

RESILIENCE IN CONVERGED NETWORKS

GOOD PRACTICE GUIDANCE

May 2009

Abstract: Converged networks, also known as next generation networks, (NGN), are increasingly used to provide telecommunications services. As the components of risk are all increasing it is important for buyers and users of modern telecommunications services to understand the issues around resilience and be able to discuss these, as an intelligent customer, with their providers. The Guide describes a risk management approach; provides a number of questions that can be used for self assessment of a customer environment; and a set of questions designed to develop a useful dialogue between the intelligent customer and the service provider.

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to CPNI. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer

CPNI has taken every care in preparing this protective security advice, which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

Resilience in Converged Networks: Good Practice Guidance

CPNI acknowledges the assistance of UK telecommunications providers, CNI customers and Government Agencies, in providing the input into this process and thanks them for their efforts and co-operation.

UK Network Security Information Exchange (NSIE)

The UK Network Security Information Exchange (UK-NSIE) was formed in April 2003 to share sensitive information and work together within the Information and Communications Technologies sector for the benefit of the UK CNI as a whole. The forum includes members from traditional telecommunications providers, core mobile operators and telecommunications industry organisations.

EXECUTIVE SUMMARY	4
1. INTRODUCTION.....	5
2. SCOPE OF THE GUIDE	5
2.1. AIMS OF THE GUIDE	6
2.2. AUDIENCE FOR THE GUIDE.....	6
2.3. APPROACH ADOPTED FOR THE GUIDE.....	6
2.4. STRUCTURE OF THE GUIDE AND HOW TO USE IT	6
2.5. WHAT IS A CONVERGED NETWORK?	7
3. UNDERSTAND WHY RESILIENCE IS IMPORTANT	8
3.1. THE COMMUNICATIONS ENVIRONMENT.....	8
3.2. THE ASSURANCE OF CONVERGED NETWORKS	9
4. DECIDE WHAT RESILIENCE IS NEEDED.....	9
4.1. RISK ASSESSMENT	9
4.2. SELF ASSESSMENT QUESTIONNAIRE	10
4.3. SERVICES JUDGED TO BE MEDIUM/LOW RISK	11
4.4. SERVICES JUDGED TO BE MISSION CRITICAL AND HIGH RISK.....	12
5. PRINCIPLES OF ‘BEST PRACTICE’ FOR CONVERGED NETWORKS.....	12
5.1. SINGLE POINTS OF FAILURE	13
5.2. TRANSPARENCY	13
5.3. DEPENDENCY ON A SINGLE PROVIDER.....	14
5.4. DUE DILIGENCE IN SELECTING THE PROVIDER	14
5.5. EMERGENCY SITUATIONS	15
6. HOW TO ENSURE EFFECTIVE SOLUTIONS.....	15
6.1. RESILIENCE OPTIONS	16
6.2. NETWORK RESILIENCE.....	17
6.3. NETWORK INFRASTRUCTURE: RELIABLE COMPONENTS.....	18
6.4. CORE NETWORK CONSIDERATIONS.....	18
6.5. ACCESS NETWORK CONSIDERATIONS	19
6.6. THIRD PARTY ACCESS TO CORPORATE NETWORKS.....	20
7. SUMMARY OF RECOMMENDATIONS	21
GLOSSARY	24
ACKNOWLEDGEMENTS	27
ANNEX 1 - SELF ASSESSMENT QUESTIONNAIRE.....	28
ANNEX 2 – TWENTY QUESTIONS TO ASK YOUR PROVIDER	31

EXECUTIVE SUMMARY

The risks to telecommunications have increased:

- The threat from the insider and from organised crime has increased;
- The vulnerability of the network has increased with complexity and increased shared access;
- The impact of loss has increased as society and the economy becomes more dependent on telecommunications.

As networks converge, the development of Next Generation Networks (NGN) has introduced a new paradigm to telecommunications and a number of basic issues have changed:

- Previously segregated networks for voice, data and control (signalling) converge into one within an operator domain;
- Platforms that use complex communications protocols based on open standards, often provided by non-traditional suppliers, carry the traffic;
- Confidentiality is a requirement of the data owner while the service provider is more focussed on network availability.

However, the typical converged network combines the robustness of the IP network with the resilience of the legacy transmission layers.

Work performed by government and industry together indicates that a well designed converged network can provide assurance commensurate with legacy PSTN.

Organisations should be able to identify their critical applications and services, and the telecommunications services they depend upon, and discuss the arrangements to make these as resilient as necessary with their service provider.

Where appropriate, additional protection should be procured; this is particularly applicable if there is a dependence upon international connectivity.

Where availability is a major issue, use a single provider to guarantee separation and work with this provider to achieve full transparency of the service and its components.

If home-working is going to provide a critical service to the organisation in the event of a mass evacuation scenario, organisations should be confident that the provision and structure of the remote access service will support this when everyone else is trying to do the same.

1. Introduction

The UK has, for many decades, benefited from a public switched telephone network that has delivered a reasonable expectation of privacy and integrity of communications, and that has offered substantial resilience at the regional and national level. Packet switched services provided to the private and public sectors have had similar characteristics.

Over the past few years, the components of risk (threat, vulnerability and impact) have all increased, and are expected to continue increasing for the foreseeable future as telecommunications move into a converged network environment. As this continues it is important for organisations to understand how the factors affecting resilience may have changed.

The threat has increased as disgruntled employees and criminals find new ways to exploit communications services. They may wish to damage communications services as a way of attacking a third party, for example to disable security measures or to steal data; or they may wish to attack the communications system directly through vandalism, theft of property, fraud or extortion by revenue denial; or their motivations may be ideological.

The vulnerability of the telecommunications network is increasing, as deregulation and local-loop unbundling brings a greater variety of suppliers and contractors into the industry, while the increasing use of internet technologies means there is more awareness of security weaknesses amongst those wishing to cause harm.

The potential impact of any damage is also increasing as society and the economy are increasingly dependent on global communications services for just-in-time business delivery, on-line banking and retail, and access to health and public sector services.

The Guide attempts to answer the “Why”, “What”, and “How” aspects of telecommunications resilience by providing questions for the reader to ask of their own organisation, and of their telecommunications provider. It also provides a set of recommendations written to make the reader a more informed customer.

‘Best Practice’ is defined as those measures that can be taken to guarantee resilience, where cost is not the main issue. ‘Good Practice’ can therefore be defined as those measures which can be taken to provide resilience commensurate with the corporate risk strategy. It is important for an organisation to understand when Best Practice is necessary, and when Good Practice is more appropriate.

2. Scope of the Guide

In May 2004, the original ‘Good Practice Guide to Telecommunications Resilience’¹ was issued. The scope of this new guide aims to complement the original guide by looking at new resilience issues and solutions resulting from convergence as

¹ Good Practice Guide to Telecommunications Resilience - <http://www.cpni.gov.uk/docs/re-20040501-00393.pdf>

described below. This new guide recognises that these emerging networks are changing and evolving at different rates for different service providers.

Within this document the title ‘Resilience in Converged Networks: Good Practice Guidance’ will be referred to simply as the Guide. The Guide deals with the resilience of telecommunications services in a converged telecommunications environment, referred to as ‘services’.

