Good Practice Guide

Telecommunications Resilience

DISCLAIMER

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

NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Good Practice Guide To Telecommunications Resilience

NISCC 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.

Document History	Version	Date of Issue
Original	V1.0	10 May 2004
OFCOM Withdrawal of Essential Requirements Guidelines	V2.0	30 March 2006

National Infrastructure Security Co-ordination Centre (NISCC)

Aim

The National Infrastructure Security Co-ordination Centre (NISCC) was established by the Home Secretary to promote the protection of the UK's Critical National Infrastructure from electronic attack, and to report on the level of protection in place. For further information on NISCC please see www.niscc.gov.uk

Good Practice Guidance

When NISCC was created in 1999, the production and promotion of good practice guidance was specifically included in its remit. The NISCC Good Practice Guide to Telecommunications Resilience makes a number of recommendations for the provision of resilient telecommunications networks, which we hope will thereby increase the resilience of the CNI as a whole.

The Critical National Infrastructure

The Critical National Infrastructure (CNI) is defined as "those parts of the UK's Infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic or other grave social consequences for the community, or any significant portion of the community, or would otherwise be of immediate concern to the Government".

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

It is vital that an organisation understands which of its telecommunications systems are critical to the business, and how to provide the appropriate level of resilience for these systems.

In this Guide, NISCC has provided a series of recommendations aimed at helping an organisation understand why resilience is an issue, what resilience is needed and how it can be delivered.

Key recommendations are:

- Identify those communications systems that are deemed mission critical and which carry a high risk to the business if they are disrupted.

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

- Understand the architectural options for separacy and diversity based services e.g. what does 'end to end separacy' actually mean.

- Recognise that high availability and high resilience services will cost more than standard services, and do not use cost as the main criterion when procuring these services.

The simple message delivered in this Guide is:

- **Know your communications system requirements**

- **Talk to your Provider**

- **Focus on the Services required, not the technology**

- **Provide the required level of resilience**

- **Expect to pay for it**

1 INTRODUCTION

The dependability of the telecommunications infrastructure is vital to the well being of most organisations. However, 100% guaranteed telecommunications resilience will never be possible. Each organisation must therefore balance the risks to their business from a telecommunications failure with the cost of providing enhanced resilience.

The impact of the loss of critical telecommunications services on an organisation is the same regardless of the cause of the disruption. It is therefore vitally important for organisations to take appropriate measures to ensure that their telecommunications systems are robust enough to continue to provide the critical services in the face of any disruption.

Best Practice is defined as those measures that can be taken to guarantee resilience, irrespective of cost. Good Practice can therefore be defined as those measures which can be taken to provide a degree of 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.

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, and a set of recommendations written to make the reader a more informed and cognisant Customer.

2 SCOPE OF THE GUIDE

Within this document the title 'Good Practice Guide to Telecommunications Resilience' will be referred to simply as the Guide. The Guide deals with the resilience of Telecommunications Services, referred to as 'Services'.

The scope of the Guide is the resilience of telecommunications networks that carry voice and data services over the fixed and mobile (wireless) infrastructure in both the public and private circuit domains. It does not address the customers' own networks and systems within their physical perimeter.

2.1 Aims of the Guide

The *aims* of the Guide are to raise awareness of the need for Telecommunications Resilience 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 is those people who have to commission, specify, audit or procure resilient Services. 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

The *approach* adopted within the Guide is based on providing a choice. This choice is based on an understanding of the risk exposure: 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/line plant 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 has been created in consultation with CNI Customers and Telecommunication Providers and is designed to describe why resilience is an issue, what resilience is needed and how to ensure effective resilience solutions.

The structure recognises the need to bridge the gap between the Customer's language and requirements, and the Provider's language and capability. A brief description of the technology 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.

3 UNDERSTANDING WHY RESILIENCE IS AN ISSUE

3.1 The UK Environment

The Telecommunications Industry within the UK is regulated by the Office of Communications, OFCOM, (previously known as Oftel, the Office of Telecommunications). As part of the licensing regime, Oftel required that Communications (or Service) Providers followed a number of Guidelines. The 'Essential Requirements Guidelines[1]' were particularly relevant to the resilience of the UK public networks. Following consultation, OFCOM withdrew the Guidelines in the Regulation of VoIP Services Statement on 22 February 2006. A revised set of guidelines, the TI-EPF[2] Resilience Guidelines[3], has been developed by the TI-EPF as a voluntary code of practice. Additionally, major Communications Providers had co-operated with Oftel in the creation of a National Emergency Plan for the UK

---

[1] OFCOM 'Guidelines on the Essential Requirements for network security and integrity' http://www.ofcom.org.uk

[2] TI-EPF: Telecommunications Industry Emergency Planning Forum

[3] TI-EPF Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure (short title 'TI-EPF Resilience Guidelines')

Telecommunications Sector, which is also described on the OFCOM web-site (http://ofcom.org.uk). This plan, and the Forum that maintains and operates it, the TI-EPF, is now sponsored by CSIA[4]. The plan is designed to help maintain the telecommunications infrastructure in emergency situations. These measures have raised the level of resilience in the telecommunications services provided as standard by UK Providers. 'Standard Service' is a non-technical term for the basic telecommunications services, such as the PSTN[5], routinely provided in UK today. These are typically available 99.999% of the time, but see Section 5 for a more detailed description of availability.

