NISCC guide to risk management¹ “Risk management and accreditation of information systems”, which is the same as the UK government’s Information security Standard No 2, should also be consulted to provide a framework for risk management in the procurement process. The following does not specify any particular risk assessment method. For UK government, the current version of CESG’s Information Security Standard No 1 should be consulted.

- a) Identify the **business processes and functions** whose underlying information systems are to be outsourced, based on the scope of the intended outsourcing.
- b) For each business process or system, identify the **specific governance, regulatory or compliance standards, key technical strategies or architectures, or other material constraints** (such as the requirement to provide services only from within the UK where legally possible) which apply to the customer’s business and their industry sector, and the implications of those constraints.
- c) For each business process or system, carry out a **Business Impact Assessment** to understand the impact of loss of Confidentiality, Integrity or Availability of the system, using a scale of impact levels for each of Confidentiality, Integrity and Availability.
- d) Assess the **security threats** to the business and its systems, in terms of the people/organisations that might attack it, and their motivation and capability to do so. CNI organisations should obtain up-to-date, authoritative threat information from NISCC. (Note that the threat information likely to influence the risk assessment the most - and subsequent security and outsourcing decision-making - is also likely to be the most sensitive).

¹ <http://www.niscc.gov.uk/niscc/docs/re-20050804-00653.pdf?lang=en>

- e) Review the **current vulnerabilities and compliance status** of each system, and identify the residual risk level which is acceptable in line with the organisation's risk appetite.
- f) Identify the **gap** between the current level of residual risk and compliance and the target level of residual risk and compliance when outsourced. (Note that if security improvements are needed to close the gap then additional transition and operational security costs will be involved).

28. The risk assessment process should take into account the possibility that additional vulnerabilities and threats may be introduced by the act of outsourcing.

29. The risk assessment results should be documented such that the Outsourcing Project Sponsor can review and approve it.

30. When providing information to suppliers during the procurement lifecycle, including at contract stage, the procurement manager should ensure that the assessment of risks and the list of governance, legal, regulatory and compliance standards which apply should be communicated to the supplier as a core part of the contractual service requirement. However, it should be noted that security risks may be sensitive to the customer and so a level of sensitivity is required as to how these are shared with the supplier.

31. Confirmation should be sought that the supplier(s) understand the implications of the risk assessment and compliance requirements.

32. The onus lies on both customer and supplier to be open and honest when agreeing assessments of risk.

33. Should either party wilfully fail to inform the other of a known material security risk which then manifests itself, that first party should expect to be held liable for the consequences on themselves and on the other party. If one party refuses to accept existence of a risk (and to implement necessary protective security measures) identified and insisted upon by the other party, they should be prepared to indemnify the other party against the consequences of its manifestation.

Managing security during the outsourcing process

34. Once a risk assessment has been carried out, it is possible to articulate security requirements such that they can be communicated to the outsourcing service provider.

35. There are a number of ways in which these requirements can be communicated – and for the security to be effective, each way requires a corresponding approach to managing security and gaining assurance that requirements have been implemented by the supplier.

36. Early in the outsourcing process, for example before Request for Information responses have been received from suppliers, it may not be clear which approach is best to use: nevertheless the assessment of risk and the statement of compliance / legal / regulatory requirements should be clear and ready for communication to potential suppliers.

37. Care should be taken to ensure that any internally developed policies and standards articulated as compliance requirements have been properly reviewed for fitness-for-purpose and consistency, as these will have a bearing on a diligent supplier. Poorly conceived internal standards could significantly distort and disrupt contract security performance, resulting in outsourcing benefits realisation difficulties.

38. Once more detailed system and service requirements are communicated to suppliers, a method of managing security can be defined in conjunction with the suppliers and specific security requirements communicated.

Supplier capability and competence

39. The key influencing factors in determining the method of managing security are the nature of the contract, the strategic intent behind it, and the capability of the supplier. This is especially important in high-risk or highly regulated areas.

40. If it is intended that the customer does not retain a large team of security professionals to micro-manage security in the contract, it is vital that the supplier demonstrates proven capability in security management, and that they are contracted to manage security using an approach which delivers the required security and assurance to the customer, without burdening the customer.

41. If, however, the contract is straightforward, of limited scope, unlikely to change in requirement or scope, and the customer has the necessary security resources, it may be possible for a less capable supplier (in terms of security management) to be used.

42. The customer should commission a security management capability due diligence review of the supplier (perhaps as part of a wider due diligence review), and check qualifications and credentials. The results of this review should influence the choice of the supplier as part of the supplier selection

process, as well as the style of customer-supplier security management to be used. Supplier motivations and loyalties should strongly align with the customer, especially in high-risk or highly regulated areas.

Communicating the security requirement – and subsequent security management and assurance

43. The security requirement to the contractor can be split into three distinct types:

- a) Requirements which set the overall security management context for the outsourcing contract and are communicated contractually at the beginning of the contract,
- b) Requirements which are set and become contractually binding during the course of the contract, according to an agreed security management process contracted between the customer and the supplier at the start of the contract,
- c) Requirements which relate to day-to-day operations, such as requirements to change user registration details or alter access control settings, investigate an incident, or interface with internal customer processes, the performance of which should normally be part of the scope of the contract.

44. The table below summarises security requirements communication, management and assurance approaches which are likely to help ensure risks are managed in accordance with customer expectations.