The scope of the Guide is the resilience of converged networks that carry voice and data services over the fixed and mobile (wireless) infrastructure in both the public and private network domains.

2.1. Aims of the Guide

The aims of the Guide are to raise awareness of the need for telecommunications resilience in a converged network environment and to bridge the knowledge gap between the language, expectations and requirements of the customers, and the language and capability of the providers.

2.2. Audience for the Guide

The audience for the Guide are the people who have to commission, specify, audit or procure resilient services in a converged network environment. At the time of writing this Guide most providers had started the migration of services to a converged network environment but some were more advanced than others. Although it is recognised that large corporate organisations will have extensive knowledge and experience in this area, feedback has shown they see value in the Guide as a reference standard and possible compliance document. For others, in both large and smaller organisations, the document will help them to become a better-informed customer of resilient services.

2.3. Approach adopted for the Guide

Like the original guide, the approach adopted within the Guide is based on providing a choice. This choice is based on an understanding of the risk: mission critical risks will by their very nature demand the highest levels of resilience, which in the context of this Guide are referred to as ‘Best Practice’.

High levels of resilience incur additional costs in equipment and process overhead and not every business or institution can therefore justify the cost associated with Best Practice. Some will therefore choose a level of Good Practice commensurate with the risk.

2.4. Structure of the Guide and how to use it

The Guide structure is designed to describe why resilience is an issue in a converged environment, what resilience is needed and how to ensure effective resilience solutions.

Where helpful to an understanding of the issues a brief description of key technologies has been provided within the text. However, it is not the aim of the Guide to be a technical manual. A brief expansion of some of the technological terminology can be found in a Glossary at the end of the Guide.

Annexes 1 and 2 provide a series of questions to be asked within an organisation, and by an organisation to its service provider, respectively, to help both parties understand the requirement and how it can be provided.

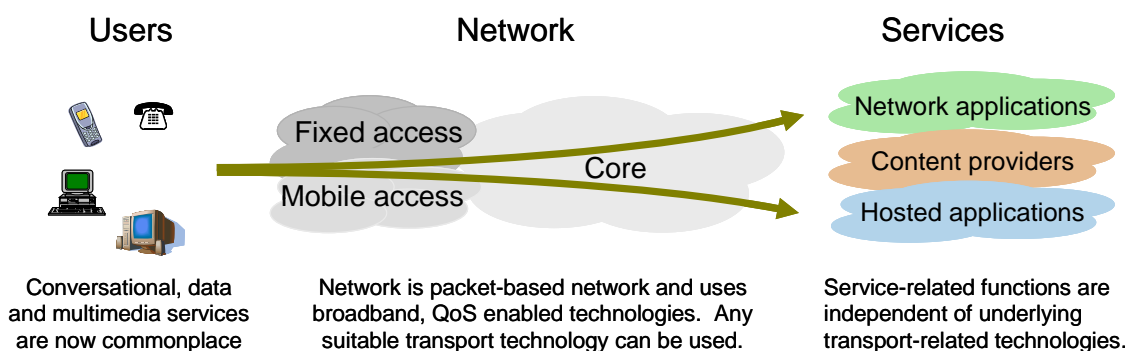
2.5. What is a Converged Network?

A converged network is a packet-based network which can carry voice and data services together, whether network access is fixed or mobile: for the purposes of the Guide, the terms Next Generation (NGN) and converged network embrace both access and core parts of the network.

An access network refers to the network that connects a consumer or business to a local telephone exchange or other local hub. It may include copper pair cables in the case of a public telephone network operator, radio systems in the case of mobile or hotspot networks or coaxial cable in the case of cable TV networks.

A core network is the central part of a telecommunications network that sets up connections to other users and provides a range of services to customers who are connected by the access network. Core networks are most commonly based on optical fibre interconnections, particularly where high capacities are needed.

A backhaul network is commonly used to interconnect access and core networks.



NGN gives users unrestricted access to different services & service providers

Fig. 1 The converged network concept

Convergence also takes a new approach to the way in which services are delivered, making a clear distinction between 'network' and 'services'. According to the ITU-T's definition of NGN,² a converged network offers unrestricted access by users of different services. An illustration of this is given in Figure 1. Where services are international they may have a dependency upon a global infrastructure and may be carried over a range of networks and submarine cables.

While this description sounds rather like the Internet, there are in fact two major differences. A converged network provides access to 'known' users whereas the

² The ITU-T defines a Next Generation Network at:
http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html

Internet allows access to anybody and can provide anonymity. This enables a converged network to offer stronger security than the Internet. Secondly a converged network supports traffic engineering techniques that allow different services such as voice, data and video to be assigned their own portion of the available bandwidth and for that portion to be given appropriate prioritisation. Unlike the Internet, this enables quality guarantees that are essential for mission critical applications to be provided.

3. Understand why resilience is important

3.1. The Communications Environment

The corollary to the development of the NGN and the convergence of voice, data and management on to a single platform has been the loss of the legacy of trust inherent in the public switched telephone network (PSTN). The PSTN had traditionally been seen as a trusted environment and one which was routinely considered to be capable of providing a resilient service. The perceived trust in the PSTN was inherited from the original single network, which was in security terms a single security domain subject to a single security policy. As the network opened up and other operators became connected, the licensing regime and a robust interconnection policy maintained a high level of trust. Availability was assumed to be provided through service level agreements and typically quoted as a figure, i.e. available for 99.xyz% of the time, equivalent to a number of minutes of downtime per user each year in accordance with defined agreements.

Within the core network, three significant changes occur when converged network services replace PSTN:

- Previously segregated networks for voice, data and control (signalling) converge into one within an operator domain;
- Platforms that use complex communications protocols based on open standards, often provided by non-traditional suppliers, carry the traffic;
- Confidentiality is increasingly a requirement of the data owner while the service provider is more focussed on network availability.

In the access network, however, one of the principal areas of concern continues to be the single connection typically provided between customer premises and local exchange or Point of Presence (POP). This is of particular concern in high-density areas such as the City of London, and is often quoted as a classic example of a single point of failure.

Local Loop Unbundling (LLU) obliges the incumbent operator, usually BT, to allow other providers use of the last mile access assets, resulting in third party providers selling circuits over the same cable routes as the incumbent. An 'unbundled' connection to a customer will normally follow the same route as the incumbent's service and will not automatically provide a physically separate connection. As there is no requirement for either provider to discuss the use of these circuits with the other, they may be unaware that a customer possibly intended the circuits to be physically separated. A customer may be lulled into a false sense of security by purchasing services from two different operators. True separation would have been possible by asking one provider for two separate circuits.

The global economy depends upon communications and has an increasing dependency upon submarine cables to carry services. Submarine cable systems are reliable and robust but face a number of environmental threats. This means cable damage is commonplace and it is vital that any organisation outsourcing critical systems or otherwise dependent upon international connectivity has taken explicit steps to understand the resilience provided.

