TISN

FOR CRITICAL INFRASTRUCTURE

RESILIENCE

Remote Access: A Tool to Support Business Continuity Planning

June 2011

Disclaimer: this document is intended as a general guide only. To the extent permitted by law, the Australian Government makes no representations or warranties of any kind, express or implied, about the accuracy or completeness of the material contained in the document. The reliability of any assessment or evaluation based on its content is a matter for the independent judgement of users. Users should seek professional advice as to their specific risks and needs. The Australian Government accepts no responsibility for the consequences of any use of this document.

Executive Summary

Remote Access: 'A tool to support business continuity' was revised in June 2011 by the Department of Broadband, Communications and the Digital Economy, on behalf of the Communication Sector Group (CSG) of the Trusted Information Sharing Network (TISN).

This guide seeks to provide senior executives and business continuity planning committees with useful and thought-provoking material that covers, at a high level, the range of remote-access technical options available today for organisations that are considering the use of remote access as part of an effective business continuity planning (BCP) strategy. This guide builds upon the information contained in a previous version of the guide, originally released through the TISN website (www.tisn.gov.au) in February 2007.

Whilst the guide is aimed towards senior executives, with a responsibility for the governance over an organisation's business continuity planning, the guide will also be of particular interest to Business Continuity Managers (BCMs) within organisations seeking to assess their business preparedness for both short-term and prolonged emergencies.

In preparing the updated guide, a key consideration was how remote-access solutions have matured since the release of the original guide, with organisations utilising remote access not only in times of emergency but also throughout day-to-day steady state operations. Underpinning this is the concept that, if an organisation designs resilient business processes for its critical services that require the use of remote-access technologies in the steady state, the business process change for an organisation when faced with an emergency can be minimised.

Effective BCP is reliant on both the competence and appropriate levels of expertise from within the organisation—it is the people that understand the organisation—its objectives, processes and risks. Through the use of best-practice tools and methodologies for the identification and analysis of the threats and risks that have the potential to impact an organisation in a time of crisis or emergency, organisations can leverage this analysis to assess the most appropriate remote-access solution for their requirements.

At the heart of this guide is a discussion of some of the tools and techniques that an organisation can use to assist with the development of effective risk management processes and detailed risk and threat assessments that become pivotal to the success of an organisation's business continuity or remote-access policy.

Whilst there is a plethora of documented and historical scenarios that may require an organisation to rely upon the use of widespread remote-access capability during an emergency or crisis, this guide has not sought to exhaustively canvass each and every scenario or threat in detail. Rather than placing a focus on the actual event or cause of the emergency, the guide has taken an all-hazards approach that places the focus on the potential impact on the organisation's critical business processes and services, regardless of the source of the threat.

Building upon the tools and techniques for effective business continuity planning and threat and risk assessment, the guide examines both mature and emerging remote-access technologies and how organisations are increasingly benefiting from the extensive use of convergent mobile devices such as tablets and smartphones to enhance their remote-access capability. The ubiquitous nature of the Internet and the maturity of web-based applications have also enabled remote-access opportunities—ranging from simple communication (email and web browsing) to enabling complex industrial control systems.

The guide acknowledges that remote-access technologies are widely deployed as part of business-as-usual operational processes for the majority of organisations today. Underpinning the pervasive usage of remote-access technologies is the growth of trends including teleworking, mobile computing device adoption and web-based application delivery. All of these trends have shifted the perimeter of an organisation's enterprise beyond the reach of the physical premises, allowing a worker to access business functionality and services in a manner that is consistent with working from the office—anywhere, anytime.

The guide concludes with a section that outlines some of the principles and pitfalls that an organisation should consider prior to and during the implementation of remote-access solutions as part of a BCP strategy. The section provides guidance relating to approaching the market, assessing the capacity and capability of potential service providers, establishing sound contractual arrangements, information security management principles and maintaining effective business continuity plans.

It should be noted by readers of this guide that the guide is not intended as a detailed technical manual for the design of remote-access solutions for an organisation, or as a comprehensive BCP manual. A list of useful resources and references is included in Annex C, along with a business continuity planning checklist in Annex E that may assist an organisation assess its business continuity readiness. Further information on related topics including business resilience, managing information security in an outsourcing arrangement and general information security principles is available for download from the TISN website.

Contents

1 Introduction

Remote-access services have evolved beyond after-hours or emergency business tools to become integral parts of day-to-day business operations. Similarly, the types of mobile devices used to access corporate data and information have also evolved to provide highly-capable multifunctional devices that deliver voice, video and data to the user. This guide examines emerging remote-access technologies and how organisations are increasingly benefiting from the extensive use of convergent mobile devices such as tablets and smartphones to enhance their remote-access capability. The ubiquitous nature of the Internet and many web-based applications are also creating remote-access opportunities ranging from simple communication (email and web browsing) to enabling complex industrial control systems.

This guide will be of particular interest to Business Continuity Managers (BCMs) within organisations seeking to assess their business preparedness for both short-term and prolonged emergencies. The guide also seeks to provide useful information that BCMs can use when critically reviewing, aligning and improving existing business continuity planning practices within their organisations.

This guide is not intended as a detailed technical manual for the design of remote-access solutions for an organisation, or as a comprehensive business continuity planning manual. For further information on both topics, a list of useful resources and references is included in Annex C, along with a business continuity planning checklist in Annex E.

In approaching this important topic, the guide has sought to consider how remote access is used not only in times of emergency but also throughout day-to-day steady state operations for an organisation. Underpinning this is the concept that, if an organisation designs resilient business processes for its critical services that require the use of remote-access technologies in the steady state, the business process change for an organisation when faced with an emergency can be minimised (issues such as congestion and scalability of connectivity still remain).

The Department of Broadband, Communications and the Digital Economy, on behalf of the Communication Sector Group (CSG) of the Trusted Information Sharing Network, reviewed and updated the guide that was originally written in February 2007. Key stakeholders from the CSG and the Information Technology Security Expert Advisory Group were consulted as part of the preparation of this report. A list of the individuals consulted is provided at Annex A.

Figure 1 shows the transition from the steady state through to an event/emergency and the relationship between available bandwidth and the number of users accessing remote access as an organisational business continuity strategy. The graph shows how the aggregated bandwidth supplied collectively by providers in the marketplace would be reduced during an event or immediately thereafter. However, at the same time, the number of remote users needing access to maintain critical business services and processes would suddenly increase. This scenario has the potential to be further impacted if telecommunications providers have oversubscribed services to their clients. They would have done that on the basis that under normal conditions it would be unlikely that all of their customers would use the services at the same time. The graph also indicates how the slow restoration of services and bandwidth to pre-event levels would help stabilise and lessen the impact of critical remote-access users across the board.

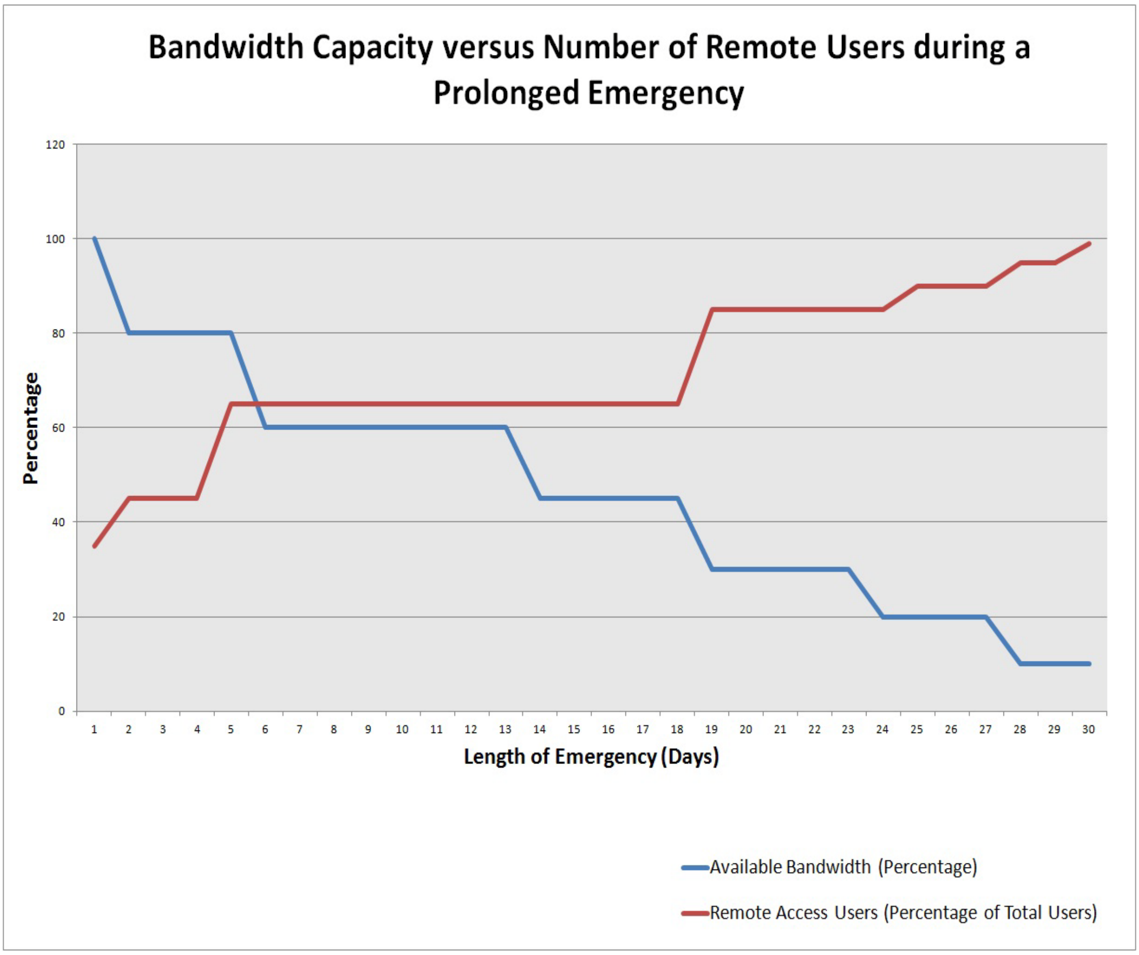

Figure 1: Remote-access bandwidth availability during emergencies

1.1 Structure and purpose of the guide

This document is intended as a guide only. It is strongly advised that the standards and strategies referenced be considered carefully before use in the creation, and/or review, of the organisation's Business Resilience, and Continuity Strategies and Policies. Organisations with existing processes, policies and strategies may consider the use of this document to assist in the critical review, alignment and improvement of their existing practices.