Option	Approach	Features
<p>Option 1 - Detailed controls specification</p>	<p>Customer specifies in detail:</p> <ul style="list-style-type: none"> • the assessment of risk; • the compliance requirements; and • the security requirements, in terms of the detailed controls to be employed, and the level to which those controls are employed for every system in the inventory of the services being outsourced. <p>ISO17799:2005 may be used as a basis to identify the control areas to be specified, though other security standards may be used.</p> <p>A detailed system-specific security policy is contractually invoked for each system (or group of systems).</p>	<p>Customer is likely to spend considerable security professional resource specifying and negotiating the controls with the supplier.</p> <p>Customer can be specific about exactly how security is to be operated.</p> <p>The supplier is likely to be constrained in what they can and cannot do.</p> <p>Customer takes responsibility for the fitness for purpose of the detailed controls specification.</p> <p>Any control not specified</p>

	<p>Supplier operates security in accordance with the detailed system-specific security policy, developing whatever technical configurations, standards, procedures, records or processes required to implement the controls. The customer should specify as part of the system-specific security policy which elements of the controls are to be documented and supported by retained, documented records.</p> <p>Customer gains assurance from a combination of:</p> <ul style="list-style-type: none"> • security performance reporting; • customer-commissioned security audits; • reports from supplier-commissioned security audits; and • letters of representation from supplier. <p>Customer requires supplier to use a similar approach with all subcontracts (and sub-sub-contracts).</p>	<p>will not be carried out by the supplier – the control specification is likely to override any intent implied in communication of risk assessments or compliance requirements.</p>
<p>Option 2 Control-objective based specification with independent third party review</p>	<p>Customer specifies in detail:</p> <ul style="list-style-type: none"> • the assessment of risk; and • the compliance requirements; <p>and invokes them within the contract.</p> <p>Customer develops a set of high-level control objectives in conjunction with the supplier and a 3rd party independent auditor.</p> <p>Supplier transforms high-level control objectives into detailed system security policies, procedures, physical security, technical configurations and personnel security measures (perhaps using</p>	<p>Customer is likely to spend less professional security resource on detailed controls specification.</p> <p>Supplier has considerable flexibility in determining how to meet the requirements of the control objectives.</p> <p>Supplier costs may increase due to the need to commission 3rd party audit work.</p> <p>Assurance approach inherently integrated</p>

	<p>ISO17799:2005 as a guide for completeness).</p> <p>Supplier operates system in accordance with detailed system security policies.</p> <p>Customer contractually requires supplier to provide a management attestation and to commission a 3rd party audit review, for example using SAS70 principles and which may be a formal SAS70 audit, to provide assurance that control objectives have been complied with.</p> <p>Customer requires supplier to use a similar approach with all subcontracts (and sub-sub-contracts).</p>	<p>with the security management approach, and can meet assurance requirements of regulatory compliance reporting.</p> <p>3rd party review opinion by regulated audit firm can provide strong reliance due to the liability taken on by the auditor.</p>
<p>ISO 27001 ISMS with certification</p>	<p>Customer and supplier agree the risk assessment, compliance requirements specification and control objectives to be used as the basis of the ISO27001 ISMS.</p> <p>The ISO27001 Statement of Applicability is defined to include the entire scope of the outsourcing contract and all people, processes, facilities and systems supporting it if full coverage is to be achieved.</p> <p>Supplier implements, operates, monitors, reviews, maintains and improves the ISMS in accordance with ISO 27001, carrying out all ISO27001 requirements.</p> <p>Supplier commissions ISO27001 registered auditor to review the ISMS and grant ISO27001 certification.</p> <p>At the customer's option, the supplier contracts with a regulated audit firm who are also registered ISO27001 auditors to provide dual assurance, comprising ISO27001 certification and a SAS70 opinion.</p> <p>Customer requires supplier to use a</p>	<p>ISO27001 ISMS involve considerable formalised processes and documentation. This is likely to be costly to implement on a custom IT outsourcing operation, but may be cost-effective when using components of leveraged, shared infrastructure.</p> <p>It is vital to ensure that the risk assessment, control objectives and Statement of Applicability represent the customer's risk assessment, control requirements and contract scope for a certification to be relied upon.</p> <p>ISO27001 audits are often procedural in nature, with the certification company accepting little legal liability to those to whom</p>

	similar approach with all subcontracts (and sub-sub-contracts).	the certificate is granted, and none to those relying on it.
--	---	--

45. One of these approaches should be selected and implemented contractually at the outset of the contract.

Security during the transition

46. To ensure security risks continue to be managed during the transition, there should be a security management transition plan developed by the customer and the supplier jointly, the first part of which transitions current security operations to the supplier alongside service transitioning. The second part of the plan should be the supplier's responsibility to execute, to transition the ISMS into one which meets the risk assessment, compliance requirements, control specification and other contractual requirements.

47. Co-development of the first part of the plan should be a contractual obligation on the supplier (alongside service transition planning), and development and execution of the second part, to complete the ISMS transition to the 'final state' should be a contractual obligation on the supplier, with clear dates given for plan issue and implementation completion. Finally, there should be a post-implementation assurance review of a form specified by the customer, compatible with the security management approach used.

Ongoing security management

48. Performance of security against requirements should form a key part of the service level agreements which are monitored and linked to contractual bonuses or performance penalties.