3.2. The assurance of converged networks

Recognising that the advent of convergence in information and communications technology was going to have a major impact on telecommunications in UK, a group of experts from industry and government were tasked to determine the level of assurance that any PSTN voice replacement service, and its associated supporting and management infrastructure, should support. They used the available technical knowledge of the capabilities of the converged network, considered the supply chain issues and public perception, and drew upon years of experience in the assurance of networks to identify a suitable assurance level for converged networks. It was determined that converged networks using untrusted³ protocols, and equipment from non-traditional suppliers can reasonably be expected to be designed and implemented to provide a level of performance within the tolerances of PSTN.

4. Decide what resilience is needed

4.1. Risk Assessment

The risk assessment approach outlined below has not fundamentally changed from that described in the original guide. What has changed, however, are the types of risks associated with resilience for converged network services. In particular, the fact that converged network technologies, standards and processes are emerging and evolving indicates that risks will also change more frequently. This may not be transparent to the customer organisation, as the functionality of the service may stay exactly the same as it was before migrating to a converged network environment.

It is important to recognise that in any organisation, not every communications link, system or circuit needs 100% availability. Systems range from non-essential leisure and administration to mission critical. In general the majority of systems such as telephones, and most e-mail services can tolerate some downtime, because they are either not systems which require immediate response or are not mission critical. However, those systems that are mission critical need to have specific resilience measures in place. A realistic risk assessment of the corporate communications systems will identify these.

This section provides information that the reader can use within a risk assessment exercise.

³ Untrusted: stems from the uncertainty regarding the reliance that can be placed on the characteristics of an organisation or elements from a different security domain and using different security policies. In the context of NGN, all third party components and suppliers are considered untrusted unless and until a formal assessment of the risk of use has been carried out.

Recommendation 1: Identify those applications and services that are deemed mission critical and which carry a high risk to the business if the telecommunication services they depend upon are disrupted.

Recommendation 2: Wherever possible separate out the high risk services from those that only carry a medium or low risk to the business if disrupted.

Recommendation 3: Discuss your requirements for availability of the services you have identified with your service provider and ensure that you are content with the availability provided.

There will be instances in which a high risk application is ‘bundled’ with a number of medium or low risk applications in one service, either end-to-end or for a segment of the link. This could for example be a VPN⁴, which, with Quality of Service (QoS), can provide voice, video and e-mail applications. In these cases, the composite or aggregate service should be classed as high risk and treated accordingly.

Recommendation 4: Associate the high-risk (to the business) applications with the services they are provided over.

The remainder of this chapter focuses on identifying what resilience is needed based on an understanding of the risk.

Recommendation 5: Analyse the threats and vulnerabilities to the mission critical high risk services – e.g. natural disaster, malicious attack, single point of failure, commercial dependency, any lack of transparency in how they are delivered.

In reality, many risk assessments will fall somewhere between mission critical and low risk. The Guide describes ‘Best Practice’ in addressing the threats/vulnerabilities outlined and leaves the reader to make the decision on how much of this best practice they can justify on the basis of cost and risk mitigation. In doing this they will in effect define their own good practice.

4.2. Self Assessment Questionnaire

The ‘Self Assessment Questionnaire’ in Annex 1 has been designed to provoke analysis and discussion in order to provide input to a risk assessment. Annex 2, ‘20 Questions to ask your Provider’, has been produced with the cooperation of a number of telecommunications providers to facilitate discussions between the customer and the provider(s) on the resilience of the telecommunications services provided or proposed, as part of a risk assessment exercise. It recognizes that different providers may supply different services.

Recommendation 6: Conduct a self-assessment to understand the extent of your risk exposure due to any shortcomings in the resilience of the telecommunications services in use.

Unlike legacy PSTN, a converged network allows different classes of service to deliver different levels of resilience. There can be three fundamental levels of availability in a converged network environment:

⁴ Virtual Private Network: see Glossary.

1. 'Sub PSTN' level of availability applies to converged network technologies which do not meet the availability assurance levels equivalent to legacy PSTN. Voice over IP services over the public Internet would fall into this category.
2. Equivalent PSTN level of availability applies to converged network technologies which meet the availability assurance levels of legacy PSTN. It is expected that most large providers will provide this level of service as standard. Work on the availability of converged network components indicate that an availability equivalent to that of PSTN is achievable.
3. High levels of availability are required where loss of service is likely to be mission critical or result in serious loss to the business. These services will be designed specifically for high availability using techniques such as separacy and diversity to overcome single points of failure in much the same way as they have in the past. This will address single points of failure in the local loop which may need dual connections to the local nodes.

For a business to get best value for money it is therefore important to assess which telecommunications services can be met by PSTN equivalent levels of availability and which ones require higher availability. The choice may depend on which part of the company is using the service and what they are using it for. It may also depend on whether the service is packaged or 'bundled' with others (for example VoIP may be bundled with a VPN). The risk assessment approach described in section 4.2 will identify those areas of the business where the business could survive if certain types of communications fail for a period, as well as those where unbroken telecommunications services are of critical importance.

To assess what would happen in a particular situation it will be important to understand the resilience and recovery processes that the provider has in place.

4.3. Services judged to be medium/low risk

The resilience of any service depends upon the inherent reliability of the components used to deliver the service and on the network protection and restoration methods used (see Section 5.1). While providers choose their equipment, architecture and repair processes so that good network resilience is inherent within their standard services, they must do this within a budget. The very highest resilience can only be achieved by taking additional measures which will add to costs. At the other extreme some providers offer services with little or no guarantees of availability (such as best effort Internet services) so that users can obtain the lowest possible prices.

If the risk assessment has shown that an assurance level equivalent to a standard PSTN service is adequate and occasional interruptions to service amounting to say a few hours per year would not prevent the company from achieving its mission, then the service may be considered to be at medium risk. It is envisaged that providers will offer these services to customers who can identify where the requirement for continuity of service overrides the prospective cost savings of using the lowest availability level. It is expected that most users will adopt the standard service, with resilience equivalent to the PSTN, but will choose a higher resilience service for critical business functions (see section 4.4).

If a risk assessment has shown that best efforts are good enough for services with low criticality then it may be appropriate to choose a telecommunications service offered at ‘sub PSTN’ levels of availability.

Recommendation 7: Look carefully at the cost/benefit of ‘sub PSTN’ services in relation to the reduced quality of service and challenge the provider to explain what, if any, resilience is being offered.

These considerations should help customers determine if the services they buy have sufficient resilience for those applications deemed to be medium or low risk to the business.

4.4. Services judged to be mission critical and high risk

Where a risk assessment has identified services as being high risk then additional consideration must be made when selecting services and a service provider. Mission critical/high risk applications justify high levels of availability. Examples of high risk applications include financial transactions, emergency/lifeline services and control systems. A high level of availability can be provided in a variety of ways including automatic protection and the elimination of single points of failure within the access and core network. In the context of this Guide:

- Protected services or circuits are those services identified between provider and customer as requiring a superior response than normal or standard services.
- Separacy describes the physical separation of specific circuits so that there are no common components, interconnection points or cable routes.
- Diversity provides alternative infrastructure and connectivity in the event of congestion or failure.

Recommendation 8: Ask your provider how much of the network path for your service is automatically protected and, if there was a converged network equipment or cable failure, how long it would take to restore service.

It should be noted that separacy guarantees diversity, but diversity does not guarantee separacy, which in commercial terms means that diversity services can be lower cost than separation based services.

