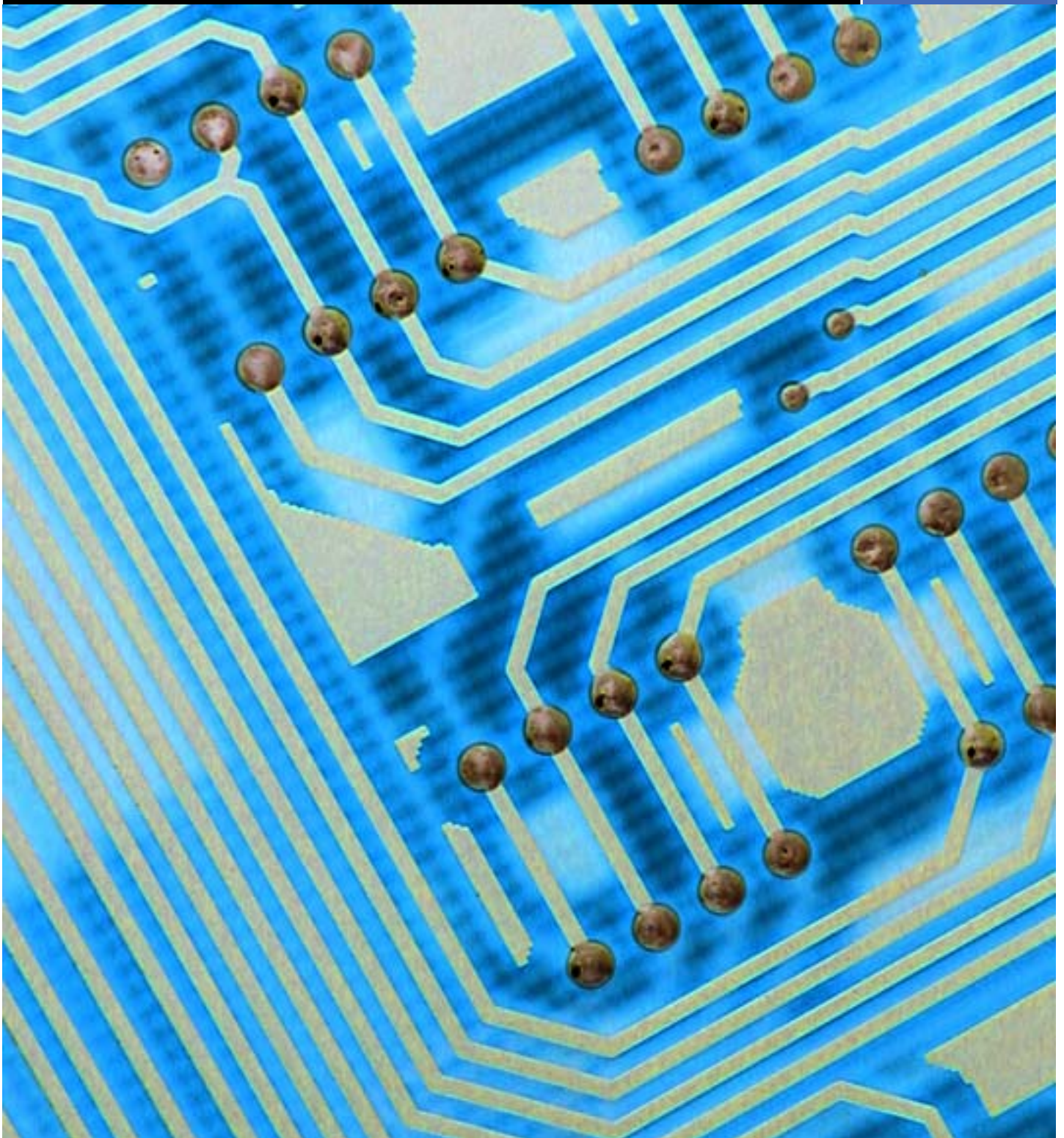


Next Generation Networks

Procurement Standards, Guidance and Model Clauses



Contents

2

	Page
Definitions and Acronyms	3
1 Introduction and Purpose	5
- (1a) Background and Purpose	5
- (1b) Structure and Use of the Guidance	6
2 Procurement Strategy and Process Considerations	8
3 Prior Indicative Notice and <i>OJEU</i> Notice	9
4 PQQ Questions and Wording	11
5 Tender Questions (ITT/ITPD/ITN)	16
- (5a) Service Provision Overview	17
- (5b) Supply Chain	18
- (5c) Risk Mitigation	20
- (5d) Security	22
- (5e) Network Design and Architecture	27
- (5f) Network Deployment, Performance and Monitoring	30
- (5g) Ongoing Network Development, Testing and Change Control	32
- (5h) Business Continuity Planning	33
- (5i) Audit and Additional Information	35
6 Additional Terms and Conditions	37
- (6a) Next Generation Networks - Special Conditions	37
- (6b) Conditions for Existing Telecommunication Contracts	48
7 Contract and Supplier Management	49

Definitions and Acronyms

Authority	The public sector organisation competing the requirement.
Blackhole routing capability	The capability to route traffic to a null IP address.
Business critical/tier one supplier	Any supplier to the service provider (involved in the manufacture or supply of goods or services used in order to provide the services) that is business critical in respect of the provision of the services.
Carrier class	High-speed and highly reliable hardware, firmware and software.
Checksum functionality	A measure used for protecting the integrity of software or data by detecting changes in its composition.
Components	Any apparatus (including any software) used in a telecommunication system which is part of a Next Generation Network.
Comprehensive failure mode and criticality analysis	A detailed analysis of possible risks, their probability and associated impact.
CPB	Central Purchasing Body.
CPNI	Centre for the Protection of National Infrastructure.
DoS	Denial of Service.
EU	European Union.
Impact levels	A measure of risk based on the impact of the risk occurring and measured using a scale of 0-6, with 6 being the highest.
Intelligence core	System architecture, applications and configuration essential for the solution to operate effectively.
IP	Internet Protocol.
IPR	Intellectual Property Rights.
ITIL	Information Technology Infrastructure Library.
ITN	Invitation to Negotiate.
ITPD	Invitation to Participate in a Competitive Dialogue.
ITT	Invitation to Tender.
Next Generation Network (NGN)	<i>'A Next Generation Network (NGN) is a packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, QoS-</i>

enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.' – International Telecommunication Union.

NICC	Network Interoperability Consultative Committee.
OECD	Organisation for Economic Co-operation and Development.
<i>OJEU</i>	<i>Official Journal of the European Union.</i>
Personnel	Employees, contractors, consultants, associates and similar.
QoS	Quality of Service.
R&D	Research and Development.
Risk mitigation plan	The counter-measures applied, or to be applied, to reduce identified risks to an acceptable level.
Service provider	The telecommunications company (or consortium) that would be providing the services required.
Sinkhole routing capability	The capability to route traffic to a designated IP address for subsequent analysis.
SPOFs	Single Points of Failure.
Supplier	The service provider's business critical/tier one suppliers.
Traffic	Voice and/or data packets being transmitted over the network.
VPNS	Virtual Private Network Services.

(1a) Background and Purpose

The Next Generation Networks (NGN) Procurement Standards Project was initiated as part of the Cabinet Office's NGN Risk Mitigation Programme. The objective of the Project was to produce 'best practice' procurement standards and guidance that will assist buyers of NGN-based telecommunication services and set standards that service providers will need to meet in order to supply to government. This document forms the core output of the Project.

Historically, UK telecommunication networks have been regarded as trusted, reliable and resilient. However, the global telecommunications industry is migrating from stand-alone, bespoke technology, to networks (NGNs) that consolidate services on to a suite of platforms based on frame-based technology, e.g. IP (Internet Protocol) software and hardware. These changes will bring significant benefits to organisations, businesses and consumers; not least by creating greater functionality and flexibility whilst also reducing costs. Indeed, government is eager to embrace NGNs and realise the associated benefits. It also recognises, however, that NGNs bring with them challenges and risks which need to be appropriately addressed in order for the UK to continue to benefit from a reliable communications infrastructure.

To operate efficiently and effectively, NGNs interconnect to form a 'virtual network'. It is within this virtual network that vulnerabilities in one network could potentially impact on other networks. This makes it fundamentally important that **all public sector buyers** of NGN-based telecommunication services apply the standards and guidance described here. Moreover, as NGNs are already being implemented and will almost certainly become the de facto technology, **the standards and guidance described here should be applied with immediate effect.**

In summary, this guidance helps to ensure that the public sector **only** contracts with service providers who invest in robust security and risk-mitigation measures. The guidance and standards outlined are aimed at experienced procurement and technology professionals with a good knowledge of telecommunications issues. **This is NOT a comprehensive guide to buying telecommunications.** Rather, it should be used to support and supplement, where appropriate, organisations' internal strategies, processes and standards. Expert technical, procurement and legal input should be applied locally when competing a requirement. You should also ensure that the specification fully meets your needs – for example, in terms of coverage, confidentiality, integrity and availability. Equally, Service Level Agreements (SLAs) and indemnities remain paramount, e.g. fault clearance time, maximum down-time in a given period, down-time measurements, attributable service credits etc.