49. Processes should be put in place contractually for ongoing management of the security relationship with the supplier, covering:

- Changes in the risk (including business processes, business impact, threat and vulnerability)
- Changes in regulatory or compliance aspects
- Changes in security requirements, including control specifications
- Commissioning of, results of, and corrective actions from security performance and assurance reporting
- Material scope changes relating to security

50. A procedure should be contractually agreed between the customer and the supplier to use the agreed approach for any new systems or changes to systems which have a material effect on security.

51. Procedures should be put in place to clarify how day-to-day security requirements of the customer (such as additions and changes to user rights) are authorised and processed by the supplier.

Force majeure

52. Force majeure clauses ordinarily seek to limit the liability of the supplier in certain circumstances which are reasonably beyond their control. However, sometimes suppliers seek to limit their liability for eventualities which are reasonably their responsibility and under their control.

53. When managing security in outsourcing, by definition certain eventualities which might otherwise be considered 'force majeure' should in fact be considered the supplier's responsibility. These eventualities include:

- The consequences of any action taken by a source of security threat which has been identified in a contractually-agreed risk assessment, where a control requirement was specified to address the threat, and where the control failed to prevent the incident owing to ineffective implementation or operation of the control by the supplier or their sub-contractors.
- The consequences of any action taken directly or indirectly by a source of security threat which has been identified in a contractually-agreed risk assessment which exploited a vulnerability, when a control requirement was specified contractually to eliminate vulnerabilities in customer-specified equipment installed, configured and operated by the supplier or their sub-contractors.
- The consequences of any action taken directly or indirectly by a source of security threat which has been identified in a contractually-agreed risk assessment which exploited a vulnerability in supplier-specified equipment, software or service.
- The consequences of any act of war, natural disaster, or terrorism in any place (other than the country of jurisdiction of the contract) where the decision to operate services from that place was taken solely by the supplier or their sub-contractors or sub-sub-contractors without the express written consent of the customer.
- The consequences of any action, including strikes or other industrial action, taken by any employee, sub-contractor or sub-sub-contractor in connection with the services of the supplier to the customer which causes harm to the customer.

54. The term sub-contractor should be defined to include any other supplier contracted directly or indirectly by the supplier, including:

- Manufacturers of hardware and software
- Service and maintenance suppliers
- Telecommunications service providers
- Energy, fuel, water or utility service providers
- Transport providers

55. 'Source of security threat' should be defined in the contract such that it specifically does not exclude the actions of any government, organisation or person.

Assurance and conformance

56. A key part of managing security in outsourcing is gaining assurance that risks have been managed, are being managed and will continue to be managed.

57. Outsourced systems often involve such significant corporate risk that customers cannot wait for an incident to happen and then seek to claim damages.

Assurance can be gained using a variety of methods, detailed below. Some assurance methods, for example SAS70 audit or ISO27001, are associated with particular approaches to outsourcing; but there is no restriction on the use of these methods with any of the approaches in this document. Organisations in the public sector may well wish to examine the OGC Successful Delivery Toolkit which supports service management and delivery. Also, ISACA's COBIT² provides a framework within which overall IT governance maturity can be assessed³.

58. The customer should contractually agree with the supplier the nature, scope, content, format, specification and frequency of the assurance reports (or reviews) required, and the degree to which additional reviews are in-scope.

Method	Approach
Regular security management scorecards	Report in a summary way the security status (and any near-misses or incidents) of each set of outsourced systems as part of overall service reporting.
Supplier-commissioned security reviews	Supplier commissions regular independent reviews or tests of the security of the systems being operated, and reports to the customer the results of the reviews, the corrective actions identified, and the progress of work to address the corrective actions.

²<http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>

³ The relationship between COBIT, ITIL and ISO27001 is usefully described in "Aligning COBIT, ITIL and ISO 17799 for Business Benefit" at <http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490>

Customer-commissioned security reviews	<p>Using a contractual right-of-audit and right-of-access, customer commissions own (or independent) auditors to review or test the security of supplier-operated systems, with access to people, systems, information and records necessary for the review.</p> <p>The customer may make it a requirement that certain key systems are subject to a formalised accreditation process; these processes should be agreed as part of the security requirements for those systems.</p>
SAS70 review	<p>Customer contractually requires supplier to commission a SAS70 review by an independent regulated auditor to confirm that:</p> <ul style="list-style-type: none"> • the design of controls is sufficient to meet the control objectives; and • the controls in operation have been tested such that they operate in accordance with their design and the control objective. <p>SAS70 reviews can be used to satisfy regulatory or compliance assurance requirements in specific industry sectors.</p>
Letters (or affidavit) of assurance	<p>Formal report from a company officer of the supplier to the customer that security has been operated and has been verified to be operating in accordance with the security requirements, compliance requirements and assessment of risk, and that there have been no known security incidents, suspected incidents or near misses other than those already reported in writing.</p> <p>Customer could opt to contract with supplier for a regulated auditor to counter-sign the letter of assurance.</p>
ISO27001 certification	<p>Supplier commissions independent accredited certification firm to review the ISMS against ISO27001 and issue a certificate.</p>

Security in the contract lifecycle

59. The overall approach to defining security in the contract lifecycle is shown in Figure 3 and detailed in the table which follows.