In general separacy is designed into the converged network core, while this is not usually the case for the access network where higher levels of availability are provided at a cost.

Recommendation 9: Work with your provider to understand the physical routes taken by the systems supporting your critical services.

5. Principles of ‘Best Practice’ for converged networks

If any services are ‘mission critical’, then justifying the high cost of best practice to ensure they are resilient is going to be easier than if they are not mission critical. This section looks at best practice and focuses on addressing the threats relating to single points of failure, transparency and provider dependency.

Best practice for mission critical services guarantees resilience by eliminating single points of failure, by guaranteeing separacy and providing protected circuits, and by providing full transparency in using a single provider to guarantee separacy.

5.1. Single Points of Failure

In legacy networks, concerns relating to the physical threat of disruption caused by a single point of failure, for example a damaged cable, or a disabled exchange have always existed. To mitigate the risk against a single point of failure the traditional solution has been to provide separate or diverse infrastructure elements.

For a converged network the use of intelligent routing algorithms and packet-switched architecture already provides a high level of protection against a single point of failure. This does not mean that all services will be completely uninterrupted by a network failure, although in general the interruption will be minimal and traffic quickly re-routed to avoid the failure. For applications requiring the highest levels of availability, separacy can still be introduced in a converged network environment.

Resilience can be further improved by choosing components that have inherent resilience because of their design. The mechanisms typically involve some form of 'hot-standby' and a rapid transition to alternative network elements or components. It is relevant to consider the time taken to complete restoration of the traffic. Service providers use self healing technologies with built-in redundancy in the core network and at the transport layer. In some cases however, separacy has been provided in the core network, at significant additional cost, where the redundant and self healing features are not considered by the customer to be enough to mitigate the risk.

Recommendation 10: If the risk exposure to a single point of failure is not acceptable, then consider using end to end separation of all components, including separate building entry points, risers, ducts, exchanges and core network routes;

Recommendation 11: Use components and services with inherent resilience; for example ask for a protected service rather than a standard unprotected service.

Recommendation 12: Use service provider who can offer true separacy for applications requiring the highest levels of availability.

5.2. Transparency

Within the context of this Guide, transparency describes the extent to which the customer has visibility of the services provided, and the way in which they are provided. As providers migrate existing services to converged network platforms transparency can be more important than it was in the PSTN environment.

Contracts and Service Level Agreements should include the right for the customer to have visibility of their network services. This is more likely to occur if the customer has a close relationship with the provider, and where the provider knows they are the single provider for the end-to-end separacy service. Providing additional resource by both parties to help build these relationships will also help the customer make full use of the information provided and improve the level of confidence and quality of the assurance.

If the risk exposure stemming from any lack of transparency is not acceptable, the following recommendations should be considered:

Recommendation 13: Use a single provider for single end to end separacy and diversity services and do not rely on dual providers to guarantee separation;

Recommendation 14: Invest more time and effort into building relationships with a single supplier, for example by sharing testing and assurance activities;

Recommendation 15: Make allowance in the contract or SLA for transparency of the service provision, including separacy and diversity, both at the time of provision and through the life of the contract.

Recommendation 16: Understanding your provider's migration strategy to converged networks and agree the migration issues to jointly be reviewed and actioned.

5.3. Dependency on a single provider

Convergence strengthens the separation between networks and the services running over them, which means that customers need no longer be served by a single provider for all services. A competitive marketplace means that customers can now consider using different providers for specific services and networks as well as multiple providers for the separate elements. This does place greater responsibility on the customer to co-ordinate the service and network elements and consequently many will choose to continue to source both from a single provider. As previously described a single provider solution can provide full separacy and transparency. However, if dependency on a single provider for a particular service is identified as a high risk then using more than one provider for each end-to-end service can reduce it.

There are some advantages to adopting a multi-provider strategy; for example it counters the risk of a provider going out of business, and in some cases may produce short term financial advantages. A duplication of providers for two separate and distinct end-to-end services has been adopted by at least one CNI organisation.

Recommendation 17: If the risk associated with a dependency on a single provider for specific services is not acceptable, then consider the use of more than one provider for each critical service but take steps to ensure that there are no common points or single points of failure.

5.4. Due diligence in selecting the provider

Since the previous guidance was issued the telecommunications industry has changed substantially. With the globalisation of the supply chain and a wider supplier base, greater understanding of the risks in the supply of components has required more clarity in terms of financial and legal responsibilities.

Partnerships with third parties are an essential part of business. However, it is equally essential that interaction with the third party does not compromise a CNI organisation's ability to protect its key data assets. CNI organisations should review their third party access requirements to ensure that the existing measures meet the business needs.

Recommendation 18: Identify those personnel in your company who are able to request or authorise changes to the service configuration, and give your Network Provider a pre-authorised list of names.

5.5. Emergency situations

In certain types of emergency situation, for example a pandemic or long term evacuation of business premises, large numbers of people could be required to work from home using remote access. Broadband networks are economical because they allow expensive resources to be shared among many people. When providers plan their broadband networks they make assumptions about how many people are likely to use the broadband service at the same time so that they can ensure that sufficient of the shared network resources are available. Domestic or residential broadband access systems are designed to offer high access speeds. The bandwidth, or data rate, available is dependent upon the number of users, as determined by the service provider for normal use. However, the average office desktop is directly connected to a port running at 100 Mb/s. The pattern of broadband usage in a pandemic would be very different to that in a normal situation and some bandwidth dependent applications will suffer. If business critical applications are expected to perform at high data rates under evacuation or home working conditions, then domestic broadband may not be suitable.

Recommendation 19: If broadband access is critical to your business applications in an evacuation scenario then consideration should be given to providing dedicated bandwidth capabilities for key personnel or locations.

Initial studies indicate that the choke points in this case would be the remote access servers (RAS) at the corporate gateway rather than the public network, where increased contention for service may result in a slower but workable service.

Recommendation 20: Scale your remote access servers to be able to cope with those numbers of members of staff you need to have access in the case of an evacuation or a pandemic situation.

6. How to ensure effective solutions

To recap the previous sections, in a converged network, services run over the network and these can now be considered separate entities. The customer has maximum influence over the provider in terms of the services procured. The network, however, is the provider's domain. The network consists of the access network, over which the customer has a major influence, and the core network which is the provider's area of expertise but where the customer can still have some influence.

In the context of this Guide, public and private networks are defined as:

Public Network: A network used to provide a service to the general public, usually on a subscription or other payment basis. For example a national telephone system, including local loops, exchanges, trunks, and international links for providing telephone service to the general public, or the public Internet. This includes the components used to provide commercially leased facilities used to build private networks.

Non public (Private) Network: Any network used to communicate within an organization (as distinct from providing service to the public) or to supply such communications to organisations, based on a configuration of their own or commercially leased facilities. The term includes networks used by private companies, state enterprises, or government entities.

The resilient solutions for public networks and private networks are different for three reasons:

- Public and private networks are used by companies in different ways and for different services;
- Ofcom sets different regulatory requirements on public and private networks: the requirements on public networks are more stringent than those on private networks;
- Network providers may use different resilience solutions for public and private networks.