(1b) Structure and Use of the Guidance

The structure of this guidance broadly follows that of the procurement process, i.e. commencing with the procurement strategy, progressing through the competition process in accordance with the EU procurement regime and culminating in contract and supplier management. The guidance is structured as follows:

1. **Procurement Strategy** and process considerations. Some key strategic issues to consider in terms of the procurement of NGN-based telecommunication services are included in this section.
2. **PIN/OJEU Advertisement**. Recommended wording to be included in PIN notices and OJEU advertisements is included here.
3. **The Pre-Qualification Questionnaire (PQQ)** which selects service providers who have the necessary financial standing, capability and capacity to deliver the requirement. It can also be used to rank potential service providers in order to select an appropriate number for the next stage of the competition. Example questions and recommended wording are given here, along with more general guidance on suitable approaches to drafting a PQQ.
4. **Invitation to Tender (ITT), Invitation to Participate in a Competitive Dialogue (ITPD) or Invitation to Negotiate (ITN)** which lead to the contract being awarded to the service provider(s) which submits the best tender to deliver the requirements. The guidance contained here is presented as suggested questions to service providers. For each, the driver for the question and some possible responses are also given.
5. **Terms and Conditions** which govern the resulting contract. This section includes a number of clauses that are either specific to, or highly relevant to, NGN-based telecommunication services contracts. These clauses are not intended to be exhaustive, and are certainly not a complete contract template. Additionally, this section contains a clause for inclusion within most existing telecommunication contracts. The use of these clauses should be as directed by appropriate legal support.
6. **Contract and Supplier Management** guidance. In addition to best practice contract and supplier management principles, the guidance covers some key NGN-specific issues that should be considered during the operational phase of the contract. Again, it is emphasised that this is not intended to be a complete guide to contract and supplier management.

The example questions consist of both good practice ICT procurement questions and questions specifically developed with regard to NGNs. **The NGN-specific questions are shown in blue. Additionally, questions regarded as being more important, and therefore should be allocated higher weightings, are shown in bold (in black or blue).** Standard good practice procurement questions regarding matters such as service providers' financial stability, quality processes etc are not included.

Not all the questions should necessarily be used for every procurement for NGN-based telecommunication services, although most will be relevant for major contracts. But judgement should be exercised in terms of the specific service and contract needs. Moreover, where the Competitive Dialogue procedure is used, consideration should be given as to what stage in the process the questions should be asked.

The sample responses are not intended to be exhaustive or an example of an optimal service provider response – although in some instances examples of best practice are indicated. Where a service provider cites the sample responses, this indicates a good response and should be scored accordingly.

This guidance is not intended to be proscriptive, nor is it intended to create an arbitrary security and risk mitigation ‘pass mark’ for service providers. Rather, it sets out to help ensure individual procurements take full account of service providers’ investment in security and risk mitigation. In all instances, therefore, you should develop your own model answers – using the guidance where appropriate – but based on the needs for each specific contract; and decide on appropriate award criteria and weightings in line with the EU procurement regime.

Further information or guidance on procurement matters is available from the OGC Service Desk on 0845 000 4999. Questions relating to security issues should be addressed in the first instance to the [Central Sponsor for Information Assurance \(CSIA\)](#).

2 Procurement Strategy and Process Considerations

This section contains some key strategic and process issues that should be considered in terms of the procurement of NGN-based telecommunication services.

Prior to commencing any procurement, and especially for telecommunication services that could involve new and significant risks, you should consider your procurement strategy. For instance:

- What level of protection is required? In terms of Impact Levels (as contained in Appendix 3 of [HMG Infosec Standard No. 1](#) and measured on a scale of 0 to 6 – with 6 being the highest) ***it is expected that most NGN-based solutions will meet a 2-2-4 profile. That is to say they will provide assurance to IL2 for risks to confidentiality and integrity and to IL4 for risks to availability, and as such will only be suitable for traffic classified BELOW 'RESTRICTED' unless additional measures are undertaken, e.g. encryption.***
- Where should the risk be best placed? In many instances this will be with the service provider, in which case an output/outcome-based contract may be most appropriate.
- Are there other electronic communication services that should be 'bundled' together, e.g. data, broadband, mobile telephony services?
- Are there opportunities for greater aggregation and leverage with other organisations, for example, by joining up with another authority (or authorities) to procure a 'shared service' or by acting as a Central Purchasing Body under the Public Contracts Regulations 2006?
- Do suitable telecommunication solutions frameworks already exist that could be used, e.g. OGCBuying.solutions' [Managed Telecoms Services](#) or [Telecoms Frameworks](#)?

Additionally, you should consider matters such as whether there is a need to trial a number of shortlisted service providers as part of the evaluation process or whether a 'pilot project' post contract award is required or whether a period of 'parallel running' using existing technology is appropriate. Where applicable, these requirements should be clearly communicated early in the procurement, along with the envisaged payment mechanism.

With regard to the actual procurement process you should consider what the appropriate timescales are for service providers to respond during the different stages. In particular, it may be reasonable to extend somewhat the normal time allowed for ITT/ITPD/ITN responses in the case of a complex service. Decisions on the most appropriate timescales, however, must be consistent with value for money and the EU procurement regime.

3 Prior Indicative Notice and *OJEU* Notice

This section contains recommended wording to be included in Prior Indicative Notices (PIN) and *OJEU* advertisements.

A PIN is published to give advance warning of contracts to be advertised in the *OJEU*. It is not compulsory to publish a PIN but it is good practice to notify the market of future requirements (which can help stimulate competition).

The *OJEU* Notice or advertisement gives formal notification that the procurement is launched and invites potential service providers to express interest in the contract(s). This guidance provides wording to be considered for inclusion in PIN and *OJEU* Notices. It sets the scene for the procurement of NGN-based telecommunication services and advises service providers of key issues that will be addressed throughout the procurement process. It will also help to ensure that unsuitable service providers deselect themselves.

Content	Purpose/Driver
<p>The following wording should be considered for inclusion in all appropriate PIN and <i>OJEU</i> Notices:</p> <p>‘The Authority recognises the benefits associated with Next Generation Networks (NGNs). It is also aware, however, that NGNs can bring various issues and risks that must be appropriately addressed, and therefore fundamental evaluation criteria will include whether robust risk mitigation and security measures are in place. Such measures will be mandatory requirements.</p> <p>Additionally, where service providers intend to migrate to an NGN-based solution over the duration of any resulting contract, the Authority will (in its sole opinion) need to be satisfied that robust risk mitigation and security measures of contractual effect are in place prior to any migration to NGN-based technology, and that such migration will be dealt with under Change Control procedures.’</p>	<p>The use of this wording in all appropriate PIN and <i>OJEU</i> Notices will signal to the market the importance the public sector places on robust risk mitigation and security measures, that you are an informed customer, and that it would not be a good use of a service provider’s time to bid unless robust risk mitigation and security measures are in place/will be applied.</p>

Content	Purpose/Driver
<p>All appropriate PIN and <i>OJEU</i> Notices should specify the Impact Levels of confidentiality, integrity and availability required (e.g. baseline 2-2-4 or higher).</p>	<p>In determining the level of confidentiality, integrity and availability required, you should liaise with your IT Security Officer to ensure compliance with all appropriate Security Electronic Notices, and in particular S(E)N 2006/10. Specifying the level of confidentiality, integrity and availability required in the PIN and <i>OJEU</i> Notices will assist the market to understand better the requirement, and help unsuitable service providers to deselect themselves.</p>

OJEU Notice Only

Content	Purpose/Driver
<p>You should also consider whether other public sector organisations may wish to jointly procure these services or whether the Authority wishes to act as a Central Purchasing Body (CPB) to procure these services on behalf of itself and/or other authorities.</p> <p>Where the Authority wishes to act as a CPB and other such organisations can be identified, they should be cited within the <i>OJEU</i> Notice. For example, 'this contract may also be used by other UK public authorities including the Home Office, the Metropolitan Police and London-region Local Authorities which have a need to purchase telecommunication services'.</p>	<p>The inclusion of this wording will create the provision for such organisations to use the resulting contract(s) where appropriate. Further guidance on CPBs is also available from OGC.</p>

4 PQQ Questions and Wording

Within this section are example PQQ (Pre-Qualification Questionnaire) questions and recommended wording, along with more general guidance on suitable approaches to drafting a PQQ.

The purpose of a PQQ is to select a number of service providers who appear to have the capability and capacity to deliver the requirements outlined in the *OJEU* Notice. Those service providers then go forward to the evaluation stage (ITT or ITN) at which point the final service provider(s) is chosen and the contract(s) awarded.

The PQQ is **not** designed to identify the ‘best’ or winning service provider; its purpose is principally to select those that are suitable. If there are more feasible service providers than required for the evaluation stage, then the PQQ should also provide the means to rank the potential service providers so that the most suitable ones can be taken forward. For a single contract, usually between 3 and 8 service providers should go through to the evaluation stage (a minimum of 5 providers where the restricted procedure is the chosen route). If a framework is being let, then 20 or more may go through depending on the size of the desired final framework list.