This guide is structured into four sections:

1. Role of Remote Access in Business Continuity Planning (BCP)—this section provides an overview of remote access and its interrelationship with BCP and management.

2. Remote access and BCP, issues and areas of focus—this section provides advice on identifying key business processes and personnel for a remote-access capability by taking a look at the various technical, operational and business continuity issues.

3. Remote access: trends and emerging technology option—this section provides an overview of remote-access technologies that can support an organisation's remote-access strategy and discusses the issues BCMs and Chief Information Officers (CIOs) may consider in implementing a remote-access solution. It also considers a number of factors pertaining to the selection of remote-access communication channels based on trade-offs between cost, security and functionality.

4. Implementing remote access in a BCP, strategy, principles and pitfalls—this section discusses practical advice that may assist an organisation with its consideration of remote-access capabilities. This should help maintain the availability of key business processes and functions for a prolonged period during an emergency situation.

This guide is not intended as a technical resource on remote access. Technical guidance is available from a wide range of sources that are listed in Annex C.

2 The Role of Remote Access in Business Continuity Planning

2.1 ‘Remote Access’ and ‘Business Continuity Planning’ defined

A fundamental objective for business owners and operators is business continuity during an immediate or prolonged emergency. It is important that organisations anticipate a variety of disruptions and have appropriate contingency plans that are designed with rigour and appropriately tested on a regular basis. Regardless of the cause of the business disruption, business owners, clients and regulatory authorities expect a quick restoration to critical business services. For this reason, a remote-access capability that can be easily transitioned from a steady state to an emergency state catering to a variety of scenarios of varying degrees of interruption should be considered an important component of effective Business Continuity Planning (BCP).

For the purposes of this guide, BCP is defined as the planning actions taken by an organisation relating to the development, implementation and maintenance of policies, frameworks and programs to assist an entity to manage a business disruption, as well as build entity resilience. It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a disruptive event[1].

In the context of BCP, remote access provides the ability to use information and communications technology (ICT) systems to sustain key business processes or functions from a remote location, for a short or extended period of time.

A remote location is defined as a place other than the principle place of employment for the employee. This may include:

- alternative offices or a disaster recovery site in accordance with business continuity arrangements
- field staff operating critical business functions via mobile communication devices
- an employee’s home environment
- a hotel
- public access sites such as internet cafes.

An organisation’s remote-access requirements may differ markedly due to remote-access capability being a continuum and dependent on the nature of the organisation. Generally, a distinction can be drawn between a basic and an advanced capability where:

- basic remote-access capability is restricted to a small number of basic business processes such as email and data access, and limited to a defined group of staff with low-priority access
- advanced remote-access capability provides for key business processes and includes a subset of the organisation’s personnel (that is, executives, infrastructure specialists, etc.) who require a higher priority level of access to email and data as well as to other advanced services such as voice, video and emergency management services.

This guide does not limit the consideration of remote access purely to the facilitation of access to the enterprise systems and services for employees and other trusted third parties. It also considers that remote access includes device to device connections between the enterprise and a remote location.

[1] Australian National Audit Office, Business Continuity Management, Better Practice Guide, June 2009.

2.2 Enabling effective Business Continuity Planning and Business Resilience through the use of Remote Access—benefits and outcomes

The benefits of remote-access capability extend beyond supporting organisational BCP. Many job functions are inextricably linked to an organisation’s enterprise applications and services and, as such, having an effective remote-access capability can provide organisations with many tangible benefits by bringing the workplace to the employee. Effective remote-access capabilities can provide enhanced productivity and profitability by allowing employees to respond quickly to organisational and client requests. It can also provide more flexible working arrangements for staff by allowing 24-hour, seven-days-a-week access to job functions. Apart from the benefits to an organisation’s workforce, a well-designed and implemented remote-access solution can assist an organisation facing an emergency situation to maintain:

- financial viability through the continued provision of services
- its reputation and brand equity with clients
- compliance to regulatory obligations
- protection from risk and security exposures.

These tangible benefits have driven the organisational adoption of remote-access solutions as an integral part of an effective BCP strategy.

3 Remote access and Business Continuity Planning, issues and areas of focus

3.1 Establishing appropriate governance mechanisms

Successful BCP relies on expertise from within the organisation. It is the people that understand the organisation, its objectives, processes and risks. It requires a strong understanding of the threats and risks that have the potential to impact an organisation in a time of crisis or emergency. The structure of an organisation's business continuity governance committee should include representatives from both the executive and the operational areas of the business as well as representatives from the risk management and audit committee.

To enhance the resilience capacity of the organisation to effectively mitigate the impact of an emergency, there should be regular assessments of both strategic and operational threats and risks. The outcomes of that assessment can then be used to update the business continuity plan, part of which would include the processes needed to quickly implement remote access to enable the critical business services.

3.2 Understanding the threat and risk landscape

Effective risk management processes and detailed risk and threat assessments are pivotal to the success of any Business Continuity or Remote Access policy. Information security risk can be closely tied to other business risks, such as reputational or financial. As such, the importance of gaining a clear understanding of the relationship between information security risk and an organisation's overall corporate risk assessment cannot be understated.

In considering the range of threats that may potentially impact the effectiveness of remote access as part of a business continuity solution, an organisation should evaluate the potential likelihood and consequences of threats that include but may not be limited to:

- naturally-occurring hazards
  - geological hazards
  - meteorological hazards
  - biological hazards
- human-caused events
  - accidental
  - intentional
- technological-caused events
  - computer failure
  - communications failure
  - energy/power/utility failure[2].

Prior to performing an effective threat and risk assessment related to the inclusion of remote access as a business continuity enabler, an organisation should ensure that an appropriate risk management methodology has been selected to govern the approach to risk and threat analysis. AS/NZS ISO/IEC 31000 describes a process for managing risk throughout the risk management lifecycle[3]:

[2] Further detail on threat sources can be located in Annex A, NFPA 1600, National Fire Protection Association, Standard on Disaster/Emergency Management and Business Continuity Programs 2007.

[3] AS/NZS ISO/IEC 31000:2009, Risk Management—Principles and Guidelines, Standards Australia, Sydney 2009.

3.3 Designing resilient critical business processes

Table 1 outlines some of the high-level strategic, operational and technical questions that need to be considered when planning to reduce the business continuity risk.

Table 1: Resilient business process planning and remote access

Description		
Strategic	What	What business processes or applications are supported by the remote-access solution? The BCM and ICT Manager should have a clear understanding of all the applications that are accessible using steady-state remote-access services.
Operational	Who	Who has access to applications and business processes via remote access? The total number of remote users, what services they have access to, and the equipment they use to connect, such as laptops and handheld devices, must be documented.
	Where	Where do users need to access these work environments from? If the majority of workers are metropolitan-based, then what range of services will be required to support them?
	When	When do users need to get access to these services? Are service-level agreements in place that will ensure the provision of sufficient telecommunications capacity to the organisation and remote users in periods of peak demand during a prolonged emergency?
Technical	How	How are the services delivered? There is likely to be a range of services and technologies that will deliver the remote-access services. A clear understanding of the various channels, capacity and security is critical in design and catering for emergency situations.

To help with the planning for the use of remote access, the various considerations can be classified under three categories—namely the strategic, operational and technical constraints outlined in tables 2–4. In other words, determining the why, what, who, where, when and how of remote access are important business planning considerations.

Table 2: Strategic issues when planning for remote access

Issue	Notes
Legislation	There are many legislative requirements relating to remote-access mechanisms. For example, government classified information must be protected under the *Crimes Act 1914*, personal information must be protected under the *Privacy Act 1988*, certain types of information must be retained under the Archives Act, and certain private sector records must be kept under various other Acts relating to corporate operations. Organisations should ensure that any remote-access mechanisms under consideration are capable of complying with relevant laws and regulations.
Benefits	Organisations should determine the potential benefits in adopting remote-access capabilities. One of the key drivers might be to maintain business continuity during periods where employees are unable to physically attend their normal place of work.
Risk	Organisations should model their remote-access business processes and determine the potential risks involved. This will determine the operational security requirements of the remote-access architecture.
Cost	Since remote-access capabilities comes at a cost (new technology, procedures, support arrangements, etc.), it is important to conduct a thorough cost-benefit analysis to ensure a positive return on investment.
Standards	There are many national and international standards relating to communications protocols, data formats and information technology. Organisations that have not implemented remote-access technologies in the past or those that use proprietary mechanisms should consider adopting these standards. This will help to ensure that remote employees, partners, clients or customers can use off-the-shelf hardware and software to facilitate remote access.
Policies	Organisations might consider establishing and implementing policies to assist employees to work away from their principal worksites, with appropriate access to applications. Changes may also be required to corporate security policies and IT security policies, configuration management plans and maintenance plans.
Training	Organisations might consider cross-training employees to perform essential business functions remotely to improve resiliency. If remote-access mechanisms are new to the organisation, employees and support/technical staff will require training on the operation of the relevant hardware and software components of the remote-access architecture.

Table 3: Operational issues when planning for remote access

Issue	Notes
Requirements	The operational requirements of an organisation's remote-access architecture should be driven by the organisation's overall strategic plan.
Bandwidth	Different business processes have varying bandwidth requirements depending on the application type and the information structures involved. Organisations should conduct a bandwidth audit to ensure there is sufficient capacity on the chosen communications channels particularly in periods of peak demand.
Coverage	Not all communication technologies are available continuously or have complete coverage over Australia. Organisations should determine their geographic and global remote-access requirements and select communications appropriately.
Resilience	Organisations should be aware of the reliability and resilience of the various telecommunications channels.
Support	The level of support required is usually proportional to the scope of the roll out of remote-access mechanisms. New and infrequent users will inevitably experience teething problems as they familiarise themselves with the new technology and procedures.
Procedures	Standard operating procedures will need to be developed for the chosen remote-access architecture. This applies particularly to security.