Essentially, for a given service, CNI organisations will either buy services over a public network or build a private network. The emphasis of this paper is on the former and organisations that build private networks are strongly advised to take expert advice on the most resilient architectures to use for their particular application. This paper does not attempt to be a text book on resilient architecture, but highlights the issues that should be considered.

6.1. Resilience Options

Converged network services include voice, higher bandwidth broadband internet access and 3G (broadband) mobile. Within these main headings a wide range of different service features are available such as voice messaging, call redirection and instant messaging. The most common service offering over a converged network to private/enterprise users is a VPN. Enterprises use VPNs to obtain a well controlled service domain with defined quality, security and costs. They can be used to carry a wide range of services including voice, video and data.

6.1.1. Voice over IP

The principal public service offered by NGN is VoIP telephony. Access to this service may be via traditional analogue copper pairs that terminate at a local concentrator, or may be via a broadband technology such as DSL. Call quality is controlled through the use of traffic engineering techniques available in the IP/MPLS architecture. This will ensure that call quality is reliable and not prone to the variable levels sometimes experienced when using VoIP over the Internet. Additionally, private network based services include Managed VoIP⁵, telemetry, control and alarms, leased lines, Ethernet connections, card services, cash machines and banking.

VoIP has been used in restricted ways within public voice networks for several years, such as in the interconnections between cellular and fixed networks and in the international connections where bandwidth efficiency is particularly important. VoIP is also widely used in call centres to ease the integration of voice and data services, and because it enables other benefits such as virtualisation and predictive dialling. Thus, many of the component parts of a converged network have been subject to considerable examination and stress testing in a live environment without significant issues.

⁵ CPNI advice on Managed and Enterprise VoIP can be found at www.cpni.gov.uk

6.1.2. Broadband Internet Access

A large and growing part of the UK economy uses some form of Internet access. Broadband provides access to IP based core networks, in particular to the Internet. The most widely used applications are VoIP⁶, email, surfing the WWW, purchasing and banking. However TV viewing and video clips are gaining in popularity and broadband is often used for finding or downloading information for work. As video based, higher speed services grow in popularity and as broadband continues to grow, providers will need to progressively upgrade their broadband network bandwidth to keep pace with demand. Any delays in upgrading needed bandwidth will result in contention in busy periods with consequent reduction in available bandwidth and performance. A specific example of this contention would be in the event of a pandemic incident which is described later.

Recommendation 21: Recognise that the load on your broadband network will increase with time and ask your provider how he guarantees that service performance for both voice and data will not fall below the agreed limits.

6.1.3. Legacy Control and Telemetry Services

Almost all critical industrial infrastructures and processes are managed remotely from central control rooms, using computers and communications networks. The flow of gas and oil through pipes, the processing and distribution of water, the management of the electricity grid, the operation of chemical plants, and the signalling network for railways. These all use various forms of process control and supervisory control and data acquisition (SCADA) technology⁷. A detailed analysis of SCADA resilience is beyond the scope of this paper, but CPNI provides specific advice on SCADA issues.

There have been concerns and much discussion surrounding the latency of IP based networks and their ability to support critical utilities. Any organisations with remote assets that require control or supervisory communications, and particularly systems that have been used for some time, should discuss their requirements with their service provider in some detail.

This emphasises the need for customers to be vigilant when migrating existing services across to a converged network and to seek guarantees from the supplier about the ability of the proposed solution to fully satisfy the service requirements.

Recommendation 22: Any organisations with remote assets that require control or supervisory communications, and particularly systems that have been used for some time, should discuss their requirements with their service provider in some detail.

6.2. Network Resilience

Resilience in a network is provided by

- The use of highly reliable components;
- The provision of redundant capacity into the infrastructure and the prompt use of it.

⁶ CPNI advice on Internet telephony can be found at www.cpni.gov.uk

⁷ CPNI advice on SCADA vulnerabilities and mitigation can be found at www.cpni.gov.uk

The choice of reliable components is the responsibility of the provider and can be viewed as a property of the network. The amount of redundant capacity and the way in which it is switched in is a part of the network design and is a major influence on the resilience of different services. While the network design is carried out by the provider, it is in response to customer requirements for a particular service level and reliability target.

6.3. Network Infrastructure: Reliable Components

6.3.1. Router reliability

Users of enterprise networks should be aware that in general the availability figures for router based networks have been significantly lower than that required by carrier grade telecommunication networks. Availability figures for routers have typically been in the region of 99.95% to 99.99%. The current generation of routers can achieve 99.999% availability by the use of dual hardware and software redundancy in a single router. Non-stop routing designs use one or more backup route controllers to maintain the routing tables and support connections with surrounding routers. They also have the capability to perform 'in service' software upgrades, whereby a network operator loads a new software image onto a backup route controller while the primary continues to operate. The backup is then brought into service and the primary is kept available as a standby in case a problem should arise with the new software. Once the new software has been proven the original software can be upgraded. Seamless software upgrades eliminate router downtime and are essential to delivering high availability.

Recommendation 23: Understand how router reliability is addressed by your service provider in migrating to a converged network.

One of the benefits of converged networks is that providers can use the same core network and access network for providing both public and private network services. A converged network is able to distinguish between different classes of service and offers resilience mechanisms that are appropriate to each class, which may differ in the core network and the access networks due to their different physical and topological natures. Service providers will therefore be able to offer different levels of resilience for public services, from within the same access and core network infrastructure.

6.4. Core Network Considerations

The core network is the service provider domain. In the converged network core, IP networks with IETF⁸ standard Multi Protocol Label Switching (IP/MPLS) technology is becoming widely preferred by network providers because it is a key technology for the delivery of virtual private networks (VPNs) and Ethernet services due to its traffic engineering features. An IP/MPLS network normally operates over either Synchronous Digital Hierarchy (SDH) or Dense Wavelength Division Multiplex (DWDM) transmission infrastructure.

Core network architecture is very proprietary, although generally standards based. Each service provider will design and build their own to meet the specific

⁸ Internet Engineering Task Force.

marketplace and business case. Customers should engage their provider to understand the architecture and its features.

Recommendation 24: Discuss the architecture of the network, from end to end, with your provider and understand the features that affect your services.

6.4.1. Redundant Capacity

Redundant capacity is an important feature of the core architecture which can be switched in either through protection or restoration processes.

In the protection process spare capacity is dedicated and pre-planned; when a network element fails, live traffic is automatically switched to a known alternative path around the failure. This is the fastest way to restore service and typically takes 10's to 100's of milliseconds.

In the restoration process spare capacity is not pre-planned and, following a failure, a search for any suitable available capacity must be made before the traffic can be switched over. This takes longer to restore service and typically takes 10's of seconds to a few minutes, as time must be allowed for alternative capacity to be found.

Recommendation 25: Ask your provider to explain how redundant capacity is provided and used, and how it affects your services.

6.5. Access Network Considerations

The access network in general provides local terminations to an area exchange or point of presence (POP); they are relatively short links and their characteristics are determined by factors such as location and terrain, distance to closest exchange, data rates required and media available. Cabled systems continue to be vulnerable to damage by civil works and extremes of weather.

Public service access connections (whether for voice or broadband, fixed or mobile) normally rely on a single connection back to the core network. Resilient access has been available in the past to the public as a business service.