However, in the event of a failure of the standard service, the response and restoration of services, even under the National Emergency Plan, is a standard response. Basic services are restored as quickly as possible and in a way that brings the greatest relief to the mass of users. The term 'Standard Services' implies no customer priorities.

One of the principal areas of concern is the route congestion between customer premises and local exchange or Point of Presence (POP). This is of particular concern in built up or high-density areas such as the City of London, and is often a classic example of a single point of failure. Due to the historical position of BT as the incumbent telecommunications Provider before privatisation, the 'local loop' or last mile in the majority of cases is a BT asset. Local Loop Unbundling (LLU) obliges BT to allow other Providers use of these assets, resulting in third party Providers selling circuits over the same cable routes as BT. As there is no requirement for either Provider to discuss the use of these circuits with the other, they may be unaware that the customer possibly intended the circuits to be separated. In this way the customer may be lulled into a false sense of security. True separation, or separacy as it is known, in this example would have been possible by asking one Provider for two separate circuits. It is worth noting here that buying two similar circuits from the same Provider may actually be more economical than buying one circuit each from two Providers. This in turn, however, raises concern over the dependency on a single provider. Section 5 includes a description separacy and discusses single-provider dependency.

3.2   Lessons Learned from the US Experience

The attack on the World Trade Centre on 11 September 2001 provides a learning opportunity. In particular, the 'Lower Manhattan Telecom Users' Working Group' issued a report in August 2002[6], outlining their findings and recommendations for building a 21st Century Telecom Infrastructure. Some of these findings are relevant to the UK environment, and the Manhattan report is highly recommended as further reading for any CNI organisation wishing to build a good understanding of the threats and vulnerabilities associated with resilience.

The following findings in particular are relevant:

---

[4] CSIA: Central Sponsor for Information Assurance (a division of the Cabinet Office)
[5] PSTN: Public Switched Telephony Network, the standard UK telephone service
[6] Building a 21st Century Telecom Infrastructure – Lower Manhattan Telecommunications User's Working Group Findings and Recommendations, August 2002. - www.downtownny.com/files/TelecomReport.pdf

- "Communications outages after the attacks were a result of an under-appreciation of potential failure points rather than a deficient infrastructure". The infrastructure in and around the World Trade Centre was comprehensive and many organisations had back-up systems in place. The communications outages were caused by the massive loss of concentration points to an extent that disaster planners had been unable to visualise.

- "Local exchange redundancy was not offered as a standard service". Unlike UK, standard services in the US do not provide Local Exchange redundancy and so the loss of a local exchange resulted in the loss of all associated services.

- "Carrier redundancy does not necessarily mean true redundancy". Organisations had purchased services from multiple 'carriers' or providers, but many of these services had simply been bought from the same provider and resold. As a result many back-up systems were provided over the same cable as the main systems.

- "The 'last mile' (between local exchange and customer premises) is the key to the resilience of a business telecommunications network". The provider's network has a high level of built in resilience resulting in few failures. The last mile connection to the customer however is usually a single point of failure, often because there is simply no alternative route. It is also the most exposed part of the network to external interference or disruption. Any company with more than one route into the Provider's network has more than doubled its survivability.

- "Property owners and building landlords play a key role in providing telecommunications reliability". In shared accommodation such as a multi-story office block, the landlord has the opportunity to provide alternate or diverse cable routes, power supplies and access points for the tenant companies, which can in turn help the telecommunications providers to provide multiple routes.

- The US telecommunications providers agreed that the majority of the recommendations of the Report could be implemented as part of a service. They felt however that multiple entrances in buildings and multiple carrier-neutral risers in buildings were beyond their remit and should be provided by the owners of buildings.

4 DECIDING WHAT RESILIENCE IS NEEDED

4.1 Mission Critical Systems

Systems are described as 'mission critical' if the loss of the system would cause the primary aim of the Company to fail.

4.2 Risk Assessment

It is important to recognise that in any organisation, not every communications link, system or circuit needs 100% availability. Customers will know that their systems range from non-essential leisure and administrative to mission critical systems. In general the majority of systems such as telephones, facsimile (fax) and most e-mail services can tolerate some downtime, because they are either not systems which require immediate response or are not mission critical. 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. It is not unusual to find the 80/20 rule at work, where 20% of the systems require 80% of the resource.

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

> **Recommendation 1:** Understand the types of resilience-based risks associated with your Services.

> **Recommendation 2:** Identify those communications systems that are deemed mission critical and which carry a high risk to the business if they are disrupted.

Where possible, associate the high-risk applications with the Services they are provided over. 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 Virtual Private Network (VPN), which, with Quality of Service (QoS)[7], 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 3:** Wherever possible separate out the high risk services from those that only carry a medium or low risk to the business if disrupted.

> **Recommendation 4:** Analyse the threats and vulnerabilities to the mission critical high risk services – eg natural disaster, malicious attack, single point of failure, commercial dependency, lack of transparency.

The main threats/vulnerabilities described in the previous section relate to single points of failure and the lack of transparency of these single points of failure. This section focuses on what the reader can do to counter these threats/vulnerabilities, based on an assessment of the risk, and makes appropriate recommendations, summarised in section 7.