Best practice suggests that PQQs should not be overly onerous for service providers or evaluators. A small number of insightful questions are recommended rather than dozens of detailed questions. The questions should be aimed at differentiating between suitable and unsuitable service providers; and ranking the suitable service providers in order to choose the best possible shortlist. Questions in the first category are generally marked on a binary basis; the service provider is either ‘in or out’. For instance, financial questions may lead to the elimination of service providers who cannot meet a minimum standard of financial stability, defined level of asset value or similar.

PQQ questions should focus on:

- financial capacity (e.g. turnover, ability to fund investment)
- business capacity (e.g. production capacity, quantity of skilled staff)
- business capability (e.g. evidence of particular skills, past experience).

Financial capacity should always be explored with all telecommunications service providers, as indeed it should for all but the most nugatory contracts. Considerable guidance is available on this subject, for example OGC’s [Supplier Selection Guidance](#). Business capacity and capability questions should be designed appropriately for each specific procurement. It is important, however, to look for relevant capability without becoming so specific that the only service provider which can progress is one that has done **exactly** the same work for **exactly** the same sort of customer. That situation leads to uncompetitive markets. So a balance should be struck; relevant capability needs to be evidenced but it can be with different customers or in a somewhat different supply area.

Example PQQ questions are provided in the table below. To reiterate, **NGN-specific questions are shown in blue and questions regarded as being more important are shown in bold (in black or blue)**. In applying the NGN-specific PQQ questions, care should be taken to ensure that service providers' scorings are not distorted. Equally, care should be exercised to ensure that service providers are not excluded based on their historical capability and capacity, as opposed to their relevant capability to deliver the requirement – which may not be apparent until the evaluation stage.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>1 Which, if any, NGN-related telecommunication industry bodies is your company (consortium) a member of, and for how long has it been a member?</p>	<p>To establish whether the service provider has been involved in NGN-related telecommunication industry bodies addressing the associated risks and issues, and for how long.</p>	<ul style="list-style-type: none"> ■ A founder member of NGNUK (or equivalent).
<p>2 Outline any specific contributions your company has made in assisting the telecommunications industry address the risks and issues associated with NGNs.</p>	<p>To establish the degree to which the service provider has been involved in assisting the telecommunications industry in addressing the associated risks and issues.</p>	<ul style="list-style-type: none"> ■ Making available R&D results to the industry. ■ Leading various industry body workstreams.
<p>3 Provide details (including the organisation, a brief description of the services involved and dates of contract award) of a maximum of three public sector and three private sector contracts won in the last three years for services similar to those required by the Authority. Where appropriate, include (and highlight) examples of such services being provided using NGNs. Note: The Authority reserves the right to</p>	<p>To establish the service provider's experience of providing services similar to those required by the Authority using NGNs.</p>	<p>As NGNs are, by definition, emerging technology, service providers which are unable to cite examples of where they are already, or will shortly be, providing NGN-based services should NOT be automatically excluded. Careful consideration, however, should be given as to whether the Authority would wish to be their first NGN client.</p>

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>contact the organisations cited for references, and your permission to do so is hereby given.</p>		
<p>4 Outline the high-level security measures your company applies.</p>	<p>To emphasise the importance of security and to establish the high-level security measures applied.</p>	<ul style="list-style-type: none"> ■ Robust physical security measures. ■ Robust technical security measures. ■ Appropriate personnel checks. ■ Appropriate business critical/tier one supplier checks. ■ The application of good practice information security controls such as ITIL, ISO27001 and ITU X1051 (or equivalents). ■ The use of an Information Security Management System (ISMS). ■ Ongoing security reviews being undertaken. <p>Should a service provider not demonstrate robust high-level security measures they should be excluded from further consideration.</p>

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>5 Outline the high-level aspects of your company's risk mitigation plans.</p>	<p>To emphasise the importance of risk mitigation and to establish the high-level risk mitigation measures applied.</p>	<ul style="list-style-type: none"> ■ Consideration of the political stability of areas and the risk of natural disasters. ■ Dual sourcing/multi-country sourcing of business critical components and services. ■ Network rollback policy. ■ Updated and regularly tested contingency plans. ■ A formal Risk Treatment Register (RTR), recording all risks, decisions made and resolutions. ■ Board-level ownership of the contingency plans. <p>Should a service provider not demonstrate robust high-level risk mitigation plans they should be excluded from further consideration.</p>
<p>6 Outline your company's business critical/tier one suppliers and what they provide.</p> <p>We would generally expect service providers to have between 5 and 15 such suppliers.)</p>	<p>To gain an overview of the service provider's business critical/tier one suppliers and to ensure that most are 'recognised' component and service suppliers.</p>	<p>Where a significant number of business critical/tier one suppliers cited are unknown to you or have not been cited by other service providers, further investigation should be undertaken prior to inviting the service provider through to the next stage of the procurement process.</p>

You should also consider including the following standard wording in your PQQ. Again, this will signal to the market the importance of robust security and risk mitigation and provide an indication of the rigour that will be applied as part of the procurement process.

‘Please note that as part of the ITT, ITPD or ITN issued at the next stage of the procurement process, the Authority will require detailed information regarding your service provision; supply chain; risk mitigation; security; network design and architecture; network deployment, performance and monitoring; ongoing network development, testing and change control; business continuity planning; and similar, in terms of how they contribute to your overall solution for this project. Given the risks and issues around NGNs, a high weighting will be placed on your responses to these questions as they illustrate the underlying security and robustness of your solution. Strong responses will increase your probability of winning business; inadequate responses may result in your bid being excluded from further consideration due to non-compliance with the Authority’s mandatory security and risk mitigation requirements.’

5 Tender Questions (ITT, ITPD or ITN)

This section contains good practice tendering guidance and suggested questions to service providers. For each question, the associated driver and some possible responses are also given.

The ITT (or ITPD in the case of the competitive dialogue procedure or ITN in the case of the negotiated procedure) is designed to inform the choice of the 'best' offer for the provision of the goods or services required by the Authority. 'Best' will usually be formally defined as 'most economically advantageous'. In practice, this usually means a combination of whole-life cost (which can include upfront pricing, maintenance, spares cost, support costs, disposal costs etc), along with other factors that relate to overall value, such as the quality of the service.

It is worth noting that, where a selection is being run between service providers already on a framework, the competition can be much more straightforward. The overarching framework agreement should already cover many of the points of interest and will probably have some agreed pricing. It should also have assessed that the service providers can meet the required NGN security and related criteria described here. Questions to the framework service providers can then focus on the specific requirements and how the service provider plans to meet them and on specific pricing, given the defined requirements.

The questions included in this guidance focus primarily on security and risk-mitigation issues. However, good tender documentation should also include questions covering the range of capabilities required for the delivery of the project. While these should be tailored for each specific case, appropriate questions will often fit under headings such as:

- Operational capability
- Customer service
- Risk transfer and management
- Transition planning and management
- Strength of service provider team and service provider 'attitude'
- Innovation and continuous improvement.

The following pages contain example questions and possible responses in respect of NGN-based telecommunication solutions and address aspects such as: service provision; supply chain; risk mitigation; security; network design and architecture; network deployment, performance and monitoring; ongoing network development, testing and change control; business continuity planning; and audit and additional information.

To reiterate, however, not all the questions should necessarily be used for every NGN procurement, although most will be relevant for major contracts. Equally, the responses are only examples and you should develop your own model answers and weightings based on the needs of each specific requirement.

(5a) Service Provision Overview

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>7 From where and how would the performance of the different aspects of the services required be provided, e.g. customer service, network monitoring and management, technical support and billing? In particular, describe how you would ensure all related information-security legalisation, including the Data Protection Act (DPA) 1998, would be fully compiled with.</p>	<p>To establish visibility of where the different aspects of the services required would be provided from, and to ensure that all information-security legalisation, including the DPA 1998, would be fully compiled with.</p>	<ul style="list-style-type: none"> ■ Demonstrable knowledge of the provisions of the DPA 1998. ■ Where applicable, demonstrable knowledge of: where non-EU countries have implemented the DPA 1998 principles in statute; ‘safe harbour’ provisions; and the use of OECD model clauses in relation to DPA principles. <p>Consideration should be given to the political stability of the proposed country(ies)/region(s) and any security issues associated with them.</p>