Table 4: Technical issues when planning for remote access

Issue	Notes
Specifications	The functional specifications of the remote-access architecture should be formally derived from the operational requirements. This will avoid stovepipe and proprietary solutions that may suffer incompatibility problems both within the organisation, and with external partners, clients or customers.
Supportability	Organisations should consider whether remote-access support functions will be provided in house, contracted, or outsourced. When key personnel move, information security, loss of capacity and functionality and the loss of expertise will need to be considered.
Integration	In all but the simplest remote-access processes (for example, email), organisations may need to consider interfaces to integrate remote-access clients with back-end systems behind remote-access gateways.
Security	Organisations should select remote-access security controls based on a formal threat and risk assessment of the various architectural options. This will help to determine whether the individual operational security requirements will be satisfied by technical or procedural controls (or both).

3.4 Business as usual, immediate threat and prolonged emergency scenarios

Whilst there are numerous documented scenarios that would necessitate the implementation of widespread remote-access capability for a majority of staff, the actual event or cause of the need to implement this capability is only a secondary concern. The main focus should be the creation and implementation of Remote Access and Business Continuity strategies and policies that allow for the easy rollout of this capability without needing to focus on the nature of the event but rather the impact that the event has presented the organisation.

Further to the list of potential threats that should be considered during the threat and risk management analysis process covered in a previous section, there are many varied potential scenarios where staff might be unable to attend their normal place of employment for extended periods, such as:

- a major health crisis
- natural disasters
- terrorist incidents.

Faced with such a scenario, an organisation may assess its likelihood as being either short-term or of a prolonged nature. BCPs are thus recommended to be adaptive to accommodate the duration of an event.

3.5 Capability, capacity and availability management principles

Capacity management[4] seeks to provide a continual optimal balance between supply against demand, and costs against resources needed. This optimum balance is only achieved both now and in the future by ensuring that capacity management is involved in all aspects of the service delivery lifecycle. When this does not occur, Capacity Management only operates as a reactive process, with limited benefits achieved as a result.

Capacity management when used reactively is only implemented when disruptions begin to occur as demand has exceeded supply. While the implemented capacity does work to resolve the disruptions, there are some consequences to this type of reactive behaviour including:

- purchase of IT infrastructure components that do not optimally fit the requirements or architecture
- budget overruns for the unforeseen and unanticipated purchases
- periods of time where there are potentially large amounts of excess capacity
- reduced customer and user satisfaction with the affected IT services
- a general negatively affected perception of the IT organisation as a whole.

To assist an organisation in understanding their maturity levels, the established industry standard, the P3M3® (Portfolio, Programme and Project Management Maturity Model) self-assessment[5] questionnaire from the United Kingdom's Office of Government Commerce, can be used to:

- gauge the current level of organisational maturity in respect of portfolio, program and/or project management
- gain an understanding of the key practices in effective portfolio, program and project management processes
- identify the key practices that need to be embedded within an organisation for it to improve process capability and achieve the next maturity level
- understand and improve an organisation's capability to manage its portfolio, programs and projects more effectively.

[4] ITIL Service Management Publications www.best-management-practice.com/Publications-Library/IT-Service-Management-ITIL/

[5] Portfolio, Programme, and Project Management Maturity Model (P3M3) Publications and Self Assessment Tools available at: www.p3m3-officialsite.com/P3M3Model/P3M3Model.aspx

By completing the self-assessment questionnaire, a relatively quick evaluation of the current organisational maturity with respect to capacity, capability and availability management is obtained for the organisation as well as for their suppliers.

Availability management is one of five components in the IT infrastructure library service delivery area [6]. It is responsible for ensuring application systems are up and available for use according to the conditions of the service-level agreements (SLAs).

The establishment of an appropriately-skilled availability management team within an organisation can establish and review business process availability requirements, ensuring the most cost-effective contingency plans are put in place and tested on a regular basis to deliver the organisation's business requirements.

Availability management is also the lead-in component failure impact analysis and service outage analysis initiatives, determining cause, analysing trends and taking any appropriate actions to ensure service availability meets SLAs.

Availability management activities include:

- ensuring service availability meets SLAs
- determining the cause of availability failures
- reviewing business requirements for availability of business systems
- cataloguing business requirements
- ensuring proper contingency plans are in place and tested
- establishing high-availability, redundant systems to support mission-critical applications.

Benefits to implementing availability management processes include:

- Services are available for use during expected time frames as specified in SLAs.
- Services are provisioned on specific infrastructure depending upon their availability needs. This avoids unnecessary costs due to provisioning services with longer recovery times on more expensive high-availability platforms.
- Potential service availability issues are identified and corrected before they negatively impact services.

[6] ITIL Service Management Publications www.best-management-practice.com/Publications-Library/IT-Service-Management-ITIL/

4 Remote Access, trends and emerging technology options

4.1 Mature remote-access options

Remote-access technologies are widely deployed as part of business-as-usual operational processes for the majority of organisations today. Underpinning the pervasive usage of remote-access technologies is the growth of trends including teleworking, mobile computing device adoption and web-based application delivery. All of these trends have shifted the perimeter of an organisation's enterprise beyond the reach of the physical premises, allowing a worker to access business functionality and services in a manner that is consistent with working from the office—anywhere, anytime.

As discussed in a previous section, the extended use of remote access has enabled organisations to design resilient business processes that from a user's perspective do not significantly change work practices from a business-as-usual steady state, to an initial response to an emergency, through to a prolonged emergency.

This section examines the current remote-access technology landscape, considering the range of mature technologies, the emerging trends, and the potential use of newer technologies. It also contains some high-level guidance to assist an organisation to select the most appropriate remote-access technologies.

Figure 2 below shows the wide range of potential remote-access connections that an enterprise may utilise as part of its remote-access capability in both a business-as-usual mode of operation and an emergency situation. In all cases, the issues of reliability and scalability are core to the successful use of remote access. Reliability refers to the ability for users or devices to connect to the required enterprise resources as required and scalability refers to the ability of the remote-access systems to cater for increased connections during an immediate or prolonged outage.

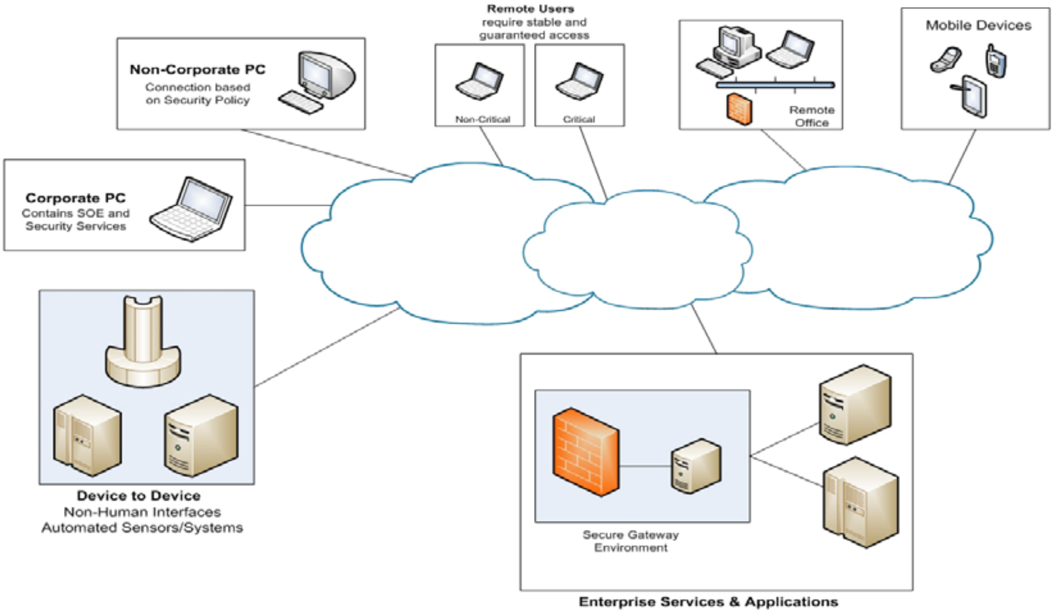

Figure 4: Remote-access user and device types

Whilst the figure above provides a view of the different types of users and devices that require remote access, the transport mechanisms that facilitate these connections are wide-ranging. The following section of the guide provides an overview of the mature remote-access technology types available to an organisation.

4.1.1 Wired services

Fixed-line services have traditionally provided the majority of remote-access telecommunication channels. Fixed-line services can be categorised in two classes based on speed, narrowband and broadband.

Narrowband services are those services that provide lower downstream and upstream data rates—generally accepted to be less than 256/64 kilobits per second—provided by dial-up across the public subscriber telephone network (PSTN) or integrated services digital network connections.

Fixed line broadband services provide a variety of access services operating at speeds at or above 256/64 kilobits per second ranging through to speeds of 1 gigabit per second. These services are delivered by a wide array of technologies that include ADSL, ADSL 2+, cable, frame relay, digital data services and Asynchronous Transfer Mode (ATM). The service can provide direct or indirect access to an organisation's enterprise services or access to the public internet.

Whilst the usage by organisations of narrowband connections is reducing due to the proliferation of cheaper and more accessible broadband connections, narrowband connections can still provide a valuable remote-access mechanism to an organisation as part of its BCP strategy. The use of narrowband connections—for example, dial-up through the PSTN—may still offer an organisation a relatively low-cost and stable connection for low-volume data connections such as device-to-device connections or sensor reporting.

Where an organisation relies upon the PSTN for a remote-access connection it is important to engage with the service provider to gain an understanding of whether or not there are any service guarantees in place that cover the availability of the service. Where service guarantees are not available and the service delivered through the remote-access connection is deemed to be critical, an organisation should assess alternative remote-access technologies to ensure that the organisation's risk profile is adequately supported.

4.1.2 Wireless Services

Wireless communication options for the provision of remote-access data services have increased substantially in the past few years. The proliferation of handheld computing devices beyond a simple voice-based mobile phone has led many organisations to rely for their day-to-day business operations on wireless services such as GSM High-Speed Downlink Packet Access (HSDPA) services based on the 3G standard, Worldwide interoperability for Microwave access (WiMax) and 802.11x Wi-Fi services.