In reality, many risk assessments will fall somewhere between mission critical and low risk. This is recognised by describing 'Best Practice' in addressing the threats/vulnerabilities outlined and leaving 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 be defining their own good practice.

---

[7] VPN; QoS: see Glossary

4.3 Self Assessment Questionnaire

The 'Self Assessment Questionnaire' in Annex 1 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 as part of a risk assessment exercise. It recognizes that different Providers may supply different services, for example data services from one Provider, voice services from another. This questionnaire has been designed to provoke analysis and discussion in order to provide input to a risk assessment.

> **Recommendation 5:** Conduct a self-assessment to understand your risk exposure.

4.4 Availability Definition

It is common practice in the Telecommunications industry to refer to system availability, or reliability, in terms of a percentage of the overall time. This is easier to understand, and most widely quoted, using the inverse concept of total unavailability, so that 90% availability equates to 10% unavailability, which in turn equates to 36.5 days lost in a year. A comparison of typically used figures is shown in Table 1 below.

Table 1: Comparison of System Availability Data

Serial	Percentage Quoted	Unavailability (Not usually quoted)	System Unavailability	Typical Example
1	90%	10%	36.5 days/year	Mail server
2	99%	1%	3.65 days/year	Web server
3	99.9%	0.1%	8.8 hours/year	A good ISP
4	99.99%	0.01%	53 minutes/year	GPS
5	99.999%	0.001%	5 minutes/year	UK PSTN
6	99.9999%	0.0001%	32 seconds/year	

Some Providers will quote an availability figure equal to so many faults in a given period, eg one fault in ten years. This is not particularly useful unless it is accompanied by a detailed breakdown of the network components and their reliability data.

4.5 Services judged to be medium or low risk

As mentioned in the previous section, it is widely recognised that the PSTN infrastructure is one of the most reliable infrastructures in the world, with examples of Services being quoted as having '*five 9's availability*' (99.999%).

Service Providers will often quote end-to-end availability figures, e.g. for an Asynchronous Transfer Mode (ATM)[8] service this is typically 99.9%. This is significantly less than the five 9's but is understandable given the complex technology and the dependence on local connectivity. For low/medium risk applications these levels of availability could be acceptable from a cost/benefit perspective.

It is apparent that the marketing statements on some Providers' websites are written at a high level to encourage the reader to contact the Provider for more advice. It is important to make this contact but resilience is a complex subject that relies on a good understanding of the architectural and component issues, so it is important that both parties in these discussions use the same terminology and have a similar technical background.

> **Recommendation 6:** Challenge the Provider to explain the marketing statements made on resilience and availability and ensure that you are talking to the right Provider representative.

It should be noted however that the accuracy of published availability figures might be subject to some anomalies in the market place. Discussions with the Provider will help to clarify many of the Service Level Agreement (SLA) issues and definitions, but it is likely that if resilience higher than that of standard services is needed, then this will come at a cost.

An alternative to Providers' sales and marketing figures is to look at statistics produced under the observation of independent parties, e.g. the OFCOM 'Quality of Service' reporting scheme[9].

These considerations should all help customers determine if standard Services offer sufficient resilience for those applications deemed to be medium or low risk to the business. However, it should be recognised that most of these published figures relate to threats from natural disasters or equipment and process failures. They do not reflect the consequences from incidents such as the attack of September 11. If standard Services offer sufficient resilience, then these will be the lowest cost solutions. If they do not, then the applications in question should be elevated to high risk and dealt with as described in the next section.

> **Recommendation 7:** Understand what your Provider(s) do to meet the TI-EPF Resilience Guidelines, described in Section 3, and form a judgement as to whether these satisfy your requirements. If not, then adjust the risk assessment as appropriate.

4.6   Services judged to be mission critical and high risk

If an application or Service is 'mission critical', then justifying a high cost to ensure it is resilient is going to be easier than if it is not mission critical. The remainder of this

---

[8], not Automatic Teller Machine – see Glossary
[9] The Mobile Networks Call Success Rate Survey (http://www.ofcom.org.uk) and Fixed Operators Comparable Performance Indicators (http://cpi.org.uk)

section looks at Best Practice and focuses on addressing the threats relating to single points of failure, transparency and provider dependency

4.7   Single Point of Failure

The concerns of the previous section relate to the physical threat of disruption caused by a single point of failure, for example a cable damaged, or an exchange disabled. A dispersed system such as a management system is not considered to be a single point of failure. To mitigate the risk against a single point of failure the solution is to provide separate or diverse infrastructure elements.

In the context of this Guide, *separacy* describes the physical separation of specific circuits so that there are no common exchanges, interconnection points or cable routes. Diversity provides alternative routes and connectivity in the event of congestion or failure.

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.

Analysis of Providers' service offerings relating to separacy and diversity refer mainly to the provision of physical, fixed private circuits and therefore their routes and network utilisation are determinate, which makes the concept of separation easier to visualise than logical or switched Services. Packet based Private Virtual Circuits (PVCs), such as those provided by ATM services, have built in separation, but they are less deterministic and make the visualisation of separacy more difficult.