(5b) Supply Chain

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>8 In providing the services required, who would be your business critical/tier one suppliers and what would they provide? (We would generally expect service providers to have between 5 and 10 such suppliers.)</p>	<p>To gain visibility of the service provider's business critical/tier one suppliers that would be involved in providing the services and to help ensure that the components being used are 'carrier class'.</p>	<p>Where a business critical/tier one supplier cited is unknown to you or has not been cited by other service providers, further investigation should be undertaken prior to contract award.</p>
<p>9 In relation to the services required, to what extent do you have visibility of the supply chain for business critical components and services, e.g. do you have complete visibility from point of origin? Please cite specific examples or provide rationale as to why this visibility does not exist.</p>	<p>To determine the extent to which the service provider has a detailed understanding of the supply chain.</p>	<p>The less evidence of supply chain visibility a service provider is able to provide, the more their response should be marked down, unless compelling mitigation is cited.</p>
<p>10 In acquiring the aforementioned business critical components and services in respect of the services required, what key considerations are taken into account as part of your procurement process and how do you ensure that these considerations are appropriately addressed?</p>	<p>To determine the breadth and depth of rigour applied in the service provider's procurement process.</p>	<ul style="list-style-type: none"> ■ Cost. ■ Reliability of supply. ■ Political stability and security risks associated with the country or region. ■ Supplier's financial stability. ■ Supplier's risk mitigation plans. ■ Supplier's security measures.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
		<ul style="list-style-type: none"> ■ Supplier's personnel security checking procedures. ■ Supplier's quality-assurance processes. ■ Undertaking supplier site inspections.
<p>11 In respect of the services required, outline how you would manage your business critical/tier one supplier relationships.</p>	<p>To ensure that there is the basis for strong relationships with the respective business critical/tier one suppliers and therefore the foundation for good supplier support.</p>	<ul style="list-style-type: none"> ■ Regular review meetings, e.g. at least quarterly. ■ The relationship being 'owned' at board-level, ideally by the Commercial Director. ■ The extent to which information is shared and to which suppliers can influence. ■ The existence of joint R&D, working groups and shared IPR ownership. ■ Service provider personnel located on supplier sites and vice versa.
<p>12 In providing the services required, which, if any, of the aforementioned business critical components and services needed would you single source, i.e. only use one manufacturer's or service provider's components/services (irrespective of the supply route), and how would you mitigate the associated risk?</p>	<p>To identify instances of business critical components and services being single sourced – as this could represent significant risk (i.e. what happens were that supplier to cease trading?). It is also to ensure there would be robust measures in place to mitigate the associated risk.</p>	<ul style="list-style-type: none"> ■ Robust procurement processes and good supplier management. ■ Sourcing via a number of supply routes. ■ Multi-country sourcing. ■ Maintaining an alternative supplier plan. <p>The more a service provider single sources business critical components and services, the more they should be marked down.</p>

(5c) Risk Mitigation

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>13 In respect of the services required, provide an overview of the findings of your comprehensive failure mode and criticality analysis undertaken, including suppliers.</p>	<p>To establish whether a comprehensive failure mode and criticality analysis has been undertaken in respect of the services required, and the risks have been identified and well considered.</p>	<p>The comprehensive failure mode and criticality analysis should address matters such as:</p> <ul style="list-style-type: none"> ■ Quality and availability of business critical components and services. ■ Protecting the 'intelligence core' of the network. ■ Security of the overall network.
<p>14 In respect of the services required, detail your risk mitigation plan.</p>	<p>To ensure that an appropriate risk mitigation plan for the services required is in place.</p>	<ul style="list-style-type: none"> ■ Robust network design (including dual homing/routing). ■ Business contingency exchanges. ■ Business contingency provisions agreed with business critical/tier one suppliers. ■ Specific fallback arrangements in place.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>15How would you ensure that the risk mitigation plan in respect of the services required is robust and kept fully up to date?</p>	<p>To ensure that the risk mitigation plan would be robust and kept fully up to date.</p>	<ul style="list-style-type: none"> ■ Risk assessment undertaken using a recognised process such as the risk assessment section of the related CPNI guidance. ■ Risk mitigation plan externally audited and/or accredited. ■ Ongoing scenario testing and re-evaluation of assumptions. ■ Regular (weekly) operational review of the plan. ■ Senior-level ownership.
<p>16Should security concerns be identified, what procedures would you have for isolating, i.e. stopping purchasing from (and, if necessary, replacing installed components from) suppliers, countries or regions?</p>	<p>To establish whether supplier isolation has been considered and appropriate provisions made.</p>	<ul style="list-style-type: none"> ■ Detailed knowledge of where business critical components and services are produced/provided from. ■ Dual sourcing and/or multi-country sourcing. ■ Contingency plans in place for replacing components (including installed components) and/or services.

(5d) Security

Question	Purpose/Driver	Examples of Positive Responses/Guidance
17 Outline the physical security measures that would be deployed to protect the network, especially the network management centres.	To ensure that robust physical security measures would be deployed to protect the network.	<ul style="list-style-type: none"> ■ Security guards 24/7. ■ Fire control measures. ■ Controlled access. ■ Restricted access areas. ■ Permit-to-work scheme. ■ CCTV monitoring.
18 Outline the technical security measures that would be deployed to protect the network.	To ensure that robust technical security measures would be deployed to protect the network.	<ul style="list-style-type: none"> ■ The application of good practice information security controls such as ITIL, ISO27001 and ITU X1051 (or equivalents). ■ Password only access. ■ Two factor/dual factor access authentication. ■ Personnel gaining only the access needed to perform their role. ■ Use of 'one-time access passes' for supplier personnel.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>19 In respect of the services required, outline the personnel proficiency and security checking processes, procedures and business controls that would be applied.</p>	<p>To ensure that robust personnel proficiency and security checking processes, procedures and business controls would be applied. Note: some companies, e.g. BT and Cable and Wireless - will be able to undertake their own security checks.</p>	<ul style="list-style-type: none"> ■ Some form of identity checks for all personnel, e.g. passport. ■ Nationality and immigration status checks. ■ Copies of key certificates obtained. ■ References taken up. ■ Experience of dealing with the relevant authorities regarding security checks. ■ A database and documented procedures to ensure any time-bound security clearances do not lapse. ■ Processes and procedures appropriately communicated. ■ Regular internal audits. <p>An example of best practice would be compliance with BS 7858 Security Screening (or equivalent).</p>

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>20 In respect of the services required, what level of security checks and any additional measures would you require for your personnel in the following roles:</p> <ul style="list-style-type: none"> ■ Senior designers and technicians with access to the network 'intelligence core'. ■ Network engineers. ■ Support staff. 	<p>To ensure that robust security checks are undertaken for more sensitive roles.</p>	<ul style="list-style-type: none"> ■ Senior designers and technicians having undergone a Management Vetting (MV) check (or equivalent). ■ Network engineers having undergone a BS Basic Standard check, or even an enhanced BS Basic Standard check (or equivalents). ■ Dependent on actual roles, but usually a Criminal Records Check (or equivalent) would be sufficient for support staff. <p>Examples of additional measures would be for all personnel to have to agree a confidentiality undertaking, and the service provider reserving the right to undertake background security checks as part of their contracts of employment/engagement.</p>
<p>21 In respect of the services required, what personnel proficiency and security checks would you require of business critical/tier one suppliers and how would you ensure these checks are carried out?</p>	<p>To ensure that business critical/tier one suppliers also apply robust proficiency and security checks.</p>	<p>Service providers should ensure that their business critical/tier one suppliers apply proficiency and security checks similar to their own. Additionally, service providers should carry out regular supplier checks and audits to ensure that the checks are being applied.</p>

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>22 In respect of the services required, outline the specific checks you would undertake to ensure components would not have undocumented functionality that could be used to disrupt or compromise the security of the network.</p>	<p>To ensure that service providers are aware of and would undertake at least the fundamental checks for undocumented functionality.</p>	<ul style="list-style-type: none"> ■ Robust procurement processes and good supplier management. ■ Design documentation demonstrating the controls in place for the management and testing of all components. ■ Use of checksum functionality to detect unauthorised changes made to software. ■ Completion of code checks and reviews. ■ Completion of penetration tests. ■ Protective monitoring of component performance. ■ Service providers retaining and exercising the right of audit, onsite inspection and security compliance testing in relation to suppliers.
<p>23 Which specific network security measures would you use? In particular, your response should address firewalls, anti-virus, anti-spam and anti-malware measures deployed. It should also include measures used to prevent DoS attacks, and data exfiltration and alteration.</p>	<p>To ensure that the service provider would deploy robust network security protection.</p>	<ul style="list-style-type: none"> ■ The use of established firewall, anti-virus, anti-spam and anti-malware products. ■ Measures to prevent DoS attacks, and data exfiltration and alteration.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
24 How would you ensure that appropriate new security and risk mitigation technologies and techniques would be applied as they become available?	To ensure that service providers are committed to continual improvement.	<ul style="list-style-type: none">■ Being part of NGN-related industry bodies.■ Working with peers.■ Continual improvement should also form part of product development and/or security management processes.■ Regular product development audits and validation of the technology used.