Wireless data provides an alternate communications path for the 'last mile' connectivity in relation to remote-access services. These services are independent of the fixed-line network until they reach the core network of the carrier or service.

The data rates offered by GSM HSDPA, WiMax and Wi-Fi are comparable to domestic broadband services such as ADSL and ADSL 2+ (depending on the coverage offered by the provider). As a result, many enterprise services that have been traditionally provided from within an organisation's physical premises are now delivered wirelessly.

Whilst wireless technologies deliver opportunities for organisational resources to access enterprise resources regardless of location, security considerations regarding the protection of data at both rest and during transmission need to be commensurate with the security profile of the data.

Further to security considerations, organisations need to assess the likelihood of wireless services becoming either unavailable or at the very least degraded during an emergency situation through either damage or through congestion resulting for a large spike in usage. In both cases, where an organisation is reliant upon the use of wireless data transmission mechanisms for remote access to critical services, alternative remote-access mechanisms that utilise non-wireless technologies should be considered as a backup.

The emerging technology section which follows provides some further commentary on the technical advances with wireless technologies and the growth in the use of mobile computing devices.

4.1.3 Virtual Private Networks (VPN)

A VPN uses a public network—usually the internet—to connect remote sites or users together. Instead of using a dedicated, fixed-line or wireless connection, it uses connections routed through the internet from the company's private network to the remote site or employee.

VPNs provide a number of options that help to merge enterprise network services along with remote-access services. VPNs provide a blend of traditional access services such as dedicated frame relay and Asynchronous Transfer Mode (ATM) fixed-line connections along with ADSL and emerging wireless services such as HSDPA.

The deployment of a range of transmission mechanisms means organisations can offer remote-access solutions that avoid reliance on a particular type of data transmission, allowing the user to select the most appropriate option. For example, this may mean the use of ADSL when working from home, HSDPA when working from a mobile device, or a frame relay connection from a regional office in a remote location.

VPN technologies are wide–ranging, and whilst a discussion of the benefits of one technology type over another goes beyond the reach of this paper, two of the most widely-used VPN technologies are Secure Sockets Layer (SSL) which generally utilises a web browser’s security to form the basis of the connection, and Internet Protocol Security which provides both authentication and encryption of data across an untrusted connection.

For many organisations, a well-designed VPN has become the core remote-access mechanism for enterprise applications and services due to the flexibility and diversity of connections it supports. Again, as discussed in the wireless technology section, for a VPN to be an effective remote-access mechanism, an organisation needs to thoroughly assess the security of data at rest and during transmission through the VPN to ensure it supports its security posture and risk profile.

4.1.4 Managed network services

In many cases, remote-access solutions have been built and maintained by an organisation’s IT department; however, a wide range of service providers offer mature remote-access services that are available as managed services to organisations.

Managed services are generally based on private data-switched networks designed and maintained by telecommunication carriers and information technology service providers. However, while the integration of new services or technology, such as wireless 3G HSDPA, is the responsibility of the provider, the introduction of a new service or technology is a commercial decision for the organisation.

Further to the commercial implications for an organisation considering the use of managed services for the facilitation of remote-access services, the security implications of outsourcing the responsibility for the delivery of services to a third party should be thoroughly assessed by an organisation prior to the establishment of any formal contractual arrangements. This assessment should include the review of:

- the suitability of the data to be managed, stored and transmitted by a third party—this could include the security classification of the data or its commercial sensitivity
- the ability and experience of the service provider to deliver the service in line with the organisation’s security posture and risk profile
- the storage location of the data as well as the transmission path taken by the data across the service, as data transmitted internationally may expose it to privacy or security legislation from the countries that it transverses.

Further information on this area can be obtained from the TISN guide ’Managing IT security when outsourcing to an IT service provider’[7].

Whilst managed services can deliver benefits to an organisation, including the reduction of management and technical resources and access to updated technologies as they mature, in many cases remote-access managed services are sold as a standard offering with little opportunity for customisation. As a result, for an organisation to reap the benefits from a remote-access managed service, an organisation’s business processes may require adaptation to ensure that they work seamlessly with the managed service. A further discussion on this point occurs in the emerging technology section in relation to the use of cloud computing as a delivery model.

4.1.5 Evaluated products

When planning the design of a remote-access solution, an organisation may find the evaluated products list published by the Australian Government useful in assisting to manage risk and cost. Evaluated products are those that have been assessed and approved for use for defined data purposes up to a specified level of sensitivity. These are both software and hardware products.

In Australia, the Defence Signals Directorate (DSD) established the Australasian Information Security Evaluation Programme in 1995. The program ensures the ready availability of a comprehensive list of independently assessed IT products—the Evaluated Products List (EPL)[8]. A process of international recognition allows for products evaluated in countries that subscribe to the Common Criteria Evaluation Scheme to have that evaluation accepted in member countries. In addition, the EPL provides high grade as well as one-off evaluations. These evaluations are typically performed internally by DSD and are afforded the same or higher status than common criteria evaluations. There is specific guidance associated with these products as to the data classification levels for which they are suitable.

4.2 Emerging remote-access technologies and their potential application

Emerging remote-access technologies included for consideration in this section were selected on the basis that they are currently in use by organisations as part of their remote-access strategies, but are still evolving in their development on an ongoing basis, with the introduction of greater speed, stability or accessibility. This section covers a range of technologies including cloud computing, 4G wireless, and a brief overview of some of the trends that are emerging, particularly with regards to the greater use of mobile computing devices within an organisation.

[7] Trusted Information Sharing Network, IT Security Expert Advisory Group, May 2007, Managing IT Security when Outsourcing to an IT Service Provider, viewed June 2011, www.tisn.gov.au

[8] www.dsd.gov.au/infosec/epl/index.php

4.2.1 Cloud Computing

Cloud computing, as a business model for service provision, is becoming more prevalent, driven by the potential for cost and time efficiencies. Cloud computing can be defined as a 'model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[9]. Cloud computing offers the following:

- infrastructure as a service (IaaS)—which involves the vendor providing physical computer hardware including processing, memory, data storage and network connectivity
- platform as a service (PaaS)—which includes the vendor provisioning IaaS as well as operating systems and server applications
- software as a service (SaaS)—which includes the vendor providing cloud hosted software applications.

Cloud computing is also categorised by a range of different deployment models that include:

- the public cloud, which is shared by multiple organisations and accessed through the public internet
- the private cloud, where an organisation utilises a cloud that is provisioned by the vendor for its sole use and accessed through a private connectivity mechanism
- a community cloud, which is generally used by like-type organisations with a similar security and risk profile
- the hybrid cloud, which involves a combination of the other three deployment models.

From a remote-access and BCP perspective, cloud computing, if deemed suitable by an organisation, can offer the ability for enterprise services users to gain access to information and applications regardless of location. Secondly, cloud computing allows an organisation to host its applications and business services beyond the physical boundaries of its premises, potentially mitigating the risk of a service disruption in the case of a geographically-specific incident or emergency.

It should, however, be noted that whilst this may be potential mitigation, it also results in exposing the organisation to a geographical incident related to the location of where the cloud service provider has chosen to host the data. As a result, prior to the selection of a cloud-based service it is important for an organisation to assess the hosting location of the data, the suitability of the model for the types of services to be provisioned, as well as the capability of the service provider to meet the security and risk requirements.

4.2.2 4G Mobile Services

4G is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards. 4G has the potential to deliver further advances in both speed and reliability for mobile device communications including peak speeds of 100 megabits per second for high-mobility communication (such as from trains and cars) and 1 gigabit per second for low-mobility communication (such as pedestrians and stationary users).

A 4G system is expected to provide a comprehensive and secure all IP-based mobile broadband solution to laptop computer wireless modems, smartphones, and other mobile devices.

[9] National Institute of Standards and Technology (NIST), The NIST Definition of Cloud Computing (Draft), NIST Special Publication, 800–145, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

From a remote-access and business continuity planning perspective, 4G mobile services have the ability to further enable the ability of users that require access to enterprise services remotely to gain access at a higher speed.

However, it should be noted that 4G services are still in their infancy. Whilst they have the potential to enable access to higher-bandwidth applications remotely, at this point in time fixed-line connections may still be required by organisations to fulfil this requirement in the case of an emergency.

4.2.3 Wi-Fi

Whilst Wi-Fi access speeds have increased in recent years, from a remote-access and business continuity perspective, the increased availability of public Wi-Fi hotspots through a diverse range of providers has the potential for organisations to leverage these connections in a time of crisis (utilising devices or connection mechanisms that support the desired security controls within the organisation).

It is, however, important to note that the use of publicly-available Wi-Fi hotspots is inherently insecure and can result in security exposures including data interception or the compromise of unprotected devices from malware. As such, it is of paramount importance that an organisation ensures that it takes adequate security protection measures prior to usage of these services as part of an effective remote-access strategy.

Further to the increased number of public Wi-Fi connections is the availability of pocket Wi-Fi devices or smart devices, such as iPhones, that have the ability to act as a Wi-Fi hotspot connecting through to the mobile data network. Again, whilst these connections rely upon the availability of the carrier network or public infrastructure that is not subject to service guarantees, as reliability and capacity improves over time they may form an important component of an organisation’s remote-access strategy.

4.2.4 Tablets and Smart phones

The growth in both the capability and number of smartphones and handheld computing devices has been phenomenal. As an illustration, Apple CEO, Steve Jobs reported in 2010 that more than 15 million iPads had been sold in nine months and that more than 100 million iPhones had been sold at that point in time. The proliferation of this category of devices indicates a strong trend that is expected to continue relating to the mobility of workers and their use of remote access as part of business as usual operations.

From a business continuity perspective, smartphones and handheld devices open up many possibilities for organisations to provide increased levels of access to enterprise applications and services in new and creative ways. In the case of an emergency, the increased number of devices seeking to gain access to communications infrastructure to fulfil their roles from a remote location is likely to place burdens on that infrastructure that cannot be fully tested without an actual emergency.