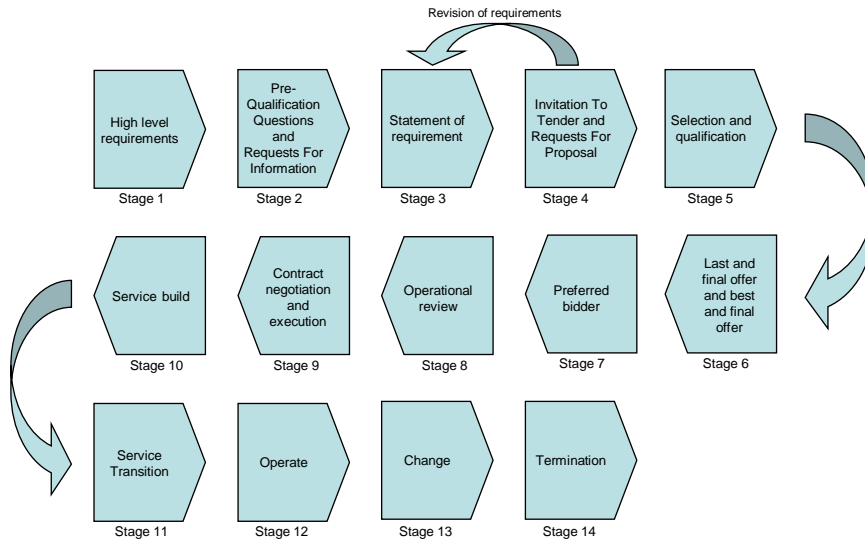


Figure 3: Security in the Contract Lifecycle

Stage	Procurement activities	Security specific activities
1 High level requirements	Customer defines the high level requirements for the services to be provided under the outsourcing contract.	<p>The customer’s outsourcing team engages involvement of qualified, experienced security professionals.</p> <p>Customer carries out the initial risk assessment and compliance requirement to articulate:</p> <ul style="list-style-type: none"> • the assessment of risks to be managed; and • the statement of applicable compliance, regulatory, architectural and policy requirements.

<p>2. Pre-qualification questions and Request for Information</p>	<p>Customer provides high level requirements to suppliers and issues a set of pre-qualification questions to suppliers and invites responses.</p> <p>Suppliers respond.</p>	<p>Customer issues assessment of risks and compliance requirements to suppliers, and invites responses as to their suggested methods of managing security, as well as seeking evidence of security management capabilities.</p> <p>Customer binds suppliers with a confidentiality agreement to protect customer-issues information and information derived from it.</p>
<p>3. Statement of Requirement</p>	<p>Customer develops more detailed statement of requirement</p>	<p>Customer selects preferred methods of managing security and develops and issues high-level control objectives relating to the systems within the statement of requirement.</p> <p>Customer validates security approach with those responsible for assurance within own organisation.</p>

<p>4. Invitation to Tender and Requests for Proposals</p>	<p>Customer issues detailed statement of requirement and draft Terms and Conditions to suppliers and invites tenders.</p> <p>Customer Invitation To Tender (ITT) draws attention to the materiality of security, and refers to the security risk assessment, compliance requirement, controls specification, security management approach and assurance approach.</p>	<p>Customer issues security aspects statement - risk assessment, statement of compliance requirements (including copies of all referenced documents) and high level control objectives to suppliers.</p> <p>Customer also specifies the security management and assurance approach to be used (together with the draft detailed control specifications if appropriate to that approach).</p> <p>Customer transforms security aspects into contractual specifications or contractual terms and conditions.</p>
<p>5. Selection and Qualification</p>	<p>Customer forms bid evaluation team and identifies selection criteria and scoring method for evaluating responses from suppliers.</p> <p>Priority of security areas should be linked to the level of security risk from the risk assessment.</p>	<p>Customer identifies selection criteria relating to security.</p> <p>Customer's qualified and experienced security professional evaluates security responses from suppliers as part of the bid evaluation team.</p>
<p>6. Last and Final Offer and Best and Final Offer</p>	<p>Customer elicits final offers from bidders, and seeks firm, scoped prices.</p>	<p>Customer's qualified and experienced security professional verifies that final offer bids properly address security aspects.</p>

<p>7. Preferred Bidder</p>	<p>Customer bid evaluation team identifies preferred bidder.</p> <p>Customer commissions due diligence review to verify supplier capability.</p>	<p>Customer's qualified and experienced security professional verifies that preferred bidder has the required security capability and that the material security aspects are within the bid price.</p> <p>Customer's qualified and experienced security professional commissions due diligence review to verify supplier security capability.</p>
<p>8. Operational review</p>	<p>Supplier's operational review team performs operational review of the scope of services to be outsourced, to verify conformance with the scope in the ITT and facilitate contract final price.</p>	<p>Supplier's qualified and experienced security professional performs operational review of security aspects of the scope of services to be outsourced, to verify conformance with the scope in the ITT and facilitate determination of the contract final price.</p>
<p>9. Contract negotiation and execution</p>	<p>Customer and supplier commercial, technical and procurement professionals negotiate and finalise the contract.</p> <p>Contract change and scope change processes agreed and incorporated into the contract.</p>	<p>Customer's and Supplier's qualified and experienced security professionals finalise contract security aspects with procurement and commercial professionals to ensure it contains all necessary elements of the risk assessment, statement of compliance requirements, agreed security management approach, controls specifications, and assurance approach.</p> <p>Security-related contract change and scope change processes are agreed and incorporated into the contract.</p>