(5e) Network Design and Architecture

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>25 In respect of the services required, provide an overview schematic of your network design and architecture. Where appropriate, the schema should illustrate the security measures applied, network borders, the level of dual homing and dual routing, supplier domain segregation, SPOFs, Internet traffic separation, VPNS separation, customer/sub-customer separation, and blackhole and sinkhole routing capability.</p>	<p>To ensure that the design and architecture of the network is appropriate and robust.</p>	<ul style="list-style-type: none"> ■ Security being integral to the design (rather than an afterthought). ■ Clearly defined and robustly protected network borders. ■ Suppliers separated into domains, based on the business criticality of the components and/or services being provided. ■ The number of SPOFs, where applicable. The fewer SPOFs the better, and best practice is that SPOFs are designed out. ■ Adequate separation from Internet traffic. ■ Adequate separation between services, e.g. separate VPNS. ■ Adequate separation between customers/sub-customers. ■ Appropriate level of dual homing and routing. ■ Appropriate blackhole and sinkhole routing capability.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>26 In respect of the services required, illustrate the proposed routing and describe how you would control the routing so that traffic would not be vulnerable to security or commercial compromise.</p>	<p>To ensure that traffic would not be routed in ways that could give rise to security or commercial compromise.</p>	<p>Routing of traffic needs to be carefully considered. Should an Authority require a 'UK only' network or for the services to be provided from within the UK, legal advice should be sought to ensure there is clear justification in terms of the EU procurement regime.</p> <ul style="list-style-type: none"> ■ A logical and formally defined physical path with boundary protection devices. ■ Logical and formally defined 'overflow' arrangements with boundary protection devices.
<p>27 What development and interoperability standards and protocols have been, or would be, used in developing the network?</p>	<p>To establish the development and interoperability standards.</p>	<ul style="list-style-type: none"> ■ ETSI-TISPAN is the emerging development open standard for fixed networks. ■ 3GPP is the emerging development open standard for mobile networks. ■ SIP-I is the emerging interoperability standard/protocol. <p>An example of best practice would be compliance with the interoperability standards being developed by NGNUK (or equivalent).</p>

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>28 What measures would you use to ensure that the network borders have robust protection?</p>	<p>To ensure that the network borders (a fundamental aspect of the overall security of the network) would be robustly protected.</p>	<ul style="list-style-type: none"> ■ The network boundary being unambiguous and formally documented. ■ Firewalls, session border controls and probing measures. ■ The internal network structure and capability remaining 'hidden' to other networks/service providers. ■ Procedures for ensuring components are correctly configured. ■ Testing is carried out - initially and on an ongoing basis.
<p>29 What testing would you carry out on the network as part of the development process and how would this be undertaken?</p>	<p>To ensure that the system development process includes robust testing at all stages.</p>	<ul style="list-style-type: none"> ■ Testing to verify design – technical and physical. ■ Testing key elements of the system. ■ The use of best practice, automated vulnerability testing tools. <p>An example of best practice would be complete end-to-end configuration testing prior to the network being put into service.</p>
<p>30 What independent testing, assurance and accreditation has been, or would be, carried out on the network?</p>	<p>To establish the testing, assurance and accreditation carried out or planned.</p>	<ul style="list-style-type: none"> ■ The network being assured by CESG/commercial agencies to an appropriate level. ■ ISO 27001 (or equivalent).

(5f) Network Deployment, Performance and Monitoring

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>31 Outline how you would deploy your solution and provide a copy of your proposed implementation project plan.</p>	<p>To ensure that the implementation approach would be appropriate.</p>	<ul style="list-style-type: none"> ■ An implementation project plan that is consistent with other responses and based on realistic timescales. ■ The use of a recognised Project Management discipline (e.g. PRINCE2). ■ The appropriate use of trials, pilot projects and parallel-running using existing technology. ■ Appropriate levels of assurance. ■ Appropriate fallback arrangements.
<p>32 How would you monitor and manage the network, i.e. how many people at what level would be deployed and what processes and technology would be used?</p>	<p>To ensure that adequate resources would be assigned and that there would be appropriate investment in network monitoring equipment.</p>	<ul style="list-style-type: none"> ■ Number and level of personnel engaged. ■ Change control processes used. ■ Policies for patching, testing, releases etc. ■ The use of recognised hardware and software monitoring tools. ■ An accurate circuit records database.
<p>33 How would you ensure that traffic is not exfiltrated or altered by your (or your suppliers') personnel?</p>	<p>To ensure that this risk has been considered and addressed.</p>	<ul style="list-style-type: none"> ■ Network security controls, monitoring, and change controls. ■ Only tools configured not to record or store the content of transmissions can be used on the network.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
34 What proactive testing and maintenance would you carry out on the network?	To ensure that the service provider invests in proactive testing and maintenance.	<ul style="list-style-type: none"> ■ Vulnerability tests. ■ Stress tests (capacity and performance testing under adverse loading conditions).
35 What measures would you apply to detect network attacks and security breaches and to repair the network?	To ensure that the service provider would apply appropriate measures to detect network attacks and security breaches and to repair the network.	<ul style="list-style-type: none"> ■ Intrusion detection. ■ Unusual-event detection and response. ■ DoS detection. ■ Automated 'close down'. ■ Automated 'self heal'.
36 In respect of the services required, describe your incident management, escalation and reporting procedures (including suppliers and customers).	To ensure that the service provider would have appropriate incident management, escalation and reporting procedures which also include suppliers and customers.	<ul style="list-style-type: none"> ■ Use of NICC templates. ■ Use of online solutions. ■ Communication with suppliers. ■ Communication with the Authority and within the specified timeframe.

(5g) Ongoing Network Development, Testing and Change Control

Question	Purpose/Driver	Examples of Positive Responses/Guidance
37 Outline the ongoing network development and testing process that would be applied.	To ensure that development and test environments would be used.	<ul style="list-style-type: none"> ■ A formal change control system, including development and test environments, whereby hardware, firmware and software would be developed and deployed in a controlled manner. ■ 'Witness testing' by suppliers, so that the functionality can be demonstrated.
38 Describe the procedures that would be applied for handling and implementing change requests and the procedures that would be applied to ensure that changes are appropriately implemented.	To ensure that only official change requests would be implemented and that appropriate controls and checks would be applied to the change control process.	<ul style="list-style-type: none"> ■ ISO 9001/27001 and/or ITIL (or equivalents) compliant change control processes. ■ All changes made in writing and approved by two previously agreed authorisers. ■ A change log capturing all changes. ■ Random audits of changes and an audit log. ■ Audits of all supplier changes. ■ Retention of change and audit logs for a period of at least six months.
39 Outline what provisions would be made for network testing by the Authority (or an appropriate third party acting on its behalf)?	To ensure that the provision would exist for the Authority (or an appropriate third party acting on its behalf) to undertake appropriate checks on the network.	<ul style="list-style-type: none"> ■ Access to the network as reasonably requested. ■ Access to an exact replica as reasonably requested.

(5h) Business Continuity Planning

Question	Purpose/Driver	Examples of Positive Responses/Guidance
40 Outline your business continuity plans in respect of the services required and advise whether they have been, or would be, externally validated.	To ensure that the service provider would have appropriate business continuity plans in place.	<ul style="list-style-type: none"> ■ Business continuity provisions in place with all business critical/tier one suppliers. ■ Appropriate multi-sourcing of business critical support. ■ Agreed procedures and timescales for key personnel (including supplier personnel) being available/on site. ■ Appropriate contingency plans for obtaining business critical components. ■ External assurance of business continuity plans.
41 How often would the aforementioned business continuity plan be tested, who would be responsible for it and how would it be updated?	To ensure that the business continuity plan would be actively tested and updated.	<ul style="list-style-type: none"> ■ Regular contact with the Security Service regarding potential threats. ■ Reviewed and updated monthly. ■ Tested at least once every six months. ■ 'Owned' by a board member.
42 For what software would you require your suppliers to deposit and maintain Escrow Agreements with reputable agencies?	To ensure that the service provider has considered the scenario of a supplier ceasing to exist and, in such event, the service provider would have access to the necessary code to maintain the service.	Service providers should ensure that Escrow Agreements exist with reputable agencies for all business critical software, and that such Agreements are appropriately updated.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>43 In respect of the services required, what network rollback arrangements would you have in place?</p>	<p>To ensure that the service provider could rollback the network to a previous robust version.</p>	<p>Service providers should have rollback arrangements for at least the business critical software used on the network.</p> <p>An example of best practice would be the availability of 'validated build' network software, i.e. a fully tested and accredited version of software used on the network.</p>
<p>44 In respect of the services required, what fallback arrangements would you have in place?</p>	<p>To ensure that the service provider would have appropriate fallback arrangements in place.</p>	<ul style="list-style-type: none"> ■ Revert to the current infrastructure. ■ Spare exchanges with the capacity to handle the work of any other exchange. <p>An example of best practice would be mobile exchanges that could be deployed where needed.</p>

(5i) Audit and Additional Information

Question	Purpose/Driver	Examples of Positive Responses/Guidance
45 Confirm that the Authority, or an appropriate third party acting on its behalf, may undertake audits during the procurement process or any resulting contract to verify representations made.	To help ensure that the Authority has the right of audit.	The more exceptions and caveats applied, the more the service provider's response should be marked down.
46 Confirm that, if requested, the Authority will in respect of the services required be provided with copies of the appropriate security and risk mitigation documentation in a timely manner.	To help ensure that the Authority has the right to copies of the relevant security and risk mitigation documentation in a timely manner.	The more exceptions and caveats applied, the more the service provider's response should be marked down.
47 Advise to what extent the Authority, or an appropriate third party acting on its behalf, would have the necessary rights to audit all the software code used in the provision of the service.	To help ensure that the Authority has the right to carry out audits on all, or as much as possible of, the software used in providing the service.	The more exceptions and caveats applied, the more the service provider's response should be marked down.