As a result of the potential capacity constraints that may occur during an emergency, an organisation must consider the potential for mobile devices to experience significant degrees of degradation or lack of access when including them as a core component of their BCP strategy.

Organisations should also consider the implementation of end-point security on any tablet or smartphone that is not equipped with a corporate standard operating environment and security profiles to ensure that, when the devices are used for remote access to enterprise applications, the organisation’s security is not compromised by unprotected devices.

4.2.5 Thin Client Computing

Whilst thin client computing has been available in the market since the early 1990s, the adoption by organisations has increased markedly in recent years. Thin client computing delivers applications or a complete desktop image remotely to the user across a wide range of devices from handhelds through to terminals with no local storage capabilities. Servers within a data centre provide the processing and data storage required for thin client computing. An advantage of thin client computing as a remote-access solution is the ability to provide additional security controls over enterprise data, as no data remains resident on the end-user devices.

4.3 Selecting the most appropriate technologies to enable BCP within an organisation

In order for an organisation to select the most appropriate remote-access technologies as part of their BCP strategy, the technologies used need to closely match user or device access requirements during an immediate or planned outage.

As per the previous risk management section, a strong understanding of the potential threats and the resultant risks and mitigations is required before making any assessment of the technologies on offer.

In concert with a strong understanding of the organisation's risk profile is a consideration of the security posture with regards to both information and intellectual property that must be maintained when faced with an immediate or prolonged emergency. Without this understanding, it is not possible for an organisation to make an informed decision on which technologies are the most suitable for their requirements.

When considering the most appropriate technologies to align to an organisation's risk profile and security posture, it is essential that an organisation considers the speed of the connection that is required and the likelihood that it can be maintained as required during an emergency. Modelling the remote-access solutions against the worst possible case scenarios may lead to a more appropriate selection of the technologies to deploy. Organisations looking to conduct this modelling and associated assessment may find useful reference material in the Australian National Audit Office business continuity guidance[10], the Australian business continuity standard[11], the Australian Standard for Information Security, and the Protective Security Policy Framework[12] governed by the Attorney General's Department.

Due to the wide range of requirements that are applicable to different organisations, this guide is unable to be prescriptive regarding which technology is the most suitable for a particular organisation or scenario. However, the BCP checklists found in Annex E may provide a useful tool to assist an organisation prepare for the selection of technologies as part of its BCP and remote-access strategy.

[10] Australian National Audit Office, Business Continuity Management. Building resilience in public sector entities, viewed May 2011, www.anao.gov.au/Publications/Better-Practice-Guides/2008-2009/Business-Continuity-Management---Building-resilience-in-public-sector-entities

[11] Standards Australia, HB 221-2004; HB 292-2006; HB 293-2006, Sydney

[12] Emergency Management in Australia, January 2011, Australian Government Protective Security Policy Framework, Attorney General's Department, www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Contents

5 Implementing Remote Access in a Business Continuity Planning strategy, principles and pitfalls

5.1 Approaching the market

As with any well-planned procurement, the definition of clear and concise requirements is essential when approaching the market for a remote-access solution. As an organisation will use the remote-access solution for both business-as-usual and immediate and prolonged emergency situations, an organisation may need to specify its capacity, availability and performance requirements against a range of scenarios that provide the necessary clarity to a potential supplier around the organisation's requirements.

5.2 Assessing the capability and capacity of suppliers

To adequately assess the capability and capacity of a potential supplier to fulfil the requirements as specified in the organisation's requirements, it is necessary to define detailed evaluation criteria for the assessment[13].

Well-structured evaluation criteria may include:

- value for money
- demonstrated experience of the potential supplier in delivering a similar service
- the ability of the potential supplier to guarantee service performance and availability in the case of an emergency
- any dependencies that the potential service provider may have on other suppliers to deliver the services in scope
- how the potential service provider will manage the prioritisation of service delivery in the case of an emergency or an outage to the service (for example, whether the potential supplier will provide higher priority to another customer in the case of an emergency)
- the potential service provider's demonstrated performance during recent emergency situations
- the maturity of the potential service provider's BCP practices
- the maturity of the potential service provider's operational service delivery processes
- the strength and number of references available to be provided by the potential service provider
- flexibility and willingness of the potential service provider to work with the organisation to find innovative solutions when faced with an emergency.

When conducting the assessment[14] of a potential supplier's capacity and capability to deliver the services, it is essential that the organisation assemble a team with the appropriate skills and experience to perform a rigorous assessment against the evaluation criteria. Where an organisation identifies gaps in their own experience and skills, engagement of independent advisors with the necessary demonstrated experience may be useful in ensuring that the assessment is conducted successfully[15].

[13] Australian Government, Department of Finance and Deregulation, December 2008, Commonwealth Procurement Guidelines – FMG 1, viewed June 2011 www.finance.gov.au/procurement/procurement-policy-and-guidance/CPG/index.html

[14] Chartered Institute of Purchasing and Supply www.cips.org/en-au/Resources/

[15] ITIL Service Management Publications www.best-management-practice.com/Publications-Library/IT-Service-Management-ITIL/

5.3 Establishing sound contractual arrangements and service-level agreements

To establish sound contractual arrangements and service-level agreements (SLAs) for a remote-access solution in a BCP context, an organisation will need to ensure that the contract explicitly specifies the service levels required of the potential service provider. The service levels must take into account the business-as-usual, immediate and prolonged emergency scenarios. The SLAs must also be enforceable and be suitable for compliance auditing.

The SLAs should include metrics that address service:

- availability
- capacity
- incident and problem management
- performance
- change management.

As an organisation's business requirements may change over time along with the organisational risk profile and security posture, it is important for an organisation to consider the ability of the contractual arrangements to provide enough flexibility to meet the ongoing needs of the organisation, whilst still maintaining the contractual obligations of the potential service provider to deliver the services bound by the contract.

5.3.1 Information Security Management Principles

Information security is the protection of information and information systems, and encompasses all infrastructures that include processes, systems, services and technology. It relates to the security of any information that is stored, processed or transmitted in electronic or similar form. IT security is a subset of information security and is concerned with the security of electronic systems, including computer, voice and data networks[16]. Whilst this definition is targeted towards public sector organisations, the definition applies equally to private-sector organisations.

Information security has the following objectives:

- confidentiality—ensuring that information is accessible only to those with a legitimate requirement and authorised for such access
- integrity—safeguarding the accuracy and completeness of information and processing methods
- availability—ensuring that authorised users have access to information and associated assets when required[17].

Underpinning these objectives is a set of principles of information security.

An example of principles is outlined by the IT Security Expert Advisory Group paper 'Secure your information: information security principles for enterprise architecture'[18] as follows:

- information security is integral to enterprise strategy
- information security impacts on the entire organisation
- enterprise risk management defines information security requirements
- information security accountabilities should be defined and acknowledged

[16] IT Security Management Audit Report No. 23, Australian National Audit Office, Dec 2005, p. 21

[17] Emergency Management in Australia, January 2011, Australian Government Protective Security Policy Framework, Attorney General's Department, p. 24

[18] Department of Broadband, Communications and the Digital Economy, 'Secure your Information: Information Security Principles for Enterprise Architecture', June 2007 www.dbcde.gov.au/__data/assets/pdf_file/0017/70622/Secure-Your-Information_CIOCSO.pdf

- information security must consider internal and external stakeholders
- information security requires understanding and commitment
- information security requires continual improvement.

5.3.2 The importance of maintaining the desired security posture

When planning the implementation of a remote-access solution to support an organisation's BCP strategy, it is essential that the security principles as outlined above are considered and used as the basis to define the organisation's security posture. Once an organisation has a defined and agreed security posture, it can be applied to range of potential remote-access solutions under consideration, providing a reference point to assess the suitability of the solutions against the organisation's business requirements.

If an organisation's BCP strategy fails to maintain its desired security posture during an emergency situation, the organisation may become exposed to legislative, or in some cases criminal exposures. As a result, it is essential that an organisation thoroughly considers the suitability of a remote-access solution in maintaining its security posture.

5.3.3 Maintaining effective Business Continuity Plans

The maintenance of effective business continuity plans is essential to an organisation's ability to operate during an immediate or prolonged emergency. All business continuity plans are based on a point-in-time assessment of the threat and risk landscape faced by the organisation, and as such should be updated on a regular basis to ensure the currency of the plans.

To maintain the effectiveness of an organisation's plans, regular testing should occur against the most up-to-date set of threats that are in view by the organisation. A useful mechanism for the development of testing scenarios is to model the impact of an actual recent emergency that may have occurred in another geographical area against the organisation's plans. Using this technique can assist an organisation to test its preparedness and resiliency against a known set of outcomes, bringing the testing to life.

Apart from the regular testing of an organisation's business continuity plans, it is also important to participate, where possible in the BCP exercises conducted by the service providers that an organisation will rely upon in the case of an emergency. Through this involvement, an organisation can gain a greater insight into the limitations or capabilities that their service providers possess. Any information gained through this additional process should also be used to inform the updated organisational business continuity plans.

Annex A: Consultation summary

CSG representatives

- Dean Veverka, Southern Cross Cables Network
- Zack Gurdon, Telstra
- Joe Giovenco, TX Australia
- Steve Flohr, Australian Broadcasting Corporation
- Bill Grace, Optus
- Hugh James, Special Broadcasting Service
- Steve Minahan, Broadcast Australia
- Andrew Potter, Foxtel

ITSEAG members

- Lawrence Ostle, CSC
- Colin Bradley, Cisco Systems
- Craig Valli, Edith Cowan University

Annex B: Glossary of terms

After-hours: Hours of operation that are not considered standard business hours.

Asynchronous transfer mode: A switching technique for telecommunication networks. It uses asynchronous time division multiplexing, and it encodes data into small fixed-sized cells. This differs from networks such as the Internet or ethernet local area networks that use variable-sized packets or frames.

Availability management: Targets allowing organisations to sustain the IT service availability to support the business at a justifiable cost. The high-level activities are realise availability requirements, compile availability plan, monitor availability, and monitor maintenance obligations. Availability management addresses the ability of an IT component to perform at an agreed level over a period of time.