Access links to critical installations may require separate access routing to achieve the highest possible level of resilience. However not all access routes connections will require this treatment and the decision about which routes to select for highest performance will be indicated following a proper risk assessment.

Recommendation 26: For critical installations, or those housing critical systems, use separate access routes.

Converged access networks are implemented using a variety of technologies. The majority of fixed broadband access systems today are based on copper cables, using either copper pairs (telecommunications) or coaxial cable (cable TV). Services offered over coaxial and copper cables can provide a broadband service, and even higher bandwidth or longer range access connections can be delivered using optical fibre.

In the fixed access network, NGN generally refers to any new technology that can provide higher speed digital packet access. Converged network broadband services can be delivered via Digital Subscriber Line (DSL) technologies over copper pairs or via cable modems over coaxial cable. Point to point fibre is used to deliver 100 Mb/s

and 1 Gb/s Ethernet services. Passive optical networks (PONs) and later versions of radio access systems are also being developed to provide converged network access services.

The mobile or radio access network is also migrating towards a high speed, IP-based infrastructure which will allow mobile telephony networks to deliver voice, data and multimedia services. Improvements in the air interface standards for mobile telephony, such as GPRS and UMTS, are extending the available capacity or bandwidth of mobile services. These changes represent the mobile industry moves towards a converged network environment.

An improvement in service availability in the access network may be achieved in converged networks by using a back up service that uses a separate access infrastructure, for example by having both a fixed and mobile voice service, or a fixed broadband line and a 3G service. However it is important to recognise that even this strategy may fail in a localised emergency situation such as widespread flooding.

There is an increasing trend towards home working, requiring high bandwidth remote access usually using a VPN. Home working can involve access to common files and applications, collaborative working at the enterprise level such as product development, and supply chain management, uses more demanding than the typical domestic use of broadband access. As domestic use of broadband grows and contention rates have more effect, consideration should be given to the procurement of guaranteed bandwidth and QoS in the access element.

Recommendation 27: For critical home workers consider the procurement of guaranteed bandwidth and quality of service; do not leave it until the last minute to order additional services for home workers.

6.6. Third party access to corporate networks

CPNI has produced a number of papers to present good practice guidance on the use of third party providers, and ways of protecting the network from abuse of privilege. It is widely considered that there are very limited technical steps available to control and manage third party access, and that the majority of mitigating actions involve tighter business and personnel processes. Contractual action, in particular, may be one of the most effective tools but it is recognised that many business arrangements are long-standing and may be costly to renegotiate. The standard set of clauses used in contracts today probably represents about 80 – 90% of the requirement to address the risks in the global market. Additional work is required by both parties to a supply contract to reduce the risk further. The Office of Government Commerce (OGC) has developed a set of Procurement Guidelines⁹ which, although targeted at government agencies, are useful to private sector organisations and give service providers direction on what makes an attractive product for discriminating buyers.

The OGC guidelines identify key points that should be considered in procuring new network services and provide a choice of control statements that could be optionally used in procurement contracts.

⁹ OGC Good Practice Guide: Next Generation Networks and the Procurement of Services Version 1.

Recommendation 28: Ensure that control statements are used at the contractual stage to reduce any risks from inappropriate access by third party suppliers.

Finally:

Recommendation 29: Recognise that high levels of availability, and highly resilient services, will cost more than standard services, and do not use cost as the main criterion when procuring these services.

and

Recommendation 30: Ensure that the corporate experts in Procurement, Business Continuity and Security are all working together with the service providers to deliver the good practices described in Recommendations 1 – 29.

7. Summary of Recommendations

The previous sections outlined 30 recommendations for a customer of resilient telecommunications services to consider, which are summarised below:

Recommendation 1: Identify those applications and services that are deemed mission critical and which carry a high risk to the business if the telecommunication services they depend upon are disrupted.

Recommendation 2: Wherever possible separate out the high risk services from those that only carry a medium or low risk to the business if disrupted.

Recommendation 3: Discuss your requirements for availability of the services you have identified with your service provider and ensure that you are content with the availability provided.

Recommendation 4: Associate the high-risk (to the business) applications with the services they are provided over.

Recommendation 5: Analyse the threats and vulnerabilities to the mission critical high risk services – e.g. natural disaster, malicious attack, single point of failure, commercial dependency, any lack of transparency in how they are delivered.

Recommendation 6: Conduct a self-assessment to understand the extent of your risk exposure due to any shortcomings in the resilience of the telecommunications services in use.

Recommendation 7: Look carefully at the cost/benefit of ‘sub PSTN’ services in relation to the reduced quality of service and challenge the provider to explain what, if any, resilience is being offered.

Recommendation 8: Ask your provider how much of the network path for your service is automatically protected and, if there was a converged network equipment or cable failure, how long it would take to restore service.

Recommendation 9: Work with your provider to understand the physical routes taken by the systems supporting your critical services.

Recommendation 10: If the risk exposure to a single point of failure is not acceptable, then consider using end to end separation of all components, including separate building entry points, risers, ducts, exchanges and core network routes;

Recommendation 11: Use components and services with inherent resilience; for example ask for a protected service rather than a standard unprotected service.

Recommendation 12: Use service provider who can offer true separacy for applications requiring the highest levels of availability.

Recommendation 13: Use a single provider for single end to end separacy and diversity services and do not rely on dual providers to guarantee separation;

Recommendation 14: Invest more time and effort into building relationships with a single supplier, for example by sharing testing and assurance activities;

Recommendation 15: Make allowance in the contract or SLA for transparency of the service provision, including separacy and diversity, both at the time of provision and through the life of the contract.

Recommendation 16: Understanding your provider's migration strategy to converged networks and agree the migration issues to jointly be reviewed and actioned.

Recommendation 17: If the risk associated with a dependency on a single provider for specific services is not acceptable, then consider the use of more than one provider for each critical service but take steps to ensure that there are no common points or single points of failure.

Recommendation 18: Identify those personnel in your company who are able to request or authorise changes to the service configuration, and give your Network Provider a pre-authorized list of names.

Recommendation 19: If broadband access is critical to your business applications in an evacuation scenario then consideration should be given to providing dedicated bandwidth capabilities for key personnel or locations.

Recommendation 20: Scale your remote access servers to be able to cope with those numbers of members of staff you need to have access in the case of an evacuation or a pandemic situation.

Recommendation 21: Recognise that the load on your broadband network will increase with time and ask your provider how he guarantees that service performance for both voice and data will not fall below the agreed limits.

Recommendation 22: Any organisations with remote assets that require control or supervisory communications, and particularly systems that have been used for some time, should discuss their requirements with their service provider in some detail.

Recommendation 23: Understand how router reliability is addressed by your service provider in migrating to a converged network.

Recommendation 24: Discuss the architecture of the network, from end to end, with your provider and understand the features that affect your services.

Recommendation 25: Ask your provider to explain how redundant capacity is provided and used, and how it affects your services.

Recommendation 26: For critical installations, or those housing critical systems, use separate access routes.

Recommendation 27: For critical home workers consider the procurement of guaranteed bandwidth and quality of service; do not leave it until the last minute to order additional services for home workers.

Recommendation 28: Ensure that control statements are used at the contractual stage to reduce any risks from inappropriate access by third party suppliers.

