



Small Business Tip Sheet

Preparing your organisation's Broadband Business Continuity Plan

Depending on the nature of your business, your broadband access line can be a critical business asset. To minimise risk to your business from failure of this line, you are advised to:

- a) Perform a 'risk assessment' for your business's use of telecommunications
- b) Obtain the most resilient broadband service that you can afford – to match the level of risk.
- c) Write an action plan for what you would do in the event of a disruption to this service (outage)

a) Perform a *risk assessment* for your business' use of telecommunications

A risk assessment will identify all the uses of telecommunications services and assess the likelihood and impact of poorly working (degraded) or failed services. Where the likelihood and impact are both serious enough, the following steps are recommended.

b) Obtain the most resilient broadband service that you can afford – to match the level of risk.

Explain to your provider your business situation

It is important that your provider knows that your telecommunications infrastructure is 'business critical' – this sets the service level expectation.

Ask your provider for 'Business Grade' services / solutions

Request detailed written material on what 'Business Grade' includes, for example:

- What resilience features are provided with your broadband solution (e.g. redundant links, automatic failover, diverse access paths, multi-site data centres, etc.)?
- Do they provide Service Level Agreements (SLAs) and do these have availability guarantees with accompanying penalty clauses for non-compliance?
- What is the cost for business grade solutions? Compare them with standard grade prices so you can make an informed decision and justify the difference.
- Some providers offer an integrated solution, for example combining a fixed line with mobile failover – ask about these types of solutions.

Consider obtaining an extra broadband line or wireless failover

If integrated resilience solutions offered by providers are too costly or otherwise not suitable for your business, you can order your own redundant (failover) line, ideally from a different provider, for diversity. For example, if you have a DSL service for your broadband, your failover can be a DSL service from a different provider. Ask providers if they have diverse paths into your building so at least one link (primary or failover) will work if there is damage caused by excavation in the street.

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation

Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | [twitter: @ACCAN_AU](https://twitter.com/ACCAN_AU)

Use automatic failover and set it up in advance

It is often possible to configure your IT equipment in advance to automatically divert to the 'failover' service in the event of failure of the main service. If this is not possible then make sure you have a *readily available* step-by-step guide to manually switch to the failover service.

Purchase an auto-failover product

If having an extra broadband line is too expensive for you or not practical for other reasons, equipment is available that can automatically divert to a wireless service when needed. Before choosing this option, check that you have good wireless coverage where your IT equipment is located. IT equipment is often behind internal walls or in the basement where an external antenna may be necessary.

Engage a Systems Integration Company or IT professional

If possible, you should engage an IT professional to set up and maintain your failover solution. If this is not possible, check your 'on call' arrangements and make sure it can help when an outage occurs.

Make sure firewalls, authentication systems and remote access features function correctly

For example, if you are using external third parties for Virtual Private Network (VPN) services, managed firewalls or authentication services, you need to be sure that these still function when failover is deployed. Also, if staff access your service remotely – check that this also functions with your failover solution.

Test your failover solution on a regular basis

Even the best Business Continuity Plans can fail if they are not regularly tested and rehearsed.

c) Write an action plan for what you would do in the event of a disruption to this service

For this step you should refer to ACCAN's Tip Sheet – 'Preparing your organisation's Business Continuity Plan (BCP)'. Some key points are repeated here:

- Make a 'short list' of essential business activities and make sure they can function during a computer or communications outage – leaving other 'day-to-day' work to be performed once services are restored. For example, capture customer details manually and leave online processing for when systems resume.
- Make sure you include contact details – especially after hours – of all the people needed to help restore your services and details of where your off-site data backup is located.
- Include a list of IT, network and telephony equipment with names and phone numbers of service providers and, if possible, a diagram of your IT configuration.
- Outline the steps you will take when vital computers and communications services are not available and who will perform them.

You will need access to someone who knows the technical configuration of your IT services to help prepare this action plan. In addition to the BCP tips listed above, the action plan will take into account specific steps that arise from item 'b' in this tip sheet.

You should regularly rehearse and update this action plan.

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation

Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | [twitter: @ACCAN_AU](https://twitter.com/ACCAN_AU)