Bandwidth: Bandwidth, network bandwidth, data bandwidth or digital bandwidth is a bit rate measure of available or consumed data communication resources expressed in bits per second or multiples of it (kilobits per second, megabits per second, etc.).

Business as usual: The normal execution of standard functional operations within an organisation, particularly in contrast to a project or program which would introduce change.

Business continuity: The activity performed by an organisation to ensure that critical business functions will be available to customers, suppliers, regulators and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control and help desk. Business continuity is not something implemented at the time of a disaster; business continuity refers to those activities performed daily to maintain service, consistency and recoverability.

Business continuity planning: Planning which identifies the organisation's exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery for the organisation, whilst maintaining competitive advantage and value system integrity. It is also called business continuity and resiliency planning. The logistical plan used in business continuity planning is called a business continuity plan. The intended effect of business continuity planning is to ensure business continuity, which is an ongoing state or methodology governing how business is conducted.

Business impact analysis: The differentiation between critical (urgent) and non-critical (non-urgent) organisation functions/activities. A function may be considered critical if the implications for stakeholders of damage to the organisation resulting are regarded as unacceptable. Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.

Capability management: Balancing economy in meeting current operational requirements, with the sustainable use of current capabilities, and the development of future capabilities, to meet the sometimes competing strategic and current operational objectives of an organisation.

Capacity management: A process used to manage IT with the primary goal to ensure that the IT capacity meets current and future business requirements in a cost-effective manner. One common interpretation of capacity management, as described in the information technology infrastructure library framework, is that capacity management comprises of three sub-processes: business capacity management, service capacity management and component capacity management.

Communications protocols: A formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. The protocol would define the syntax, semantics and synchronisation of communication, and the specified behaviour is typically independent of how it is to be implemented. It can therefore be implemented as hardware or software or both.

Component failure impact analysis: A study that attempts to predict the consequences of failures of the major components of a system.

Congestion: Deterioration of service when a node or a link is overloaded with data. Typical effects include, but are not limited to, queuing delay, packet loss or the blocking of new connections.

Convergent mobile devices: Mobile devices that increasingly do more tasks and contain increasing amounts of power, memory, etc. Examples are smartphones such as the iPhone and Android mobiles, as well as other non-phone devices such as the iPad and Xoom.

Cost-benefit analysis: An economic decision-making approach used particularly in government and business. Cost-benefit analysis is used in the assessment of whether a proposed project, program or policy is worth doing, or to choose between several alternatives. It involves comparing the total expected costs of each option against the total expected benefits, to see whether the benefits outweigh the costs, and by how much.

Governance: The act of governing relates to decisions that define expectations or verify performance. It consists of either a separate process or part of management or leadership processes. It relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility.

Information Technology Infrastructure Library (ITIL): An IT management framework that provides practices for information technology services management, IT development and IT operations. ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive checklists, tasks and procedures that any IT organisation can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom's Office of Government Commerce (OGC).

IT service management (ITSM): A discipline for managing IT systems, philosophically-centred on the customer's perspective of the contribution of IT to the business. ITSM stands in deliberate contrast to technology-centred approaches to IT management and business interaction.

Mission critical: Refers to any factor of a system (equipment, process, procedure, software, etc.) failure of which will result in the failure of business operations. That is, it is critical to the organisation's mission.

Off-the-shelf: A term defining a non-developmental item of supply that is both commercial and sold in substantial quantities in the commercial marketplace, and that can be procured or used under contract in the same precise form as available to the general public.

Office of Government Commerce (OGC): Part of the Efficiency and Reform Group of the Cabinet Office, a department of the Government of the United Kingdom. The OGC operates through Buying Solutions, an executive agency. The purpose of the OGC is to support the procurement and acquisition process of public sector organisations in the United Kingdom through policy and process guidance and the negotiation of overarching service and provision frameworks.

Portfolio, program and project management maturity model (P3M3): A reference guide for structured best practice. It breaks down the broad disciplines of portfolio, program and project management into a hierarchy of key process areas. The hierarchical approach enables organisations to assess their current capabilities and then plot a roadmap for improvement prioritised by those key process areas which will make the biggest impacts on performance.

Regulatory authorities: A public authority or government agency responsible for exercising autonomous authority over some area of human activity in a regulatory or supervisory capacity. An independent regulatory agency is a regulatory agency that is independent from other branches or arms of the government.

Resilience: The positive ability of a system or company to adapt to, or recover itself from, the consequences of a catastrophic failure caused by power outage, a fire, a bomb or similar event.

Return on investment: The ratio of money gained or lost (whether realised or unrealised) on an investment relative to the amount of money invested. The amount of money gained or lost may be referred to as interest, profit/loss, gain/loss, or net income/loss. The money invested may be referred to as the asset, capital, principal or the cost basis of the investment. Return on investment is usually expressed as a percentage.

Risk management methodology: The process or processes for identifying, assessing and prioritising risks, (defined in internal organisation standardisation (ISO) 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimise, monitor, and control the probability and/or impact of unfortunate events or to maximise the realisation of opportunities.

Scalability: The ability of a system, network, or process, to handle growing amounts of work in a graceful manner or its ability to be enlarged to accommodate that growth.

Service-level agreements: Are part of a service contract where the level of service is formally defined. In practice, the term 'service-level agreements' is sometimes used to refer to the contracted delivery time (of the service) or performance.

Service outage: The period when a system is unavailable or fails to provide or perform its primary function. The failure or unavailability can result from an unplanned event, or because of routine maintenance.

Secure sockets layer: A cryptographic protocol that provides communication security over the internet.

Steady state: The state of a system that remains unchanged in a given time frame.

Teleworking: A work arrangement in which employees enjoy flexibility in working location and hours, where the daily commute to a central place of work is replaced by telecommunication links. Many teleworkers work from home, while others, occasionally also referred to as nomad workers or web commuters, use mobile telecommunications technology to work from other locations.

Virtual private network (VPN): A secure way of connecting to a private local area network (LAN) at a remote location, using the internet or any unsecure public network to transport the network data packets privately using encryption. The VPN uses authentication to deny access to unauthorised users, and encryption to prevent unauthorised users from reading the private network packets. The VPN can carry any kind of network traffic securely, including voice, video or data. They are frequently used by remote workers or companies with remote offices to share private data and network resources. VPN's may also allow users to bypass regional internet restrictions such as firewalls, and web filtering, by tunnelling the network connection to a different region.

Annex C: References and useful resources

Standards Australia, recognised by the Australian Government as Australia's peak standards body, has developed the following standards on business continuity management practices.

- HB 221-2004: Business continuity management handbook
- HB 292-2006: A practitioner's guide to business continuity management
- HB 293-2006: Executive guide to business continuity management.

Standards Australia also runs a training program on business continuity management at www.saiglobal.com/training/assurance/instructor-led.htm

Other websites

Australia

Department of Finance and Deregulation, December 2008. Commonwealth Procurement Guidelines: FMG 1, viewed June 2011, www.finance.gov.au/procurement/procurement-policy-and-guidance/CPG/index.html

Australian National Audit Office, Business Continuity Management—Building resilience in public sector entities, viewed May 2011, www.anao.gov.au/Publications/Better-Practice-Guides/2008-2009/Business-Continuity-Management---Building-resilience-in-public-sector-entities

Australian National Audit Office, Business Continuity Management—Keeping the wheels in motion, viewed May 2011, www.anao.gov.au/uploads/documents/Business_Continuity_Management.pdf

Australian Prudential Regulation Authority April 2005. Prudential standard APS 232: Business Continuity Management, viewed May 2011, www.apra.gov.au/adi/Documents/cfdocs/APS-232-Business-Continuity-Management-1.pdf

Australian Reinsurance Pool Corporation 2010, viewed May 2011, http://arpc.treasury.gov.au/

Emergency Management in Australia, Australian emergency manual series, viewed May 2011, www.ema.gov.au/www/emaweb/emaweb.nsf/Page/PublicationsAustralian_Emergency_Manual_Series

Emergency Management in Australia, January 2011, Australian Government Protective Security Policy Framework, viewed June 2011, www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Contents

Trusted Information Sharing Network, IT Security Expert Advisory Group, December 2009. Secure your information: Information security principles for business resilience, viewed June 2011, http://tisn.gov.au/www/tisn/content.nsf/Page/TheTISN_ITSecurityGroup

Trusted Information Sharing Network, IT Security Expert Advisory Group, May 2007. Managing IT security when outsourcing to an IT service provider, viewed June 2011, http://tisn.gov.au/www/tisn/content.nsf/Page/TheTISN_ITSecurityGroup

Trusted Information Sharing Network, Resilience, 2008. Good security—good business, viewed May 2011, www.tisn.gov.au

Trusted Information Sharing Network, Resilience, 2010. Australian Government's critical infrastructure resilience strategy, viewed May 2011, http://tisn.gov.au/www/tisn/content.nsf/Page/Resilience

Chartered Institute of Purchasing and Supply, viewed May 2011, www.cips.org/en-au/Resources/

Standards Australia/Standards New Zealand, International Organisation for Standardization 2009. Risk Management: Principles and guidelines, AS/NZS ISO/IEC 31000:2009, Standards Australia, Sydney

Canada

Disaster Recovery Institute Canada, viewed May 2011, www.dri.ca

New Zealand

Ministry of Economic Development, Emergency Management: Business Continuity, viewed May 2011, www.med.govt.nz/templates/ContentTopicSummary____34023.aspx

United Kingdom

Cabinet Office, Business continuity, viewed May 2011, www.cabinetoffice.gov.uk/content/business-continuity

Business Link. Crisis management and business continuity planning, viewed May 2011, www.businesslink.gov.uk

Centre for the Protection of National Infrastructure. Business continuity planning, viewed May 2011, www.cpni.gov.uk/Security-Planning/Business-continuity-plan/

Continuity Central 2011, viewed May 2011, www.continuitycentral.com/

United States of America

Department of Homeland Security 2011, Ready Business, viewed June 2011, www.ready.gov/business/index.html

Annex D: Remote Access Technology Components

Narrowband landline

Table D1 outlines the narrowband landline channels that can be used in a remote-access solution.