Resilience can be further improved by choosing components that have inherent resilience because of their design. Synchronous Digital Hierarchy (SDH), which, when used in a ring architecture with automatic changeover, can provide continuity in the event of one part of the ring being broken. Plesiochronous Digital Hierarchy (PDH) technology on the other hand, tends to be used as a point-to-point technology and can be used in a ring with manual changeover or stand-alone changeover switches. See Glossary for more technical details.

The current move towards convergence in telecommunications has fixed and mobile technologies, and voice and data services, moving towards common platforms. Traditionally robust architectures such as the PSTN and X.25 links are moving towards an Internet Protocol (IP) base. This could be seen as a single point of failure situation, but although the typical IP network, for example the public Internet, is a best-effort system with few guarantees of service quality, the IP networks provided by the Service Providers are often closed systems with high Quality of Service guarantees. Maintenance of separate Voice and Data services could reduce the dependence upon any single technology or network component, but at the cost of the resilience, flexibility and end-to-end security of modern developments such as VPNs.

> **Recommendation 8:** If the risk exposure for a single point of failure is not acceptable, then consider:

a.   The use of end to end separation on all components, including separate building entry points, risers, ducts, exchanges and core network routes;

b.   Using components with inherent resilience, for example use an SDH ring rather than point-to-point SDH or PDH.

4.8   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.

Contracts and SLAs should include the right for the Customer to have transparency 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 to help improve the level of their confidence and quality of the assurance.

> **Recommendation 9:** If the risk exposure stemming from the lack of transparency is not acceptable, then consider:
>
> a.   The use of a single Provider for any single end to end separacy and diversity service - do not rely on dual Providers to guarantee separation;
>
> b.   The investment of more time and effort into building relationships with this single supplier, to share testing and assurance activities;
>
> c.   Making 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.

4.9   Dependency on a single Provider

The adoption of a multi-Provider strategy is an obvious one to counter the risk of the Provider going out of business. However, experience shows that the business failure of a Provider does not significantly affect the services to the Customers of these Providers. Their services continue under the management of another Provider or the original company is allowed to continue trading under close supervision. A multi-Provider strategy does not guarantee separacy and resilience. Using a single Provider for end-to-end separacy services clarifies ownership and helps improve assurance as the end-to-end separacy service can include a monitoring capability to ensure that separacy is maintained.

Simply using more than one Provider for each end-to-end separacy service can mitigate the risk of dependency on a single Provider if this is identified as a high risk. This duplication of Providers for two separate and distinct end-to-end separation services has been adopted by at least one CNI organisation.

Recommendation 10: If the risk exposure because of a dependency on a single Provider is not acceptable, then consider the use of more than one single Provider for each separacy and diversity service.

4.10 Due diligence in selecting the Provider

It is assumed all CNI organisations will have their own guidelines for due diligence. In terms of addressing transparency, it is important that the Provider can demonstrate that they have full control and visibility of their network, including any outsourced elements, to ensure they can provide true end-to-end separation. They must also be able to demonstrate that they have effective processes in place to monitor this separation to ensure it is not compromised over time.

The Customer is assumed to have developed sufficient contingency to internally support mission critical operations. The Provider should also be able to demonstrate that they have contingency plans and that they exercise them on a regular basis.

Recommendation 11: Apply rigorous due diligence in selecting the Provider, including assurance that they have visibility and control over the Services they deploy to ensure that separacy and diversity is provided and maintained. Also ensure they have adequate contingency plans in place to recover from a disaster.

5 HOW TO ENSURE EFFECTIVE SOLUTIONS

The good practice requirements and recommendations in the last section focussed on addressing the threats/vulnerabilities related to single points of failure and the lack of transparency of these single points of failure. This section keeps the same focus but describes in more detail how these requirements can be turned into effective solutions using appropriate architectures and resilient components. It is not intended to be a tutorial on telecommunications practices but illustrates some of the issues and attributes of the key technologies that support resilience-based services.

5.1 Architectural Resilience

Many of the issues discussed involve physical network properties. Careful design of the network architecture can provide a substantial increase in the network resilience. As described in the previous sections, the solution will ultimately depend on the cost/risk mitigation assessment as well as the specific physical requirements, and therefore Providers offer different levels of separation providing degrees of resilience to suit the needs and budget of the Customer.

End-to-End Separation Services

As the name implies this type of service offers completely separate routes and network assets from one Customer premises to another. End-to-end separation is only available if the Customer has dual access into their premises. Note that separate Local Exchanges or Dual Parenting are standard service offerings in the UK.
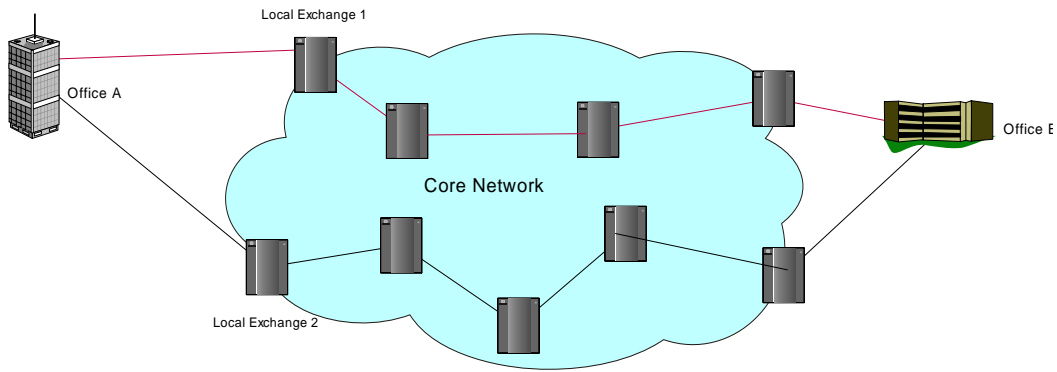
Figure 1: End-to-end separacy

This type of service is deemed Best Practice, but is likely to be the most costly solution.