<p>10. Service build</p>	<p>Supplier teams construct the necessary systems and infrastructure necessary to allow services to transition to the outsourcing provider</p>	<p>Supplier security professionals manage security in accordance with the agreed contract to ensure requirements are met for all operational services.</p> <p>Supplier provides assurance to the customer as agreed in the contract.</p>
<p>11. Service transition</p>	<p>Supplier teams transition operational service from existing onto new technology, facilities, processes and people.</p>	<p>Supplier security professionals manage security in accordance with the agreed contract to ensure requirements are met for all operational services before, during and after transition.</p> <p>Supplier and customer security professionals jointly plan and execute transition security activities.</p> <p>Supplier provides assurance to customer as agreed in the contract.</p> <p>Customer and supplier cooperate on agreed formal security accreditation reviews.</p>
<p>12. Operate</p>	<p>Supplier operates systems in accordance with contract and SLAs, and monitors performance.</p>	<p>Supplier operates security in accordance with contract and security aspects.</p> <p>Supplier provides assurance to customer as agreed in the contract.</p>

<p>13. Change</p>	<p>Supplier manages change in accordance with agreed change management approach</p>	<p>Supplier manages security-related change (either caused by service or security factors) in accordance with contractually agreed security change responsibilities and the service change management approach.</p>
<p>14. Termination</p>	<p>Supplier works with new supplier to transition systems in accordance with agreed service termination processes</p>	<p>Supplier transitions the ISMS to the new supplier in accordance with a contractually agreed ISMS termination plan.</p>

Change management

60. Most large contracts need to change over their course. Such changes may relate to security, either because the scope, functionality or performance of systems after the change has a bearing on security, or because the security requirement itself has changed.

61. Contractual change management boards should have representation by qualified and experienced security professionals from both customer and supplier.

62. As changes often cost more, the contract should clearly address, for security-related changes, which changes should be paid for by the customer as a 'scope change', and which changes should be absorbed by the outsourcing supplier.

63. The table below indicates where each change responsibility might ordinarily lie, though this may be varied in the contract between the customer and supplier depending on the nature of the risk-reward strategies and commercial frameworks.

Type of change	Normal responsibility for initiation and additional cost
<ul style="list-style-type: none"> • Variations in contract scope. • Variations in service level. • Variations in system or process functionality. • Variation in system or process performance. • Customer-defined variation in service location(s). • Increased need for vulnerability management in customer-specified technologies. • Change in customer-issued policies or standards. • Customer-caused variations in the security business impact or threat. • Customer-caused security incident investigation. 	Customer
<ul style="list-style-type: none"> • Supplier-initiated changes to service provision technologies, location(s), and people. • Increased need for vulnerability management in supplier-specified technologies. • Supplier-caused variations in the security business impact or threat. • Security incidents in supplier or 3rd party organisations which impinge upon the Customer or their systems. 	Supplier
<ul style="list-style-type: none"> • Changes in the assessed level of threat • Legislative or regulatory change • Externally caused security incident and its investigation 	For negotiation

Incident management

64. The customer should contractually oblige the supplier to report to a nominated customer contact on an agreed timely basis and format all security related:

- Incidents
- Suspected incidents
- Near-misses
- Suspected near-misses;
- Anomalies
- Contact by law enforcement, regulatory or security authorities
- Civil injunctions or search orders.

65. For the UK government and the wider public sector, the CESA Information Security Memorandum No 37 “Intrusion Detection on Managed IT Systems” (especially Chapter VI thereof) provides a guide to the environment for managing outsourced intrusion technologies that will assist in detecting information security incidents.⁴

66. It may be appropriate to require in contract that a trusted third party organisation investigates information security incidents. This may be a managed security services provider or it may be a public body. Information Security Memorandum No 37 calls this third-party organisation an Authorised External Security Support Organisation (AESSO). For the UK government, the recommended AESSO is NISCC.

67. The customer should agree with the supplier in the contract how security incidents should be investigated and corrective actions taken in an emergency. The customer may appoint a third party organisation to act as its AESSO (see paragraph 66 above). Should this occur, at the customer’s request the supplier shall supply promptly to the AESSO all records, logs and other data and material relating to a specified security related incident. The supplier shall permit the customer and/or its AESSO at all reasonable times to inspect its systems, networks, software, records, logs and other data and material at the supplier’s premises as the customer/AESSO may reasonably require in order to investigate such a security related incident, and the supplier shall fully cooperate with such an investigation. In the event that the results of such an investigation identify a failure in the contractual security service levels, then remedial sections in the contract may be invoked.

68. The customer should contractually oblige the supplier to seek their express consent before any information relating to the customer’s business, information or systems is provided to any third party, including law enforcement, regulatory or security authorities and civil actions, unless required by law or requested by a public authority or contractually pre-agreed applicable regulation.

⁴ Note that IM 37 was issued in January 2005. At the time of writing (July 2006) IM 37 was under review to reflect the guidance incorporated in this document.

69. In addition to conventional service contingency planning and disaster recovery, the customer should agree with the supplier the process to be used for managing an incident involving a sustained electronic attack which threatens the ability of the supplier to continue to operate the service in accordance with the security control requirements.