Question	Purpose/Driver	Examples of Positive Responses/Guidance
<p>48 Advise to what extent you have made the necessary contract provisions to ensure that the Authority, or an appropriate third party acting on its behalf, would be able to carry out full audits and onsite security compliance inspections on any components or service provision at any point in the supply chain.</p>	<p>To help ensure that the necessary contract provisions are made to enable the Authority to carry out such audits and onsite security compliance inspections.</p>	<p>The more exceptions and caveats applied, the more the service provider's response should be marked down.</p>
<p>49 Based on your proposed solution, provide any further information you consider relevant in respect of NGNs.</p>	<p>To ensure that the service provider has the opportunity to fully demonstrate their knowledge and experience of NGNs in respect of the services required.</p>	<p>There is a wide range of possible responses to this question. Each response should be carefully assessed in relation to how such knowledge and experience would contribute to a service provider's ability to deliver the services required.</p>

6 Additional Terms and Conditions

This section includes terms and conditions that are either specific to, or highly relevant to, NGN-based telecommunication services contracts. These clauses are not intended to be exhaustive and are certainly not a complete contract template. Additionally, section 6b contains a suggested clause for inclusion in most existing telecommunication contracts. The use of these clauses should be as directed by appropriate legal support.

(6a) Next Generation Networks - Special Conditions

The following terms and conditions should be incorporated within (1) all new NGN-based contracts and (2) all non-NGN telecommunications contracts where it is planned at contract award to migrate to NGN-based technology during the contract.

In applying such terms and conditions, it is strongly recommended that legal advice is sought, and in particular to ensure that:

- the definition of NGNs is appropriate for the particular technology that would be used to provide the services required. 'NGN' is a relatively generic term
- appropriate Schedules are developed addressing matters such as: routing of services and the locations from which services will be managed; planned transition to NGN-based technology; business critical suppliers; risk mitigation; security; supplier isolation; and business contingency measures.

1. Provision of the Services

- 1.1 It is a condition precedent to this Agreement coming into force that the Impact Level and Protective Marking is specified in the Services Schedule.
- 1.2 The Service Provider undertakes that the Services shall be secure for the type of communications being carried across the telecommunication system being used to provide the Services.
- 1.3 Any supplier to the Service Provider (involved in the manufacture or supply of goods or services used in order to provide the Services) that is business critical in respect of the provision of the Services to the Authority ("Supplier") shall be set out in the Business Critical Suppliers Schedule.
- 1.4 Notwithstanding Clause 1.3 any supplier involved in the manufacture or supply of goods or services used in order to provide the Services which has access to the network infrastructure supporting provision of the Services to the Authority shall be deemed to be included within the Business Critical Suppliers Schedule and to be a Supplier as defined herein even if not listed in such Schedule.
- 1.5 In the event of any doubt or disagreement as to whether a Supplier is business critical to the provision of Services by the Service Provider to the Authority the Authority's determination shall be final and binding however it shall pay due regard to any representations that may be made by the Service Provider in this regard.
- 1.6 The Service Provider shall apply the standard of care associated with the Impact Level and the Protective Marking specified in the Services Schedule in endeavouring to ensure that:

- 1.6.1 the Services shall not be capable of being unlawfully intercepted within the meaning of the Regulation of Investigatory Powers Act 2000;
 - 1.6.2 the data within the Services shall not be subjected to unauthorised access or modification within the meaning of the Computer Misuse Act 1990;
 - 1.6.3 the Services shall only be provided over equipment situated within those countries specified in the Services Schedule;
 - 1.6.4 the Services shall only be managed from premises situated within those countries specified in the Services Schedule. For the avoidance of doubt “managing” in this context shall include the generation and transmission of communications data relating to the Services as well as all aspects of technical support connected with the Services;
 - 1.6.5 the Services shall be diversely routed into all the premises to which they are supplied unless expressly agreed to the contrary in writing by the Authority; and
 - 1.6.6 the operator of any telecommunication system to which any communication transmitted as part of the Services is sent by the Service Provider applies no less stringent measures than are applied by the Service Provider to the Services.
- 1.7 The Service Provider shall:
- 1.7.1 not change any Supplier without the prior written consent of the Authority, such consent not to be unreasonably withheld and as part of seeking the Authority’s consent to such change the Service Provider shall provide sufficient information to the Authority so as to demonstrate that such change will not compromise security and risk mitigation; and
 - 1.7.2 ensure that it is able on request by the Authority and within a timeframe acceptable to the Authority, to source goods or services from an alternative supplier to the Supplier which are of no less functionality and performance than those supplied by the Supplier to the Service Provider and used in the provision of the Services to the Authority so as to ensure that there is no disruption to the Services.
- 1.8 The Service Provider shall:
- 1.8.1 maintain (including without limitation review no less frequently than every 6 months commencing from the date of this Agreement and continuously update in the light of experience) the risk mitigation plan and supplier isolation plan in respect of the Services as may be specified in more detail in the Services Schedule; and
 - 1.8.2 supply a copy of the updated risk mitigation plan and supplier isolation plan within 30 days of the date of completion of any such review; and
 - 1.8.3 check that the Supplier is conducting similar checks to those set out in this Clause in respect of its risk mitigation plan and supplier isolation plan.

1.9 The Service Provider shall:

- 1.9.1 maintain (including without limitation test no less frequently than every 6 months commencing from the date of this Agreement and continuously update in the light of experience) the business continuity plan in respect of the Services as may be specified in more detail in the Services Schedule;
- 1.9.2 supply a copy of the business continuity plan test results along with an updated business continuity plan within 30 days of the date of completion of any such tests; and
- 1.9.3 check that the Supplier is conducting similar checks to those set out in this Clause in respect of its business continuity plan.

2. Security

- 2.1 Throughout the life of this Agreement the Service Provider shall take all necessary measures to protect the telecommunication system used to provide the Services from unauthorised access including without limitation compliance with the requirements of the Security Schedule.
- 2.2 Without limitation to the generality of this Clause the Service Provider shall ensure that its employees and any other personnel contracted to it and engaged in the supply of the Services to the Authority shall submit to a security check (details of which shall be provided to the Authority) that would be regarded by the Authority as appropriate.
- 2.3 The Service Provider represents that it has received assurances from the Supplier that:
 - 2.3.1 it has conducted security checks on all personnel engaged in providing goods or services used in connection with the provision of the Services to the Authority; and
 - 2.3.2 it has conducted security checks on all goods and services supplied by it to the Service Provider and used in connection with the provision of the Services to the Authority.
- 2.4 The Service Provider undertakes that it has audited such checks by the Supplier referred to in Clause 2.3 and regards them and the conduct of such checks by the Supplier as appropriate with regard to security and risk mitigation in connection with the nature of the Services.
- 2.5 The communications data relating to the Services is hereby deemed to be confidential information of the Authority.
- 2.6 From time to time the Authority may advise the Service Provider of security measures to be carried out by the Service Provider in addition to those set out in the Security Schedule. Such advice shall be final and binding and the Service Provider shall comply with it forthwith.
- 2.7 The Service Provider shall ensure that access to the Services by its sub-contractors shall be mediated by firewalls and similar measures so as to maintain a strict separation between a domain in which any aspect of the Services is provided by a Supplier from any other domain relating to the Services.

- 2.8 The Service Provider shall keep fully informed of the latest best practice security and risk mitigation measures relating to the Services and deploy them as part of the Services whenever appropriate.