Main Link Separation Services

As the name implies, main link separation only provides separation between a Local Exchange serving one Customer site, and another Local Exchange serving the other Customer site.
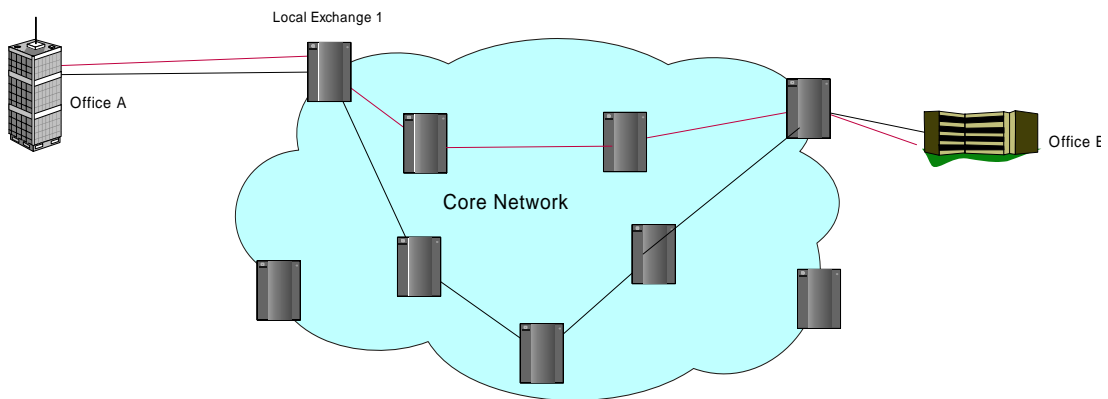

Figure 2: Main Link separacy

Diversity Services

These types of service provide diverse routes but do not guarantee separation in the physical sense, as for example a common exchange could be used in the main link between Local Exchanges, even though the equipment and cables used are different and therefore diverse.
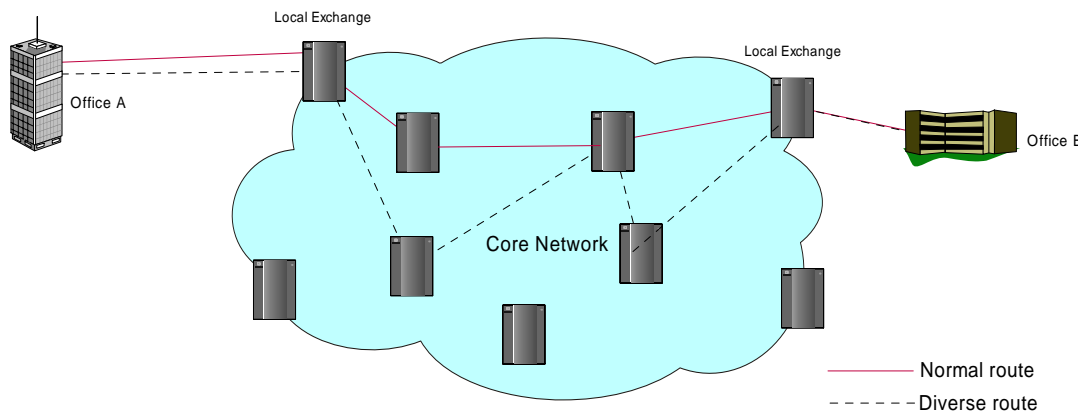
Figure 3: Diverse Routing

Recommendation 12: Understand the architectural options for separacy and diversity based services e.g. what does 'end to end separacy' actually mean.

5.2 Service Resilience

Much of the Architectural Resilience discussed above, and the components described in the Glossary, refer to physical connectivity although a degree of logical resilience is provided by the technology itself. However, there are Services that specifically provide extra resilience.

Intelligent Networks

In Intelligent Networks (IN), the network architecture separates the control, management and customer service information systems from the switching systems. This allows the database and customer service configurations to be updated without interrupting the switch and the switch to be upgraded without affecting customer records. This combination benefits from the independent development of computer and switch technology and subsequently permits enhanced service provision flexibility.

Dual Parenting

Dual Parenting can provide Service Resilience in PSTN systems by giving Customers Primary Rate ISDN or other exchange lines extra protection against network failures. The circuits of a customer are split across a pair of mutually supporting local exchanges, each with a direct connection to the Customer premise. In the event of a problem with a connection or exchange, the other pair provides continuity. **Business Continuity** and **Disaster Recovery** services can be provided to automatically transfer all calls to an alternative site.

