

32 QUESTIONS TO ASK ABOUT YOUR COMPANY'S TELECOM RESILIENCE

FROM THE UK'S CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (CPNI)

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 cooperate 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. 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 assump-

tions 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 national 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? Are 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?

More Information

The 32 questions have been excerpted with permission from CPNI's new good practice guide entitled: *Resilience in Converged Networks: Good Practice Guidance*.

Visit CPNI's website at <http://www.cpni.gov.uk/>

To link directly to the download for the 32 page guide, go to www.GUIDErequest.com/TC