Termination

70. The customer should contractually agree with the supplier how security will be managed on event of termination of the contract. Termination procedures should be contractually agreed which provide for:

- Transition of services from the service provider back to the customer (or another service provider) in a way in which security and compliance risks continue to be managed effectively
- Handing to the customer all documents, files, procedures, configurations, drawings or records relating to the customer's services
- Purging and destroying all copies of documents and records containing customer information, or if retention is agreed by contract, retention and security protection of copies
- Handing to the customer, or purging and destroying all information on storage media (such as disks and tapes)
- Certification by a director of the service provider organisation that this purging and destruction of customer information has taken place
- Continuation in perpetuity any requirements to keep confidential and protect information which the contract permits the supplier to retain on termination

Further advice

71. For further advice on managing security in outsourcing, please contact NISCC.

Appendix A - Illustrative contract clauses

72. The following illustrative clauses may be used as a starting point to guide contracts professionals when addressing security issues in contracts.

Responsibilities, risk, compliance and competence

Objective	Clause
Responsibilities	<p>The Contractor’s senior commercial director responsible for delivery of the Services to the customer shall be responsible and accountable for all aspects of the security of the Services and for compliance with the contractual security requirements as defined in this contract and associated security Schedules.</p> <p>The commercial director shall appoint service managers and transition managers as appropriate; each such manager shall be responsible and accountable at all times for the security of the Services managed by them.</p> <p>The commercial director shall appoint a professionally qualified and experienced Security Manager to advise the Contractor’s management and staff on all aspects of security and take direct responsibility for those activities delegated to them by the Contractor’s senior commercial director and service/transition managers.</p> <p>The Customer shall appoint a professionally qualified and experienced Security Manager who will be authorised by the Customer to instruct and approve actions by the Contractor relating to security. Agreements made by the Customer’s Security Manager shall be binding on the Customer.</p> <p>The Contractor shall be responsible and accountable for all aspects of security within its suppliers, advisers and sub-contractors.</p>
Risk assessment	<p>The Customer and the Contractor shall agree an assessment of security risks (Schedule S1, Security Risks), which shall identify and agree:</p> <ol style="list-style-type: none"> 1. the outsourcing scope, including a list of business processes and functions to be outsourced; 2. the list of specific governance, legal, regulatory and compliance standards, key technical strategies or architectures or other material constraints; (also see Schedule S2 below); 3. a Business Impact Assessment, stating the impact on the Customer of loss of confidentiality, integrity

	<p>and availability for each system or set of systems;</p> <ol style="list-style-type: none"> 4. the assessment of security threats; and 5. the current vulnerabilities and compliance status, and the target vulnerability and compliance status to be achieved for the Services. <p>The contents of the assessment of risk shall be contractually binding on the Customer and the Contractor and shall form part of the Contract.</p> <p>The Contractor acknowledges their understanding of the risks and compliance requirements in Schedules S1 and S2 for which they are accountable for managing and accepts responsibility for doing so, notwithstanding the Customer's control specifications in schedule S3.</p> <p>Should either party withhold wilfully knowledge from the other of a known material security risk which becomes manifest, the withholding party shall be liable to the other and indemnify them in respect of all costs and damages. Ensure that legal advice is sought on the appropriate wording for any indemnity provision.</p> <p>Should either party refuse to accept existence of a risk and avoid implementation of necessary protective measures, they shall indemnify the other party in respect of all costs and damages should the risk become manifest.</p>
Compliance requirements	<p>The Customer shall attach as schedule S2 (Compliance Requirements) version-numbered copies of all specific governance, legal, regulatory and compliance standards, key technical strategies or architectures or other material constraints to the Contract.</p> <p>The Customer shall warrant that such documents are consistent with each other and further security requirements communicated to the Contractor unless discrepancies are documented and passed to the Contractor.</p>
Competence to manage security	<p>The Contractor warrants that they have the necessary expertise, resource and skills to manage security as required by the Contract. The Contractor shall ensure that staff with security responsibilities are properly qualified, skilled, trained and experienced for their responsibilities for the duration of the Contract.</p>
Transitioning	<p>The Contractor and the Customer shall jointly develop a Security Management Transition Plan, the first part of which shall be a joint responsibility, covering transitioning of Services from the Customer to the Contractor. The Second part shall be the Contractor's responsibility, to transition security to the ISMS and assurance approach</p>

	<p>determined by the Customer.</p> <p>The Customer and the Contractor shall agree dates for the plan issue (which shall be no later than 1 month after Contract Agreement) and Transition Completion (which shall be no later than 6 months after Contract Agreement)</p>
Ongoing security management	<p>Procedures shall be agreed between the Customer and the Contractor within the first month of the Contract covering:</p> <ul style="list-style-type: none"> • agreement of changes to the risk to be managed; • agreement of changes in regulatory or compliance aspects; • changes in security requirements, including control specifications; • commissioning of, results of and corrective actions from security performance and assurance reporting; and • material scope changes relating to security. <p>These Procedures shall be used for material changes to the Services or for any change with material effect on security.</p> <p>Procedures shall also be agreed between the Customer and the Contractor within the first month of the Contract to define day-to-day security management processes (including but not limited to user registration processes) which involve interaction between the Customer and the Contractor.</p>
Force majeure	<p><i>Add to existing contract force majeure provisions:</i></p> <p>The Contractor shall be responsible and liable for the consequences of:</p> <ul style="list-style-type: none"> • any action taken by a source of security threat which has been identified in Schedule S1, where a control requirement was identified in Schedule S3, and where the control failed to prevent the incident owing to negligence or ineffective implementation or operation of the control by the Contractor or their sub-contractors; • any action taken directly or indirectly by a source of security threat which has been identified in Schedule S1 which exploited a vulnerability, when a control requirement was specified to eliminate vulnerabilities in customer-specified equipment installed, configured or operated by the Contractor or their sub-contractors and the Contractor failed to implement and operate