Internet Peering and Transit

A large number of CNI organisations own Autonomous Systems (AS) and interconnect or 'peer' with others in various private or public peering arrangements. Networks of roughly similar size exchange traffic as equals and typically money is not exchanged. Large corporates have little difficulty peering privately in mutually agreeable arrangements. Smaller corporate AS may purchase 'Transit' across other,

larger, AS, or peer at public peering points. Systems or networks that interconnect to form the fabric of the public Internet communicate using the Internet Protocols, specifically the Border Gateway Protocol (BGP).

> **Recommendation 13:** When using the Border Gateway Protocol (BGP) for peering, consider using the NISCC BGP Filtering Guidelines[10] as a common baseline.

Some peering arrangements stipulate that AS peer in more than one, and sometimes more than two, different locations. This is predominantly to ensure cost effective and balanced traffic flow. However, from a resilience perspective, it is good practice to peer at 2 or more geographically diverse sites to ensure that connectivity is maintained in the event of a site failure.

> **Recommendation 14**: When peering, consider using 2 or more geographically diverse sites.

Outsourcing

Outsourcing is a growing trend, and is commonly used to relocate web-services, for example, to specialist Service Providers. As with any business process, the Customer is recommended to follow a risk assessment process to capture the risks associated with this. Points that require specific attention include the hosting site itself in terms of disaster recovery:

- Diversity at the site

- Back-up facilities for the site

- Connectivity to the site

- Linkages back to the corporate environment, such as a Data Centre.

Off-Shoring

Off-shoring is another growing trend that offers significant cost benefits but also carries major costs in terms of resilience and security. Issues that should be considered in addition to those above (outsourcing) include the connectivity between the Customer Base and the Customer Service Advisor, typically the public Internet. Consideration should be given to diverse Points of Presence.

5.3   Component Resilience

The components used to provide a Service include various technologies and physical elements. The inherent resilience of different network components can vary greatly, so it is important to understand the characteristics of these components if a Customer aspires to adopt Best Practice. It is also important to recall that the

---

[10] NISCC BGP Filtering Guidelines available on request from NISCC

telecommunications infrastructure adopts a layered approach[11], and each Service may be provided using a mix of technologies. For example, ATM and Frame Relay[12] can run over SDH or PDH, and an IP VPN can run over combinations of Frame Relay, ATM, and SDH and back to Frame Relay before being delivered as IP to a Customer premises. It can be dangerous to oversimplify the systems used and Customers need to understand how the Services that they rely on are provided. Annex 3 contains a brief description of the primary telecommunications technologies.

These characteristics do not just apply to the different technologies, but also to physical characteristics associated with components, such as the Local Exchange or duct route. Some Providers who have recognised the threat from terrorist bombings have provided blast proof protection in their Exchanges and do not put critical equipment near windows or on the ground floor. Other Providers, who acknowledge the impact of their main routes being damaged, take special precautions, such as burying their ducts deeply in reinforced concrete casings. Backup power is almost universal, but the effectiveness of Providers' contingency plans will vary. Best Practice would be to use those components where these issues have been effectively addressed.

It is also important to recognise that although some technologies are inherently more resilient than others, they are only effective if they have been designed, implemented and maintained correctly. For example, ATM services are argued to be inherently resilient because they are packet based, but unless the point-to-point networks that carry these services are resilient, they could still fail. Many Providers use SDH technology for their core point-to-point networks to provide this resilience.

> **Recommendation 15:** Understand the inherent resilient characteristics of the components used.

5.4 Questions to ask your Provider

One of the Aims of the Guide is to provide a set of questions that would help the Customer engage with the Provider more effectively. The twenty 'Questions to ask your Provider' are listed in Annex 2 and 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.

> **Recommendation 16:** Use the twenty 'Questions to Ask Your Provider' as a way of agreeing the right solutions for your needs.

5.5 Choosing a service and a Provider

The Guide presents an approach that allows the Customer to make an informed choice as to the most appropriate level of good practice. A cost/risk mitigation exercise will

---

[11] See 'The OSI 7 Layer Model' at Glossary
[12] Frame Relay service: see Glossary

have to be performed by the Customer; for mission critical and high-risk services cost should not always be the deciding factor - the level of assurance can often be more important.

Recommendation 17: Recognise that high availability and high resilience services will cost more than standard services, and do not use cost as the main criterion when procuring these services.

6 SUMMARY OF RECOMMENDATIONS

These recommendations address the threats and vulnerabilities identified across the UK CNI, and also address the need for the CNI to have a greater understanding of the products, technologies, services, and infrastructure provided by the telecommunications sector.

The previous sections outlined 17 recommendations for a Customer of resilient telecommunications services to consider, which are summarised below:

Understand your resilience needs and *why* they should be addressed

Recommendation 1: Understand the types of resilience-based risks associated with your Services.

Recommendation 2: Identify those communications systems that are deemed mission critical and which carry a high risk to the business if they are disrupted.

Recommendation 3: Wherever possible separate out the high risk services from those that only carry a medium or low risk to the business if disrupted.

Recommendation 4: Analyse the threats and vulnerabilities to the mission critical high risk services – eg natural disaster, malicious attack, single point of failure, commercial dependency, lack of transparency.

Recommendation 5: Conduct a self-assessment to understand your risk exposure.