Table D1: Narrowband fixed-line remote-access channels

Technology	Description	Application	Data rates	Charge regime
Public Standard Telephone Network (PSTN)	A modem connected to the computer and the phone line dials the number of the remote-access device in the network (this could be another modem or an access router that enables multiple simultaneous connections) and once authenticated the user is granted remote access to the network and its resources. Before the Internet, all remote access was via dial-up, but with the advent of high-speed internet, significantly faster connections can be made using broadband technology.	PSTN dial-up used for direct dial in to enterprise applications that wish to bypass internet connections for security or functional reasons. PSTN dial-up still used for internet access where ADSL is not available.	Up to 56 kilobytes per second.	Typically, local call rates apply. Long-distance call rates apply where calls are made across charging boundaries.
Integrated Services Digital Network (ISDN)	ISDN technology has been available for a number of years. The name refers to the fact that the services are integrated (i.e. data, voice and fax can all be sent over an ISDN connection), that the service is a digital service, not analog, and that it is a network, not a fixed-line service. ISDN accounts have telephone numbers and so any ISDN subscriber can connect to any other, as can phone users. Telstra currently offers ISDN broadband internet access at a maximum of 128 kilobytes per second.	ISDN dial-up used for direct dial-in to enterprise applications that need to bypass internet connections for security or functional reasons. ISDN dial-up still used for faster internet access where ADSL is not available.	Up to 128 kilobytes per second.	Capped monthly charges. Higher than equivalent ADSL links.

Broadband landline

Table D2 outlines the various broadband landline channels that can be used in a remote-access solution.

Table D2: Broadband fixed-line remote-access channels

Technology	Description	Application	Data rates	Charge regime
ADSL ADSL 2+	This is most common technology for supplying broadband internet over the PSTN. This technology permits the simultaneous transmission of voice and data traffic. It requires that the users have a filter on the phone connections to ensure that the squeal of the data traffic is not heard. ADSL allows for significantly faster data transfer than a dial-up modem, with faster download speeds than upload speeds. ADSL 2+ has higher transfer rates than standard ADSL closer to the exchange. However, the speeds achieved become comparable to standard ADSL as the distance from the exchange increases.	Most common basis of broadband internet connectivity in Australia.	ADSL: up to 8 megabits per second ADSL2+: up to 24 megabits per second.	Low-cost monthly charges. Usage charges may apply depending on the plan.
Cable	This is telecommunications over a physical cable infrastructure. The cables are typically used to carry pay TV and other services. Internet services over this infrastructure are usually at broadband speeds or higher.	This has the same application as ADSL; however, there is a restriction on the coverage of the service. Service deployed in mainland capital cities only.	Up to 17 megabits per second.	Similar to ADSL charge regime though not as many pricing plan options.
Fibre Optic	Fibre optic cable to the node or premise when switched has the ability to deliver high-speed broadband capabilities to the end user, catering for large-volume data transfers and high-bandwidth applications such as video.	Whilst fibre optic connections have been available to large organisations for some time, the number of domestic connections remains low.	Up to 1 gigabit per second.	Charging regime yet to mature.

Wireless

Table D3 (next page) outlines the various wireless channels that can be used in a remote-access solution, noting characteristics such as bandwidth, geographical coverage, applications and comparative cost.

Table D3: Wireless remote-access channel 1

Technology	Description	Application	Data rates	Charge regime
Mobile GSM 2G	2G refers to the second-generation technology for mobile phones. GSM and CDMA are the two variants of 2G technology familiar to Australian mobile phone users. 2G supports SMS and limited data transmission.	Primarily a voice application. Can be used for data transmission.	14.4 kilobits per second.	Low-cost voice based on the corporate plan. High-cost for data applications.
Mobile GSM 2.5G	The term 2.5G was never officially used, but was created as a marketing tool for the improved 2G technologies. These include general packet radio service (GPRS) and enhanced data rates for GSM evolution (EDGE) which support wireless application protocol (WAP) and multimedia streaming (MMS). These protocols allow mobile users to surf the web and send and receive multimedia messages.	Same voice applications as 2G. Data services improved.	Up to 144 kilobits per second.	Low-cost voice based on the corporate plan. Higher cost for data applications.
Mobile GSM 3G	3G technologies enable the provision of voice, mobile multimedia services such as music, TV and video, rich entertainment content and internet access. The technology on which 3G services are delivered is based on a GSM network.	Same voice applications as 2G. Enhanced services such as multimedia and data provided.	Up to 14.4 megabits per second downlink and 384 kilobits per second uplink, with average user speed 250–750 kilobits per second downlink and 40–100 kilobits per second uplink.	Low-cost voice based on the corporate plan. Higher cost for data applications.

Technology	Description	Application	Data rates	Charge regime
Mobile GSM 4G	4G technologies enable the provision of voice, mobile multimedia services such as music, TV and video, rich entertainment content and internet access. The technology on which 4G services are delivered is based on a GSM network.	Same voice applications as 2G. Enhanced services such as multimedia and data provided at higher speeds than 3G.	Up to peak speeds of 100 megabits per second for high mobility communicate-on (such as from trains and cars) and 1 gigabit per second for low mobility communicate-on (such as pedestrians and stationary users).	Due to its infancy, pricing regime is yet to be confirmed.
Worldwide interoperability for Microwave Access (WiMax)	WiMax refers to the IEEE 802.16 wireless standard for delivering high-speed broadband. The service will provide fixed, portable and, eventually, mobile wireless broadband connectivity.	Emerging technology aimed for metropolitan and regional coverage. Complementary to mobile 2G and 3G networks.	Has the capability to deliver services of 5–10 megabits per second at a distance of 10–20 kilometres from a base station.	There are very few WiMax networks in Australia and those operational in Australia offer broadband services with a pricing regime comparable to ADSL.
Wireless fidelity (Wi-Fi or WLAN)	Wi-Fi is a term given to devices that are compliant with the IEEE 802.11 wireless standard. This standard has been widely adopted and the technology is now incorporated in most laptops and handheld devices.	Due to the low power of transmitters the service is restricted to public locations such as cafés, airports, hotels and shopping centres. The application is usually associated with wireless hotspots.	Up to 54 megabits per second.	Low-cost monthly subscription or ad-hoc pay-as-you-go scheme.
Satellite	Used for voice, data and video applications. Some restrictions on applications based on transmission latency.	Used extensively in regional areas where broadband and traditional voice services are unavailable.	1500 kilobits per second download 512 kilobits per second upload.	Initial capital cost + ongoing.

Technology	Description	Application	Data rates	Charge regime
Microwave	Microwave frequencies have been used to transmit data for many years. This is a line-of-sight technology that requires the sending and receiving dishes to be in view of each other. It is often used in remote locations where the installation of cable is prohibitively expensive or difficult.	Applications for microwave can be for backup links between data centres (part of a Disaster Recovery Plan). Typically not used in remote-access from home applications.	Carrier class links.	Initial capital cost + ongoing maintenance and spectrum licences.

Remote-access hardware and software

Remote access to public and private-sector organisations' will be via a combination of hardware and software deployed outside of the traditional enterprise boundaries. The location of this equipment will most likely be a remote-access user's home or alternate work environment, as detailed in the organisation's business continuity plan.

The equipment required to support this element of the remote-access solution can be wide-ranging according to the business services to be accessed. The equipment will range from ubiquitous devices—such as mobile phones—to specialised equipment to support certain business functions—such as financial terminals for the finance and banking industry or process control terminals for critical infrastructure providers.

The selection of remote-access hardware and software technologies should be based on the criteria in Table D4.

Table D4: Remote-access hardware/software considerations

Criteria	Consideration
Suitability	The ability of the proposed solution to adequately support the intended business functions is crucial. For example, if the remote-access solution was based on staff using home PCs then the ability of these PCs to perform the tasks would have to be assessed (operating system, configuration, applications, etc.).
Support	In the event of a remotely-displaced workforce, technical support for the remote-access hardware will be vital. Ease of use and familiarity with the proposed solution should be a major consideration in the design of the remote-access solution.
Cost	The ability of an organisation to provide the required hardware for a proposed solution will have to be determined. For example, if a plan called for supplying staff with laptops to provide remote tasks then the laptops will have to be purchased and maintained prior to an event.
Security	When changing the boundaries of an organisation during a declared event, the confidentiality, integrity and availability of the business functions has to be guaranteed. For example, if the plan called for staff to use their home PCs, are these PCs adequately protected against threats (virus, spy ware, etc.)?

Remote-access hardware

Table D5 (next page) outlines the hardware devices that can be used in a remote-access solution, noting various characteristics and considerations.

Table D5: Remote-access hardware

Technology	Description	Application	Consideration
Laptop	This describes a range of portable computers. They have battery power, attached LCD screens, a variety of external connections, such as card readers, USB ports, super video graphics array (SVGA) connections, a range of built-in wireless technologies and PC Memory Card International Association (PCMCIA) slots.	Laptops use the same operating systems and applications as PCs and are typically equipped with a range of technologies to enable remote access.	The portable nature of these devices makes them prone to loss and theft and the security of the data on the laptop needs to be considered when implementing this technology.
Desktop	This describes a range of PCs consisting of screen, keyboard, peripherals and central processing unit (CPU) case. Usually used at a fixed-location such as home or office. Not portable.	Used in home and office environments'. Lower cost alternative to laptop but without the flexibility.	If home computers are used in a remote-access plan then consideration to compatibility, support and security must be made.
Mobile phone	Mobile phones incorporate most of the features of personal digital assistants (PDA) such as email, contacts and calendar synching and voice note taking.	2G and 2.5G phones are able to be used as modems for remote access, but the speeds are limited. 3G technology will enable broadband internet connections from a mobile phone, and allow the user to surf the Internet from the phone, or to remotely access networks using the internet. Some devices such as a Blackberry are designed for email access to enterprise environments.	
Tablet or smartphone	These are small handheld devices that provide similar access to an organisation's applications as a laptop computer.	Tablets and smartphones are generally GSM, Bluetooth and Wi-Fi-enabled and are able to connect to the Internet, using wireless hotspots and access points, to access applications. They typically have the capacity to act as modems, facilitating remote access to a network.	Security from viruses and malware should be maintained on all devices that will be used to access an organisation's applications.