	<p>vulnerability elimination controls effectively as specified by the Customer;</p> <ul style="list-style-type: none"> • any action taken directly or indirectly by a source of threat which has been identified in Schedule S1, which exploited a vulnerability in Contractor-specified equipment, software or services; • the consequences of any act of war, natural disaster or terrorism in any place other than the country of jurisdiction of the contract where the decision to operate services from that place was taken solely by the Contractor or their sub-contractors without the express written consent of the Customer; and • the consequences of any action, including strikes or other industrial action, taken by any employee or sub-contractor in connection with the Services which causes harm to the Customer.
Change management	Responsibility for changes and costs of changes relating to security of the Services shall be determined as agreed in Schedule S5.
Incident management	<p>The Contractor shall report to the Customer Security Manager in the format agreed in Schedule S4 all Service security related:</p> <ul style="list-style-type: none"> • incidents; • suspected incidents; • near-misses; • suspected near-misses; • anomalies; • contact by law enforcement, regulatory or security authorities; and • civil injunctions or search orders. <p>The Contractor shall agree with the Customer within 1 month of the commencement of the contract the approach to be used for investigation and management of incidents.</p>
Disclosure of information	<p>The Contractor shall not divulge (or permit to be divulged) any information relating to the Customer or the Services, or the Customer's information to anyone without the express consent of the Customer, unless required by law or pre-agreed applicable regulation.</p> <p>Information relating to the Customer's contract and the Customer's information shall be disclosed to employees of the Contractor and any Sub-contractors on a strict need-</p>

	to-know basis.
Termination	<p>The Contractor shall agree with the Customer how security will be managed on event of termination.</p> <p>Procedures shall be agreed to provide for:</p> <ul style="list-style-type: none"> • transition of services back to the customer (or other service provider); • return of all documents, files, data, procedures, configurations, drawings or records relating to the Services; • purging and destroying all copies of documents and records containing customer information, or retention and security protection of copies if agreed by contract; • returning or purging and destroying all information on storage media; and • keeping confidential and protecting information which the contract permits the Contractor to retain on termination of the contract.
Key Definitions	<p>‘Subcontractor’ shall mean any other supplier contracted directly or indirectly by the Contractor, including but not limited to manufacturers of equipment, software suppliers, telecommunications providers, energy, fuel, water or other utility suppliers and transportation providers.</p> <p>‘Contractor’ – <i>to be defined in each specific case</i></p> <p>‘Customer’ – <i>to be defined in each specific case</i></p> <p>‘Services’ – <i>to be defined in each specific case</i></p>
Key schedules	<p>S1 – Assessment of Risks</p> <p>S2 – Compliance requirements</p> <p>S3 – Controls specification (including the system security policies of specific systems)</p> <p>S4 – Incident management</p> <p>S5 – Change management</p>

Communication of security requirements option 1 – detailed controls specification

Control specification and assurance extent	The Contractor shall operate technical, physical, procedural and personnel security measures throughout the life of the Contract in the form of an Information Security Management System in accordance with ISO 17799 which shall conform with the Assessment of Risks
--	---

	<p>(Schedule S1), the Compliance Requirements (Schedule S2), and the requirements of the Security Controls Specification (Schedule S3).</p> <p>The Contractor shall document and maintain records for those controls identified in the Security Controls Specification as requiring documentation and records.</p> <p>The Contractor shall specify relevant controls specifications to its sub-contractors.</p> <p>Agreed performance management and assurance processes shall cover the entire scope of the Services, including any aspects of the Services which the Contractor has sub-contracted.</p> <p>There shall be a post-transition security review, of a form to be agreed between the Customer and the Contractor.</p>
--	--

Communication of security requirements option 2 – control objective based specification/assurance

<p>Control Objectives and integrated assurance using the example of a SAS70 audit</p>	<p>The Contractor shall implement controls with necessary documentation and records to satisfy the requirements of the Control Objectives, schedule S3.</p> <p>The Contractor shall commission, at Contractor's cost, an initial Service Auditor's review upon completion of Transitioning, and subsequent annual reviews throughout the life of the Contract by a competent, professional regulated Auditor, in conformance with AICPA SAS70 requirements. The selection of the Auditor shall be approved by the Customer.</p> <p>The Contractor shall commission the Auditors to perform SAS70 Type 2 reviews, reporting on:</p> <ul style="list-style-type: none"> • the Auditors opinion; • the Contractor's description of the controls in place to meet the control objectives; and • the description and results of the Auditor's tests of the controls. <p>Furthermore, the Contractor shall commission the Auditor to consider and report on:</p> <ul style="list-style-type: none"> • The suitability of the controls in place for the contractually-agreed Assessment of Risk schedule (S1); and • The suitability of the controls in place to meet the Compliance Requirements (S2). <p>The Contractor shall provide the whole Auditor's report to</p>
---	---

	<p>the Customer, and the Contractor shall require the Auditor to accept liability to the Customer in respect of their opinion and report.</p> <p>The scope of the Auditor's report shall include all aspects of the Services, including any aspects of the Services which the Contractor has sub-contracted.</p>
--	--