3. Escrow

- 3.1 The Service Provider shall enter into an Escrow Agreement within 30 days of the date of this Agreement with a reputable Escrow Agent satisfactory to the Authority in relation to the Escrowed Material on terms including the following:
- 3.1.1 the Escrowed Material shall be deposited in a location in the United Kingdom satisfactory to the Authority;
 - 3.1.2 the Escrowed Material shall be deposited with the Escrow Agent within 30 days of the date of the Escrow Agreement between the Service Provider and the Escrow Agent;
 - 3.1.3 the Escrowed Material shall be updated each time the Service Provider changes the Components described by such Escrowed Material;
 - 3.1.4 all necessary password and encryption details to access the Escrowed Material shall be deposited as part of the same along with all necessary instructions for use and maintenance of the Components;
 - 3.1.5 the Escrowed Material shall contain names and contact details of the Service Provider's employees and the Supplier's personnel experienced in maintaining the Components;
 - 3.1.6 the Escrowed Material shall be kept confidential by the Escrow Agent and not used other than for the purposes of the Escrow Agreement;
 - 3.1.7 the Authority shall be entitled to require the Escrow Agent to audit the Escrowed Material upon request; and
 - 3.1.8 the Service Provider shall secure an assurance from the Escrow Agent that in the event it transfers or assigns the Escrow Agreement it shall only do so to a reputable escrow agent.
- 3.2 The Service Provider undertakes to the Authority:
- 3.2.1 to comply with the terms of the Escrow Agreement above;
 - 3.2.2 that the Escrowed Material is a complete and accurate description of the Components;
 - 3.2.3 that it owns the Intellectual Property Rights in the Escrowed Material or has been granted the right to deal with the Escrowed Material in the manner contemplated by this Clause;
 - 3.2.4 that the Escrowed Material can be released from the possession of the Escrow Agent upon the occurrence of an Escrow Release Event and that it can be used by the Authority or its nominee for the purpose of delivering the Services to the Authority which have been delivered by the Service Provider using the Components;

- 3.2.5 to supply the Authority on request with a copy of the Escrow Agreement and/or any agreement between the Service Provider and a third party granting rights to the Service Provider in respect of the Escrowed Material;
- 3.2.6 to supply the Authority with the identity of any party to whom any of the Intellectual Property Rights in the Components are assigned or encumbered in favour of; and
- 3.2.7 not to terminate the Escrow Agreement or perform any act or permit any omission which would give the Escrow Agent the right to terminate the Escrow Agreement.

4. Representations

- 4.1 Upon request the Service Provider shall produce evidence to the Authority proving to the Authority's reasonable satisfaction the correctness of any representation made:
 - 4.1.1 in any pre-contractual discussions connected with this Agreement;
 - 4.1.2 in this Agreement; or
 - 4.1.3 throughout the term of this Agreement with reference to any information connected with this Agreement.
- 4.2 Failure to provide evidence within 30 days of being requested to do so under Clause 4.1 shall entitle the Authority to enforce any of the provisions of Clause 5.4 as though non-compliance had been revealed as a result of an audit inspection by or on behalf of the Authority, notwithstanding any provision of this Agreement to the contrary.
- 4.3 Prior to each anniversary of the commencement of this Agreement the Service Provider shall provide a letter to the Authority from its Managing Director or equivalent attesting to the fact that having made due and careful inquiry during the preceding period:
 - 4.3.1 all the tests and procedures required by this Agreement have been carried out; and
 - 4.3.2 the Service Provider is confident that its security and risk mitigation procedures with respect to the Services remain effective.
- 4.4 Notwithstanding any provision of this Agreement to the contrary the Service Provider hereby repeats the Next Generation Network representations made by it in writing during any pre-contractual discussions connected with this Agreement and acknowledges that the Authority has relied on these in entering into this Agreement and the Service Provider also warrants the accuracy of all such representations made by it.

5. Audit

- 5.1 The Authority or its duly authorised representative shall be permitted to audit the goods and services used by the Service Provider in the provision of the Services

and its operational records in relation thereto and to interview its personnel used to provide the Services. The Service Provider shall permit access to its premises and personnel to enable such audit.

- 5.2 The Service Provider shall also use reasonable endeavours to secure for the Authority or its duly authorised representative the right to access and audit the premises and records of any Supplier of any goods and services used in the telecommunication system used to provide the Services.
- 5.3 If any audit or other investigation under or in connection with this Agreement reveals non-compliance by the Service Provider with:
- 5.3.1 (Clause 1) Provision of Services;
 - 5.3.2 (Clause 2) Security;
 - 5.3.2 (Clause 3) Escrow; or
 - 5.3.4 (Clause 4) Representations.
- then the Authority shall be entitled to exercise any or all of the options set out in Clause 5.5.
- 5.4 If the Authority or its representative is unable to conduct any audit contemplated by this Clause then the Authority shall be entitled to exercise any or all of the options set out in Clause 5.5.
- 5.5 Subject to Clauses 5.3 and 5.4 and notwithstanding any provision of this Agreement to the contrary the Authority shall be entitled to:
- 5.5.1 elect that the costs of any such audit or investigation or efforts to conduct the same shall be recharged to and paid by the Service Provider forthwith;
 - 5.5.2 elect that the Service Provider remedies such non-compliance forthwith, at its own expense;
 - 5.5.3 elect to re-procure the Services;
 - 5.5.4 elect that all loss, damage, costs and expenses suffered by the Authority and arising out of or connected with a breach in connection with Clause 5.3 or the occurrence of an event under Clause 5.4 including but not limited to:
 - 5.5.4.1 the Authority's costs incurred in connection with any re-procurement; and
 - 5.5.4.2 any charges payable to any alternative supplier engaged following any such re-procurement as a result of any such breach and which are additional to those that would have been otherwise payable to the Service Provider over the term of this Agreement
 shall be recharged to and paid by the Service Provider forthwith;
 - 5.5.5 suspend the Services by service of notice to the Service Provider, such suspension to take effect as of the date specified in such notice;

- 5.5.6 serve notice to the Service Provider (subject to Clause 5.6) that the Services shall not have been chargeable for the period from the date specified in such notice until such non-compliance is remedied to the reasonable satisfaction of the Authority;
- 5.5.7 treat such non-compliance as a material Default; and
- 5.5.8 terminate the Services for material Default by service of notice to the Service Provider, such termination to take effect as of the date specified in such notice and for the purposes of this Clause such material Default shall be deemed to be a Default incapable of remedy.

5.6 Should it be resolved that there was no non-compliance then the unpaid sum shall be payable within 30 days of an invoice having been received and correctly rendered. Subject to any such resolution having been made the Service Provider shall be entitled to levy interest on such unpaid sum from the date that it should originally have been paid as though it were a late payment.

6. Suspension of Services and Step-In Rights

- 6.1 Without prejudice to any other remedy that the Authority may have (whether under this Agreement or otherwise):
 - 6.1.1 where the Service Provider has failed to provide the Services to any agreed service level or otherwise in accordance with this Agreement and such failure has an adverse, material impact on the business of the Authority;
 - 6.1.2 where the Authority reasonably believes that the Service Provider is about to commit such a failure which, if committed, would have such an impact;
 - 6.1.3 where the Authority reasonably considers it necessary in order to carry out any of its statutory obligations, functions or other duties; or
 - 6.1.4 where the Authority is entitled to terminate this Agreement, and/or part of the Services, then the Authority may by giving such written notice to the Service Provider that the Authority considers reasonable in the circumstances that it intends to exercise its rights under this Clause (the "Step-In Right"), take such steps itself or engage others (each a "Step-In Third Party") to take such steps as it reasonably considers necessary to remedy the circumstances or anticipated circumstances giving rise to the Step-In Right.
- 6.2 In the event and to the extent that the Authority exercises its Step-In Right the Service Provider shall:
 - 6.2.1 co-operate fully with the Authority and any Step-In Third Party to facilitate the steps taken;
 - 6.2.2 suspend performance of the Services (the "Step In Services") subject to the Step-In Rights to the extent that the Authority so requests for the purposes of its exercise of Step-In Rights, provided always that, for the

- avoidance of doubt, the exercise of the Step-In Right shall not excuse the Service Provider from its obligation to provide the Services (excluding the Step-In Services for the period only of exercise of the Step-In Right) in accordance with this Agreement or be deemed to frustrate or waive performance of that obligation;
- 6.2.3 grant and procure that any sub-contractor or relevant third party grants the Authority such licences as are reasonably required (for itself or a Step-In Third Party) for the purposes of this Clause provided that these are no more expensive than the charges that would have been payable by the Service Provider; and
- 6.2.4 afford (and procure that its sub-contractors afford as applicable) to the Authority such co-operation, access and use (as applicable) to:
- 6.2.4.1 the Components used to provide the Services and any other goods and services used to provide the Services;
 - 6.2.4.2 all necessary associated documentation relating to the Components used by the Service Provider to provide the Services to the Authority and any other goods and services used to provide the Services so as to enable the same to be operated, maintained and provided;
 - 6.2.4.3 the Service Provider's Intellectual Property Rights in the Components and any other goods and services used to provide the Services used by the Service Provider to provide the Services;
 - 6.2.4.4 the Service Provider's Intellectual Property Rights otherwise connected with provision of the Services;
 - 6.2.4.5 the Supplier's Intellectual Property Rights in the Components used by the Service Provider to provide the Services and any other goods and services used to provide the Services; and
 - 6.2.4.6 premises, equipment, personnel, documents, information or other items as are reasonably required for the purposes of this Clause.
- 6.3 In the event and to the extent that the Authority exercises its Step-In Rights in the circumstances specified in:
- 6.3.1 Clause 6.1.1;
 - 6.3.2 Clause 6.1.4; or
 - 6.3.3 Clauses 6.1.2 or 6.1.3 and where the Authority demonstrates that the Service Provider is in Default,

the Charges in respect of the Step-In Services shall cease to be due or payable for the period of exercise of the Step-In Rights and the Service Provider shall reimburse the Authority as a liquidated debt (or, at the Authority's option, allow by

way of deduction from the Charges) the costs and expenses (including overhead costs) incurred by the Authority in taking the steps or engaging Step-In Third Parties to take the steps referred to in this Clause and in terminating any engagement of a Step-In Third Party.