Recommendation 6: Challenge the Provider to explain the marketing statements made on resilience and availability and ensure that you are talking to the right Provider representative.

Understanding *what* you need to do to satisfy these needs

For low/medium risk services:

Recommendation 7: Understand what your Provider(s) do to meet the TI-EPF Resilience Guidelines, described in Section 3, and form a judgement as to whether these satisfy your requirements. If not, then adjust the risk assessment as appropriate.

For mission critical and high risk services:

Recommendation 8: If the risk exposure for a single point of failure is not acceptable, then consider:

a.   The use of end to end separation on all components, including separate building entry points, risers, ducts, exchanges and core network routes;

b.   Using components with inherent resilience, for example use an SDH ring rather than point-to-point SDH or PDH.

Recommendation 9: If the risk exposure stemming from the lack of transparency is not acceptable, then consider:

a.　　The use of a single Provider for any single end to end separacy and diversity service - do not rely on dual Providers to guarantee separation;

b.　　The investment of more time and effort into building relationships with this single supplier, to share testing and assurance activities;

c.　　Making 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 10: If the risk exposure because of a dependency on a single Provider is not acceptable, then consider the use of more than one single Provider for each separacy and diversity service.

Recommendation 11: Apply rigorous due diligence in selecting the Provider, including assurance that they have visibility and control over the Services they deploy to ensure that separacy and diversity is provided and maintained. Also ensure they have adequate contingency plans in place to recover from a disaster.

Understanding *how* to engage your Provider to deliver these needs

Recommendation 12: Understand the architectural options for separacy and diversity based services e.g. what does 'end to end separacy' actually mean.

Recommendation 13: When using the Border Gateway Protocol (BGP) for peering, consider using the NISCC BGP Filtering Guidelines[13] as a common baseline.

Recommendation 14: When peering, consider using 2 or more geographically diverse sites.

Recommendation 15: Understand the inherent resilient characteristics of the components used.

Recommendation 16: Use the twenty 'Questions to Ask Your Provider' as a way of agreeing the right solutions for your needs.

Recommendation 17: Recognise that high availability and high resilience services will cost more than standard services, and do not use cost as the main criterion when procuring these services.

---

[13] NISCC BGP Filtering Guidelines available on request from NISCC

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
Alternative Routing	The routing of information via an alternative cable routing medium (i.e. using different networks should the normal network be rendered unavailable)
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.
ATM	Like Frame Relay, ATM (Asynchronous Transfer Mode) is a packet-switched data network protocol using Permanent Virtual Circuits (PVC) to route data. However, because ATM uses fixed-sized cells to transfer the traffic, and because it doesn't use data store-and-forward, it can better handle time-sensitive traffic like real-time voice and video. ATM is able to carry high-speed, constant bit-rate traffic in a predictable way; this is important for some mission-critical applications like real-time financial transactions. ATM networks are described as highly resilient to infrastructure failures. They are designed with many nodes and routes between the nodes, giving many options for traffic to bypass network problems. End-to-end network availability is typically between 99.7% and 99.9%, depending to a large extent on the performance of local tails to the customer office.
ATM Automatic Teller Machine	Cash dispenser; unrelated to Resilience except that the circuits used to support this service need to be secure and resilient.
AS, ASN	Autonomous System Number allocated to a network
BGP	Border Gateway Protocol; a transport layer protocol used when peering or interconnecting two autonomous networks.
Carrier Redundancy	A term from the US defining the use of more than one carrier or provider to provide a critical service

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 the specified circuits are not routed over the same cables or transmission systems. However there may be some common network nodes within the circuit routings. The ability to use, select or switch between different routes to avoid congestion or network failure.
E1, E2	E1, E2 etc describe a CCITT (ie European) Data Framing structure. E1 = 2.048 Mbps; E2 = 8.448 Mbps; E3 = 34.368 Mbps; E4 = 139.264 Mbps; E5 = 565.148 Mbps. These are commonly abbreviated to 2,8,34,140 and 565 Mbps respectively.
Fallback	Another term for alternative e.g. a fallback facility is another component/site/building that can be use when the original is unusable or unavailable.
Frame Relay Service	Frame Relay is designed to handle variable volumes of traffic, of different types, making it the ideal solution for reliable LAN-to-LAN interconnection. It is most commonly used for applications requiring between 64 Kbs and 2 Mbs. Many of the applications carried over LANs are bandwidth-hungry. Often they need the LAN for short periods of time, resulting in 'bursty' traffic patterns — periods of high volume alternating with periods of low volume. It is therefore important that the bandwidth is used efficiently. Frame Relay is designed precisely for this type of traffic flow. It offers high efficiency, minimal network delay, high availability, prioritised service levels and protocol-transparent transmission, enabling many diverse traffic types to be transported over a common, resilient and integrated network. A typical Frame Relay network is described as being highly resilient against network failures. It is designed with many nodes and routes between the nodes, giving many options for traffic to bypass network problems. Network availability is typically between 99.7% and 99.9%, depending to a large extent on the performance of local tails to the customer office.