Communication of security requirements option 3 – ISO27001 ISMS

Control specification and certification	<p>The Contractor shall operate technical, physical, procedural and personnel security measures in an ISMS compliant with ISO27001 which shall conform with the Assessment of Risks (Schedule S1), the Compliance Requirements (Schedule S2), and the requirements of the Security Controls Specification (Schedule S3).</p> <p>The ISMS shall cover the entire scope of the Services provided to the Customer, and shall include aspects of the Services which are sub-contracted. The ISMS shall operate throughout the life of the Contract.</p> <p>The ISMS shall be certified upon completion of Transitioning and maintained throughout the life of the Contract by an accredited certification organisation, and the certification shall cover the entire scope of the Services provided to the Customer, including aspects of the Services which are sub-contracted.</p> <p>Agreed assurance processes shall additionally cover the entire scope of the Services, including any aspects of the Services which the Contractor has sub-contracted.</p>
---	--

Assurance and conformance

73. Depending on requirements and the option chosen for managing security, one or more of the following security assurance methods should be used.

Security performance scorecards	<p>The Customer and the Contractor shall agree within the first month of the Contract the format and schedule of scorecards for security which the Contractor shall use to report the performance of security to the Customer, as part of Service performance reporting.</p> <p>The Contractor shall report the performance of security to the Customer using the agreed scorecards, according to the agreed schedule.</p>
Contractor-commissioned security reviews	<p>The Contractor shall commission a programme of independent security reviews of the systems forming the Services, and shall report to the Customer the reports and</p>

	<p>results from such reviews, the corrective actions identified, and the progress of work to complete the corrective actions.</p> <p>The Customer and the Contractor shall agree the programme for the reviews and the scope and coverage of each review.</p>
Customer-commissioned reviews	<p>The Customer shall have a right of audit at any time to review, inspect, test, verify, measure or interview any equipment, software, information, record, data or person relating to the provision of security of the Services.</p> <p>Such reviews shall include formal accreditation of systems when stated as a requirement in the control specifications for the systems concerned.</p>
SAS70 review	<p>The Contractor shall commission, at Contractor's cost, an initial Service Auditor's review upon completion of Transitioning, and subsequent annual reviews throughout the life of the Contract by a competent, professional regulated Auditor, in conformance with AICPA SAS70 requirements. The selection of the Auditor shall be approved by the Customer.</p> <p>The Contractor shall commission the Auditors to perform SAS70 Type 2 reviews, reporting on:</p> <ul style="list-style-type: none"> • the Auditors opinion; • the Contractor's description of the controls in place to meet the control objectives; and • the description and results of the Auditor's tests of the controls. <p>Furthermore, the Contractor shall commission the Auditor to consider and report on:</p> <ul style="list-style-type: none"> • the suitability of the controls in place for the contractually-agreed Assessment of Risk schedule (S1); and • the suitability of the controls in place to meet the Compliance Requirements (S2). <p>The Contractor shall provide the whole Auditor's report to the Customer, and the Contractor shall require the Auditor to accept liability to the Customer in respect of their opinion and report.</p> <p>The scope of the Auditor's report shall include all aspects of the Services, including any aspects of the Services which the Contractor has sub-contracted.</p>

<p>Letter of assurance</p>	<p>The Contractor shall supply the Customer with a letter of attestation from an Officer of the Contractor's company, that:</p> <ul style="list-style-type: none"> • security has been operated in accordance with the security requirements communicated in Schedules S1, S2 and S3; • performance reports of security have been true and fair without material mis-statement; and • there have been no known or suspected security incidents or near-misses affecting the Services in any way other than those reported to the Customer in writing. <p>The Contractor shall procure the counter-signature of a regulated Auditor of the letter of assurance.</p>
<p>ISO27001 certification</p>	<p>The ISMS shall be certified to ISO27001 upon completion of Transitioning and maintained throughout the life of the Contract by an accredited certification organisation, and the certification shall cover the entire scope of the Services provided to the Customer, including aspects of the Services which are sub-contracted.</p>

Appendix B – Glossary of key terms

Accountable	The individual is liable to being called to account for their actions and decisions, including all actions and decisions for which they have further delegated responsibility. Even though responsibility can be delegated, accountability in itself cannot be delegated or assigned elsewhere.
Responsible	The individual or individuals have been given specific responsibility for carrying out particular actions or decisions.
Ensuring	<p>The individual or individuals ensuring that particular actions do occur must either carry out the actions themselves, delegate the activity to carry out the actions, define policy requiring the actions to be carried out or directly manage the actions.</p> <p>In any event, the individual or individuals must make certain that the actions have been carried out correctly.</p>
Managing	The individual takes charge of, administers and regulates the carrying out of specific actions
Letter of representation	A formal letter in which management formally assert a statement of facts and assert that those facts are true.
SAS 70	<p>Statement on Auditing Standards (SAS) No. 70, <i>Service Organizations</i>, is an internationally recognised auditing standard developed by the American Institute of Certified Public Accountants (AICPA). There is no direct equivalent in the UK. A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.</p> <p>One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.</p> <p>In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.</p> <p>In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3)</p>

whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

(For more information see the <http://www.sas70.com> website from which this abridged definition was taken)

ISO27001
certification

Accredited Certification by an UK Accreditation Service accredited auditor that an Information Security Management System conforms with ISO27001, "Information Technology – Security Techniques – Information Security Management Systems – Requirements"