Recommendation 29: Recognise that high levels of availability, and highly resilient services, will cost more than standard services, and do not use cost as the main criterion when procuring these services.

Recommendation 30: Ensure that the corporate experts in Procurement, Business Continuity and Security are all working together with the service providers to deliver the good practices described in Recommendations 1 – 29.

Glossary

This Glossary aims to bridge the gap between the customer language and the telecommunications provider language.

This Glossary is not exhaustive and has been kept relatively short by focussing on the most commonly used terms. The reader can follow the Bibliography links at the end of this section if the term they seek has not been included.

Term	Description
ADSL Asymmetric Digital Subscriber Line	A digital technology that allows the use of a copper line to send a large quantity of data in one direction and a lesser quantity in the other.
Customer	This is the generic term used within the Guide to describe the organisation who procures the telecommunications networks and services from the provider. It is synonymous with other terms such as Client, Subscriber and Account. See: Provider
Diverse Routing	The routing of information using network components that can automatically provide alternative routes to avoid congestion or network failure
Diversity	Diversity ensures that specified circuits are not routed over the same cables or transmission systems. However there may be some common network nodes within the circuit routings. Diversity describes the ability to use, select or switch between different routes to avoid congestion or network failure.
Dense Wavelength Division Multiplexing	DWDM uses a technique to carry multiple signals together as separate wavelengths (colours) of light in a multiplexed signal. DWDM is a variation of Wavelength Division Multiplex (WDM) but with much higher bandwidth and density. Using DWDM, up to 80 (and theoretically more) separate wavelengths or channels of data can be multiplexed into a single optical fibre, providing huge line capacity. Another important feature of the DWDM system is that different data formats at different data rates can be transmitted together. For example, Internet (IP) data, SDH and asynchronous transfer mode (ATM) data can all be carried at the same time within the optical fibre. DWDM is a crucial component in today's optical network and widely deployed by Service Providers in their backbone network.
IP	Internet Protocol; the most commonly used network protocol

IP VPN	<p>Recent developments in Internet Protocol (IP) capability have led to the protocol competing with Frame Relay and ATM as the preferred platform for Virtual Private Networks (VPNs). Quality of Service (QoS) guarantees can now be specified for IP, meaning that the transport of time-sensitive traffic like video and voice is viable.</p> <p>IP VPN (with QoS) typically uses MPLS in private IP networks to route traffic to its destination. The packets of data are routed according to decisions made by the network switching equipment on a per packet basis. Originally, all packets were treated equally, with the result that data would take random paths across the network to its destination. While this was fine for e-mail or web-browsing data, it was not suitable for traffic requiring consistent transmission quality.</p> <p>Different operators will implement IP-VPNs in different ways, (not always interoperable) resulting in a variety of performance to choose from. Key parameters used to measure an IP-VPN are end-to-end latency, packet loss, jitter and availability, with typical availability figures of between 99.7% and 99.9% being quoted by operators.</p>
Multi-Protocol Label Switching	<p>MPLS describes network architecture for fast packet switching and routing and provides the designation, routing, forwarding and switching of traffic flows through the network. More specifically, it has mechanisms to manage traffic flows of various granularities. It is independent of the layer 2 and layer 3 protocols, such as ATM and IP. MPLS is increasingly used as the protocol of choice for the core network.</p>
NGN	<p>A Next Generation Network is a packet-based network able to provide converged services including Telecommunications 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 services. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.</p>
OSI 7-Layer Model	<p>The International Standards Organisation (ISO) proposed the Open Systems Interconnect (OSI) 7 Layer Model as a Reference Model in the 1970's. It is covered in all networking texts and will only be outlined here.</p> <p>All components of the model are implemented as a number of layers. Each layer performs a well-defined function and</p>

	operates to a defined protocol by exchanging messages with a corresponding peer layer in a remote system. Each layer has a well-defined interface between itself and the layers above and below. Each layer provides a set of services to the layer above, and uses the services of the layer below. Thus, a transport layer protocol such as the Transport Control Protocol (TCP) uses the services of a network layer protocol such as the Internet Protocol (IP), which in turn uses the services of a data link protocol such as ATM, to communicate over the physical medium to its peer transport layer in the remote host.
Packet Service	A service involving the transmission of data in the form of discrete blocks (cells, frames, packets) of information and, if necessary, the assembly and disassembly of data in this form.
Provider	This is a generic term used within the Guide to describe the organisation which provisions and operates the telecommunications network infrastructure and related services. It is synonymous with other terms such as Supplier, Operator, Service Provider and Network Provider.
PSTN	Public Switched Telephony Network
QoS	Quality of Service; defines the efficiency of the passage of data across a link or network
Redundancy	Back-up systems duplicating functionality of the systems are available to take over in the event of component or system failure.
Resilience	The equipment and architecture used are inherently reliable, secured against obvious external threats and capable of withstanding some degree of damage.
Restoration	The capabilities are in place to replace a failed system with a working one.
Separacy	Ensures that specified circuits are physically separated throughout the network so that there are no common exchanges, interconnection points or cable routes. Physical and logical separation of a circuit or system from Source to Destination
Single Point of Failure	The only (single) source of a service, activity and/or process i.e. there is no alternative, whose failure would lead to the total failure of an activity and/or dependency.
SLA	Service Level Agreement; A formal agreement between a service provider and their customer, which covers the nature,

	quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster. It should also cover service level guarantees.
Synchronous Digital Hierarchy	<p>Synchronous Digital Hierarchy (SDH) and the Synchronous Optical Network (SONET) are a set of related standards for synchronous data transmission over fibre optic networks that are often used for framing and synchronization at the physical layer. SONET is the United States version of the standard published by the American National Standards Institute (ANSI). SDH is the international version of the standard published by the International Telecommunications Union (ITU).</p> <p>SDH is a fibre centric technology and is commonly configured in resilient ring architecture, so that if any network failure occurs, service is automatically re-routed along an alternative path. The Network Terminating Equipment at customer premises would normally be connected back to independent network nodes by completely separate fibre paths, routed along different ducts, and fed into the customers' premises at separate entry points. This ring architecture provides a high level of availability.</p> <p>SDH is also used as a point-to-point service in many applications, and customers wishing to take advantage of the resilience of ring architectures should qualify this with the provider.</p>
Virtual Private Network	IP VPN above

Acknowledgements

CPNI would like to acknowledge the contribution made to the development of this Guide by members of the following industry groups:

NSIE and EC-RRG

And by CESG and the Cabinet office

Annex 1 - Self Assessment Questionnaire

32 Questions to ask your own organisation.

This Self Assessment Questionnaire has been produced by CPNI in conjunction with a number of telecommunications providers to facilitate discussions between the customer and the provider(s) on the resilience of Telecommunications Services as part of a risk assessment exercise. It recognizes that different providers may supply different services to a customer, for example data services from one provider, voice services from another. In addition, some Customers will have entered into a dual-provider relationship (similar services provided by more than one provider) in an effort to guarantee resilience and availability against the possibility of failure. In the event that more than one provider is used, this questionnaire can be used to provoke discussion of how the providers co-operate to minimize and mitigate risk.