ISDN	ISDN (Integrated Services Digital Network) provides a range of features and services for both Disaster Recovery and Business Continuity. Some of the options available are Alternate Routing, Diverse Routing, Site Assurance, Diversion on Busy, and Call Forwarding on Busy.
IP	Internet Protocol; the most commonly used network protocol
IP VPN	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.
	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.
	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.
MPLS	Multi-Protocol Label Switching
OSI 7-Layer Model	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.
	All components of the model are implemented as a number of layers. Each layer performs a well-defined function and 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.
PDH	PDH (Plesiochronous Digital Hierarchy) is essentially the forerunner to SDH and for some time was the transport mechanism of choice. It is a robust and reliable mechanism for providing fixed bandwidth for long periods of time, but suffers from a lack of flexibility and cannot cope with 'bandwidth on demand' situations.
Peer, Peering (of networks)	Networks of roughly the same size exchange traffic as equals, without exchanging money, by peering.
Peer, Peering (of protocols)	See the 7-Layer Model. Protocols in the model communicate with the protocols of the same layer in the remote host by using the services of the layers below, through well-defined interfaces with the adjoining layers.
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 (ie speed) 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 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.
SMDS	(Switched Multi-megabit Data Service), as its name implies, is a switched service that, in the UK, utilises the E1 hierarchy transmission rates. It is a public network where Customers have their own number that they use much like a telephone number. It is designed for interconnecting Local Area Networks and mainframe computers where high data rates and access across a wide area is required. The service is available throughout the UK, and through interconnect agreements to Europe and the US. In terms of resilience it can be thought of as a temporary fixed private circuit, and therefore many of the issues discussed in the section on architecture apply.
SDH	SDH (Synchronous Digital Hierarchy) 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 a Customers' 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. SDH is also used as a point-to-point service in many applications, and customers wishing to take advantage of the resilience of a ring architecture should qualify this with the provider.
Transit	When a customer connects to an ISP, the customer pays for the Transit of traffic across the ISP network. Smaller networks buy Transit from larger networks.
VPN	Virtual Private Network (See IP VPN above)
X.25 Service	The X.25 Packet Service is a highly reliable, low bit rate

	(low speed) standards-based service originally defined as part of the ISDN suite of services. Commonly used on dedicated links at speeds of up to 64 Kbps, it is declining in popularity as applications migrate to higher bandwidth systems.

Alternative Publicly Available Glossaries:

Business Continuity Institute - http://www.thebci.org/

Association for Payment Clearing Services (APACs) - http://www.apacs.org.uk/

OFCOM Glossary - http://www.ofcom.gov.uk/publications/glossary/index.htm

ACKNOWLEDGEMENTS

NISCC would like to acknowledge the contribution made to the development of this Guide by the following Organisations:

BT

Cable & Wireless

COLT
Telecommunications

Energis

LINX

NTL

APACS

OFCOM

Civil Contingencies Secretariat

The NISCC Good Practice Guide to Telecommunications Resilience

ANNEX 1 - SELF ASSESSMENT QUESTIONNAIRE

This Self Assessment Questionnaire has been produced by NISCC 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 Do you have a full and complete list of your business-critical telecommunications services, and the critical systems that support them?

Q2 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.

Q3 Can your organisation and your Provider agree on this unique identifier?

When you need urgent action regarding this service, it is important that you are both talking about the same thing.

Q4 Can you identify business critical services in order of importance or criticality (high, mission critical; medium; low)?

Network Routing

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

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 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 dual-Provider is a guarantee of 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 discus your existing services to ensure there are no dangerous 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 Providers 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 provided 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 such an incident occurring?

Q27 Have you asked for this? Is it covered in your SLA or contract?

The NISCC Good Practice Guide to Telecommunications Resilience

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 Can you explain how you comply with the TI-EPF Resilience Guidelines, so I can understand the standard levels of resilience?

Q2 Do you take part in the voluntary Quality of Service reporting scheme, and if so what are your plans/progress in addressing any improvements in telecom resilience?

Q3 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?

Providing Assurance

Q4 Are you prepared to help me understand the complexities of your network and work together to provide suitable resilient solutions, and if so how will you do this?

Q5 What resources are you prepared to commit to our relationship, and how much of this resource will have detailed technical knowledge?

Q6 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.

Q7 How do you provide assurance that separacy/diversity services meet my requirements and how do you ensure they stay appropriate?

Q8 As a single Provider of a separacy/diversity service, how will you provide transparency and assurance that they will stay resilient?

Contracts and Due Diligence

Q9 Are you prepared to build the right to transparency into the contract and SLA and what form would this take?

Q10 How can you demonstrate that you have full control and visibility of the network assets needed to provide end-to-end separation?

Q11 How can you demonstrate that you have appropriate contingency plans in place, and that they are successfully tested on a regular basis?

Availability Measures

Q12 How do you calculate Availability figures and how do you take account of major disruptive events in their calculation?

Q13 How do you determine your limits of liability associated with Availability guarantees, and what are they?

Understanding the Threats

Q14 How do you assess the physical threats against your network assets and how do you mitigate the risk against them?

Q15 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

Q16 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?

Q17 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, network routes, International links, etc; how do you identify the potential single points of failure?

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; how are they tested and what are the results?

A Single Question

Q20 You know your network attributes; what is your best practice solution for my particular requirement, and can you demonstrate to me that it can be designed and built resilient and that it will stay resilient?