- 6.4 During any exercise of Step-In Rights, the Service Provider shall be required to put forward proposals to demonstrate to the Authority that it is able to perform its obligations under this Agreement in relation to the Step-In Services. If the Service Provider can at any time demonstrate to the Authority's reasonable satisfaction that it is able to and will remedy the matter giving rise to the Step-In Right or that the matter giving rise to the Step-In Right has been remedied, then the Authority shall at its absolute discretion determine whether or not to terminate the exercise of its Step-In Rights and remove the suspension of the Service Provider's performance of the relevant Services.
- 6.5 If the Authority has exercised Step-In Rights in the circumstances specified in Clause 6.3 for a continuous period of 30 days or more, then this shall, unless the Authority notifies the Service Provider otherwise, constitute a deemed material Default incapable of remedy for which the Authority may terminate this Agreement and/or part of the Services (provided always that such termination shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority).

7. Definitions and Interpretation

- 7.1 Reference to Clauses are references to Clauses of these Special Conditions.
- 7.2 Words and phrases the definitions of which are contained or referred to in the Computer Misuse Act 1990 or the Regulation of Investigatory Powers Act 2000 shall be construed as having the meanings thereby attributed to them.
- 7.3 References to any statutory provision shall be construed as references to those provisions as amended or re-enacted or as their application is modified by other provisions from time to time and shall include references to any provisions of which they are re-enactments (whether with or without modification).
- 7.4 The headings of these Special Conditions are inserted for convenience only and shall not affect the construction of this Agreement.
- 7.5 In these Special Conditions the masculine includes the feminine and the neuter and the singular includes the plural and vice versa.
- 7.6 In the event of any conflict or ambiguity between these Special Conditions and the rest of this Agreement then notwithstanding anything to the contrary in this Agreement these Special Conditions shall override:
- 7.6.1 any term or condition of this Agreement; and
- 7.6.2 any other Schedule of this Agreement.

7.7 The following terms shall have the following meanings:

“Change of Control” – any change of control within the meaning given to the term “control” by Section 416 of the Income and Corporation Taxes Act 1988;

“Components” – any apparatus (including without limitation to the generality of the foregoing any computer software) used in a telecommunication system which is part of a Next Generation Network;

“Escrow Agreement” – an agreement whereby one party agrees to put material which is the subject matter of such agreement into the care of another party;

“Escrowed Material” – All source code to the software and firmware in the Components used by the Service Provider to provide the Services to the Authority and all necessary associated documentation to enable the same to be operated and maintained as deposited with the Escrow Agent;

“Escrow Release Event” – Any Insolvency Event, Change of Control, breach of this Agreement or assignment of the Service Provider’s Intellectual Property Rights in the Escrowed Material where the assignee does not continue the Escrow Agreement within 60 days of being informed of the existence of the Escrow Agreement;

“Holding Company” – has the meaning given to that expression in sections 736 and 736A of the Companies Act 1985 as amended by the Companies Act 1989;

“Impact Level” – the standard of care described by such name as may be more fully set out in the Services Schedule;

“Intellectual Property Rights” – patents, registered or unregistered trade marks or service marks, design rights, applications for any of the foregoing, copyright, database rights, rights in know-how, trade or business names and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom) or in any trans-border system of registration;

“Insolvency Event” – where the Service Provider or its Parent Company passes a resolution, or a court makes an order that the Service Provider or its Parent Company be wound up (otherwise than for the purpose of a bona fide and solvent reconstruction or amalgamation) or a receiver, manager or administrator on behalf of a creditor is appointed in respect of all or part of the business of the Service Provider or the Parent Company, or circumstances arise which entitle a court or a creditor to appoint a receiver, manager or administrator or which entitle the court (otherwise than for the purpose of a bona-fide and solvent reconstruction or amalgamation) to make a winding up order or the Service Provider or its Parent Company ceases to trade (otherwise than in connection with a bona fide and solvent reconstruction or amalgamation) or is unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 or any similar event occurs under the law of any other jurisdiction;

“Next Generation Network” – ‘A Next Generation Network (NGN) is a packet-based network able to provide services including telecommunication services and able to

make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.’ – International Telecommunication Union.

“Parent Company” – any company which is the ultimate Holding Company of the Service Provider or any other company of which the ultimate Holding Company of the Service Provider is also the ultimate Holding Company and which is either responsible directly or indirectly for the business activities of the Service Provider or which is engaged in the same or similar business to the Service Provider; and

“Protective Marking” – the security standard described by such name as may be more fully set out in the Services Schedule.

(6b) Conditions for Existing Telecommunication Contracts

Authorities should endeavour to ensure that a clause, along the following lines, is included within (1) all existing non NGN-based telecommunication contracts and (2) all new contracts planned to be provided using traditional technology where the possibility of migrating to NGN-based technology during the contract cannot be excluded. This would provide the Authority with the right of veto should a service provider wish to migrate to an NGN-based solution at a future point in time.

'If the Service Provider wishes to implement a Next Generation Network to provide some or all of the Services then any such change shall be subject to the Change Control provisions of this Agreement and the Authority shall be entitled to require such additional assurances including with regard to security and risk mitigation as it deems appropriate. For the avoidance of doubt "Next Generation Network" shall mean a packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users. Failure to comply with the requirements of this Clause shall be treated as a material Default.'

When migrating to an NGN-based telecommunication solution, legal advice should be sought to ensure full compliance with the EU procurement regime, i.e. that the migration does not result in the requirement becoming materially different to what was originally advertised in the *OJEU* Notice, thereby necessitating a formal re-competition.

7 Contract and Supplier Management

In addition to best practice contract and supplier management principles, this section covers some key NGN-specific issues that should be considered during the operational phase of the contract. It is emphasised that this is not intended to be a complete guide to contract and supplier management.

Once a contract has been let, it must be effectively managed in order to ensure that the requirements are met. For more strategically important contracts and suppliers, **supplier relationship management** may be important as well as the more operational **contract performance management**.

Some of the key points that should be considered for every major contract include:

- Clear ownership and governance of contract and supplier management activities.
- Development and implementation of appropriate contract performance measures and regular reviews with suppliers.
- Risk management processes for key contracts and suppliers.
- Key staff involved in these activities are suitably skilled.
- Supplier relationship management (SRM) processes for the most strategic relationships.

Further guidance on contract and supplier management is available from a number of sources, including [OGC's Managing Contracts and Service Performance guidance](#).

Whilst not exclusive to NGN-based telecommunication services contracts, the following guidance is particularly relevant to such contracts. As a minimum, contract managers responsible for NGN-based telecommunication services contracts should:

- Address at each (monthly or quarterly) contract review meeting:
 - Any planned material changes to the provision of the service, thereby maintaining your position as an 'informed customer'.
 - Any new security and risk mitigation measures being applied to protect the network, thereby reinforcing the importance of security and risk mitigation and ensuring that the service provider remains committed to continual improvement.
 - What the service provider sees as the emerging issues and risks associated with NGNs and how they plan to mitigate them. Again, reinforcing the importance of security and risk mitigation, and ensuring that the service provider does not become complacent.
- Review on a regular basis (e.g. every six months) the latest high-level findings from the service provider's business continuity plan testing, their business critical/tier one supplier audits, and the checks they have carried out in respect of undocumented functionality. This will help ensure that such tests and checks are being carried out and that issues are being addressed.
- Review on a regular basis (e.g. every six months) the latest copies of the service provider's risk mitigation plan, business continuity plan, and supplier isolation plans to ensure that they are being appropriately maintained and that issues are being addressed.

- Obtain on an annual basis a Letter of Attestation warranting the security of the solution.
- Refute all attempts to 'dilute' any clauses pertaining to the right of audit or onsite inspections. Your contract may be needed as the vehicle by which other government agencies can carry out essential audits and onsite inspections.



Office of Government Commerce

Office of Government Commerce, Trevelyan House, 26 – 30 Great Peter Street, London SW1P 2BY
Service Desk: 0845 000 4999 **E:** ServiceDesk@ogc.gsi.gov.uk **W:** www.ogc.gov.uk

About OGC

OGC - the UK Office of Government Commerce - is an Office of HM Treasury.

The OGC logo is a registered trademark of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the US Patent and Trademark Office

PRINCE2 is a trademark of the Office of Government Commerce

OGC Service Desk

OGC customers can contact the central OGC Service Desk about all aspects of OGC business.

The Service Desk will also channel queries to the appropriate second-line support. We look forward to hearing from you.

You can contact the Service Desk 8am - 6pm Monday to Friday

T: 0845 000 4999

E: ServiceDesk@ogc.gsi.gov.uk

W: www.ogc.gov.uk

Press enquiries

T: 020 7271 1318

F: 020 7271 1345

Cover image

www.freeimages.co.uk