Services

This section is intended to provoke consideration of the different telecommunications services used by your organization. Continuity of operation of a business will typically be dependent on the availability of these business critical services.

Q1 Can you identify business critical services in order of importance or criticality (high, mission critical; medium; low)?

Q2 Do you have a full and complete list of your business-critical telecommunications services, and the systems that support them?

Q3 Can you identify the telecommunications services that support your critical systems?

As a minimum, you should be able to uniquely identify each telecommunications service, circuit or trunk by a short title e.g. TRUNK1, and a circuit reference such as KX654321. When you need urgent action regarding this service, it is important that you are both talking about the same thing.

Q4 Can your organisation and your provider agree on a unique identifier for each critical service or circuit?

Network Routing

This section is intended to provoke consideration of how your business critical services are connected into the wider infrastructure.

Q5 Are you aware of where in the provider's core network your network services connect, how they are connected and the physical routings they take once they leave your premises?

The last-mile connectivity between your premises and the outer edge of your provider's network is often the most difficult link to provide resilience for.

Q6 If you are using dual providers, are you confident that there are no physical routings or points of failure common to both providers?

Dependencies

This section is intended to provoke consideration of other components within both your and the provider's core network that are vital to the supply of your services.

Q7 Within your own premises, do you have visibility of your telecommunications services all the way into the provider's duct?

Q8 Are any parts of the cabling, for example, exposed to external contractors or others beyond your control?

Q9 Who has responsibility for the safety and security of the areas identified in Q8?

Q10 Are there any third party components, such as ADSL Routers, which may fall between areas of responsibility?

Diversity

This section is intended to provoke consideration of single points of failure, whereby loss of a single (network) component will affect multiple critical services.

Q11 Do all of your services leave your premises in the same cable?

Q12 Are they all in the same duct?

Q13 Do your multiple providers share a duct system?

Consideration should also be given to whether different premises belonging to your organisation are connected to common points within the provider's network.

Separation

This section is intended to provoke consideration of how different critical services are routed outside of your premises and through the provider's network.

Q14 Do you know if critical services are routed via different network components so that a failure of one component will not affect all critical services?

Q15 Have you specifically asked for this service?

New Services

It should not be assumed that using two providers will guarantee separation. It is common practice within the Telecommunications industry for local access circuits (between the core network and customer premises) to be provided by a third party (BT, for example). In this case, it is possible that circuits supplied by different providers have a common routing.

Q16 When you order new services, do you discuss your existing services to ensure there are no unjustified assumptions made about separacy or diversity?

Q17 Do you review existing requirements to prevent duplication or compromise?

Changes to Network Structure

This section is intended to provoke consideration of how your providers manage changes to their network infrastructure. It should not be assumed that a provider's network is static. Changes are continually taking place, whether temporary (due to planned engineering work) or permanent (network restructuring including the introduction of new network components and the removal of old ones). Over time, services that were diverse or separate could be compromised by these changes, although it should be noted that providers would normally track these changes to ensure diversity/separacy where contracted to do so.

Q18 Do you regularly review your specific resilience requirements with your provider?

Q19 Do you receive notification from your provider regarding network updates, proposed engineering downtime or other changes to the status quo?

Power

Loss of power at a site, whether at your premises or within the provider's network, is a significant threat to the continuity of the telecommunications service.

Q20 Do you provide standby power on your own premises?

Q21 Do you test it regularly?

Q22 Do you have visibility of your provider's emergency power provision and the consequences of a power failure on your Services?

Contact in a Crisis

This section is intended to provoke consideration of how you will contact your service provider(s) in the event of a catastrophic impact to the UK telecommunications network.

Q23 Do you have primary and alternate methods for contacting your provider (e.g. telephone, e-mail?).

Q24 Have you supplied your provider with alternative contact details for your own response teams?

Q25 Have you discussed your respective emergency plans with your provider?

Q26 What regular updates would you expect your provider to provide in the event of an incident occurring?

Q27 Have you asked for regular updates or to be contacted in an emergency? Is your requirements for a specific response by your provider covered in your SLA or contract?

Homeworking

Do not assume that because many of your employees have high speed broadband at home they will be able to work effectively in the case of a pandemic situation or a long term mass evacuation.

Q28 Do you know what percentage of the critical business applications are used by home workers?

Q29 Do the homeworkers use domestic or residential broadband, or 'enterprise scale' connectivity, to the office systems?

Q30 Have you assessed the bandwidth requirements to maintain the business in the event of an evacuation of the main office?

Q31 Is there a point at which capacity or response time will drop below acceptable levels and do you know what it is?

Q32 Has your corporate remote access server facility been scaled to accept simultaneous connection requests from key workers in an evacuation situation?

Annex 2 – Twenty Questions to ask your Provider

The following questions have been extracted from the observations described elsewhere in this Guide. As such they are not comprehensive in terms of addressing all issues associated with resilience, but they do address the issues that are relevant to the focus of this Guide. The questions also focus on the provision of new services in the same way that the self-assessment questions in Annex 1 help with understanding the current environment.

Are Standard Services Good Enough?

Q1 What contingency plans do you have in place which supports the Ofcom ‘National Emergency Plan for the UK Telecommunications Sector’, how do you test them and what are the results?

Q2 What standards and best practice guidance do you conform to for security and availability?

Providing Assurance

Q3 Are you prepared to help our organisation to understand the complexities of your network and work together to provide suitable resilient solutions, and if so how will you do this?

Q4 What resources are you prepared to commit to our relationship, and how much of this resource will have detailed technical knowledge?

Q5 Do you have a process where we could work together on business continuity planning and disaster recovery, including testing to provide assurance?

Customers are responsible for their own Business Continuity and Disaster Recovery planning; this is a service offered by many providers and detailed consultation may not always be free of charge.

Q6 As a provider of a separacy/diversity service, how will you ensure that they will remain separate or diverse throughout the period of the contract?

Q7 How will the security and integrity of your services be maintained during maintenance activities?

Contracts and Due Diligence

Q8 Are you prepared to build the right to transparency into the contract and SLA and what form would this take?

Q9 How can you demonstrate that you have full control and visibility of the network assets needed to provide end-to-end separation?

Q10 How can you demonstrate that you have appropriate contingency plans in place, and that they are successfully tested on a regular basis?

Availability Measures

Q11 How do you calculate Availability figures and how do you take account of major disruptive events in their calculation?

Q12 How do you determine your limits of liability associated with Availability guarantees, and what are they?

Understanding the Threats

Q13 How do you assess the physical threats against your network assets and how do you mitigate the risk against them?

Q14 If you make use of wholesale network services, how do you work with the wholesaler to ensure you can deliver a resilient service?

Providing the Right Solutions

Q15 Do you have a process which captures a view of the current services you provide to my organisation, and correlates them with any new requirement, to make sure that duplication and single points of failure can be avoided?

Q16 How do you provide separacy and diversity services in relation to all the key elements: Risers, Building entry points, last mile ducts & manholes, Local exchange, and network route and how do you identify any potential single points of failure?

Q17 How do you ensure the resilience of international services?

Q18 What network components would you use for best practice separacy services and what is their inherent resilience?

Q19 What are your Power back-up, and restoration, contingency plans;

Q20 How are your contingency plans tested and what are the results?