Technology	Description	Application	Consideration
Modems/ routers	Remote access via modem uses the PSTN or ISDN infrastructure, with a maximum speed of 56 kilobytes per second.	Modems are now usually incorporated into the hardware of PCs and laptops. However, stand-alone modems are still readily available. Where multiple simultaneous modem connections are required, such as an internet service provider (ISP) or remote-access service for an organisation, a device that emulates multiple modems, such as access router, is typically used with an ISDN service.	This technology cannot provide the access speeds that broadband internet can currently provide.
Specialised hardware	Certain business functions can only be processed via specialised hardware. This propriety hardware is typically expensive and has a single function (i.e. cannot be used across a number of business applications such as PCs and laptops)	Proprietary systems such as Bloomberg's financial systems require specific hardware.	Support for these systems may be difficult in the event of a business continuity plan being implemented.

Remote-access software

Remote-access software will be required to work with the hardware platform or platforms selected. In many cases the software comes as part of the hardware solution—such as browsers for operating systems and email client software on mobile phone hardware.

Table D6 (next page) outlines the majority of remote-access software that could be considered in any remote-access solution.

Table D6: Remote-access software

Technology	Description	Application	Considerations
Browser	These applications interpret HTML code and display it as web pages. Such applications are a fundamental component of accessing the internet. They are typically free to use and come as a component of a machine's operating system. Encryption is now incorporated in all browsers, allowing secure transactions over the Internet. Browsers are now used as the user interface for a number of web-based applications such as file transfer and file-sharing applications. Commonly-used browsers include: • Internet Explorer (IE)—Microsoft's browser. IE is included in the Office suite of applications. Netscape—one of the first browsers that was freely available. Mozilla Firefox—a widely-used browser. Opera—it is not as popular or widely used, but includes the functionality of the other browsers. Safari—the most popular browser used in the Apple Mac environment.	Access to web-enabled applications.	Enterprise applications that are not web-enabled cannot be accessed by web browsers. Thin client software or specialised terminal emulation software may need to be considered.
Email client	Email clients such as Outlook or Lotus Notes are widely used in remote computing. These can be configured to access the email servers in a remote network to allow users to access email, while away from their networks. An increasing number of mobile devices are able to access email	Provides access to an organisation's email environment.	An alternative to deploying email clients to remote workers is to implement web-based email access to the organisation.

Technology	Description	Application	Considerations
	remotely using the Internet.		
Thin client	Technology such as Citrix is a widely-used technology for remote computing.	This is a server/client technology that enables access and use of a remote server. This technology allows a client machine to log onto a session on the server. The term 'thin' refers to the small boot image required for a device to be able to access a thin client service. The connection speeds that are now available using the internet allow users to connect directly to the remote network, and work as if connected locally, negating the need to remote control a device that is locally connected to achieve workable response times.	A number of manufacturers produce thin client terminals which are not much more than a keyboard, mouse and screen. Like the remote control software, only keystrokes and screens are transmitted, making this suited to low-bandwidth environments. There are problems with latency and slow response times, and this technology requires servers that are capable of performing the work locally that would normally be performed on the users' PC.
IRC—Internet Relay Chat	These applications are widely used across the internet and include applications such as MSN Messenger.	They allow users to chat in near real-time, and usually include a file transfer capability. Being deployed in enterprises where collaboration across dispersed geographical area is required.	The introduction of this application may introduce security issues.
Specialised software	Access to various enterprise applications may require specialised software such as terminal emulators. Applications such as SAP require a SAP GUI or a connection can be facilitated via a web portal.	Access to legacy applications (green screen) will require specialised emulation software loaded on the remote device.	The deployment of this software on home PCs can introduce support and configuration issues.

Remote-access security technologies

When implementing a remote-access solution, particular consideration must be given to the level of security that would be deployed in any solution. The level of security will be dependent on the threat that the proposed solution will pose to the enterprise assets.

Table D7 (next page) outlines the various security technologies that can be considered in most remote-access applications.

Table D7: Remote-access security technologies

Technology	Description	Application	Considerations
Virtual Private Network (VPN)	A VPN is a common method of establishing a remote connection. This establishes a tunnel or connection between the device and the remote network across the internet. That connection is typically encrypted to provide confidentiality of the data transiting the link, but does not have to be.	A VPN can be implemented in software or hardware, with the hardware solutions recommended for high-load/multiple-user environments. There are many vendors that provide VPN software and hardware. VPN can be based on a number of protocols. The most widely-deployed are internet protocol security (IPsec) and secure sockets layer (SSL).	The VPN protocol and enterprise side hardware will determine scale and performance issues.
Encryption	AES, 3DES, DES are symmetric encryption algorithms. The encryption and decryption keys are held by the two parties involved in the communication and are the same. In effect, the keys are a shared secret. AES and 3DES are DSD approved protocols (DAPs). A list of DAPs is on the DSD website (www.dsd.gov.au). DH, DSA, RSA, ECDSA and ECRSA are asymmetric or public key algorithms. These algorithms are used in public key infrastructure (PKI), in which the public key is publicly available and is paired with a private key that must be kept secret by the owner.	Symmetric algorithms are generally used for file or data stream encryption processes. Asymmetric algorithms are generally used for digital signatures. In a digital signature the owner encrypts a hash of the data with a private key. The encrypted hash is the digital signature. If the corresponding public key is used to decrypt the hash, and the hash is the same as the one generated by the recipient, it proves that the data has not been altered. Proof that the private key belongs to a particular person is done with a similar procedure on the digital certificate. Asymmetric algorithms are also used to encrypt symmetric keys for key exchange operations.	File encryption to be considered for the storage and transmission of data classified above in-confidence in a remote-access environment.
Public key infrastructure (PKI)	PKI links public keys to entities, enables other entities to verify the links and provides for the ongoing management of digital certificates. The major components of a PKI are: • certification authorities (CAs)—which issue and revoke certificates • registration authorities	The main operations and processes of PKI are: • registration—the process of a subscriber making themselves known to the CA directly (or through an RA) • key generation—the generation of one or more key pairs by the CA or by the subscriber • certification—the issuing of a certificate to a subscriber by a CA	

Technology	Description	Application	Considerations
	(RAs)—which verify a potential subscriber's identity and/or attributes • subscribers—certificate holders • relying parties—entities relying on the contents of a digital certificate • subscriber directories—which store public keys, digital certificates or certificate revocation lists (CRLs).	• certificate expiry—specifying the period for which a certificate will remain valid • certificate revocation—the revocation of a certificate before its expiry (e.g. where the private key has been compromised) • CRLs—lists of revoked certificates.	
Authentication	Authentication is the proving of an identity—this is fundamental to security. There are a number of commonly used authentication technologies.	Deployed to authenticate users to networks and devices.	
	Remote authentication dial-in user services (RADIUS)	Widely-used application that provides authentication services for applications and users.	Many ISPs use RADIUS as their authentication technology for remote access to their networks.
	Password authentication protocol (PAP)	This is a very simple authentication protocol. Users are asked for username and password which is then sent in the clear back to the authenticator who responds with an acknowledgement.	As the information is sent in the clear, it can be easily read by anyone who intercepted it, and thus PAP is not considered a secure authentication mechanism. Poor authentication schemes such as PAP may introduce security issues to the proposed design.
	Two-factor authentication	Two-factor authentication, also known as token-based scheme, is based on the security premise of something you know (a PIN) and something you have (a token). When used together this provides a highly-secure authentication regime as the password typically changes every minute.	As this provides the access to the enterprise assets, careful consideration must be given to the authentication scheme implemented.

Technology	Description	Application	Considerations
	Challenge handshake authentication protocol (CHAP)	CHAP uses single factor authentication; in this case it is something you know—a username and password. A three-way handshake process is undertaken after the initial link is set up between the devices. The authenticator sends a challenge to the entity being authenticated. The peer responds with a hashed value, such as MD5, of the requested information which the authenticator compares against the hashed value it has stored. If it matches, the authenticator responds with a notification of the success of the authentication, or terminates the connection if it doesn't match.	
Firewalls	Specific hardware devices, such as Netscreen, Cisco PIX firewalls, Sidewinder G2 and Gauntlet. Firewalls can also be deployed on a server such as Checkpoint. Firewall software can also be deployed on Laptops and PCs. Microsoft XP and Vista come with a Firewall built in. A number of third-party vendors also provide solutions in this area.	Firewalls are configured to restrict access to and/or from one network to another, based on a configured set of rules. These rules permit or deny traffic based on source and destination addresses, ports and applications, and are unique to each implementation. Some firewalls are able to write their own rules to create a dynamic firewall environment, where access through the firewall is configured as needed by applications and users. These firewalls keep a track of and manage all connections through the firewall, allowing traffic related to established and establishing connections, while blocking traffic that is not.	Firewall services (PC-based) for remote users should be considered. The firewall setup should reflect the organisation's policies in this area.

Annex E: Business Continuity Planning Checklist

Checklist questions	Management comments	Business continuity reference	Control exists?	Reference
1. Executive support				
The board and responsible senior management of the organisation must consider business continuity risks and controls as part of the organisation's overall risk management framework.				APRA APS 232, HB 221:2004
Is there senior management commitment for the implementation of business continuity measures?				ITIL SD7
Does the organisation have a formal policy that sets out its approach to business continuity management?				ITIL SD7; APRA APS 232
Have senior management approved the resources needed to implement the agreed strategy and ensured sufficient budgetary and other resources are allocated to allow implementation of the strategy?				ITIL SD7, ANAO BPG—BCM, APRA APS 232, HB 221:2004
Has the business continuity plan been approved by appropriate personnel (e.g. senior management)?				ANAO BPG—BCM
2. Business impact analysis				
A business impact assessment has been performed that identifies, prioritises and documents all business critical processes, resources, corporate systems, and infrastructure.				IT Gov Institute 8, ITIL SD7, APRA APS 232, ANAO BPG - BCM, CobiT DS04, HB 221:2004

Have the minimum availability requirements for each critical business process been determined by the business?				ITIL SD7, ANAO BPG, HB 221:2004
Based on the results of the business impact assessment, have key risks been ranked and mitigation strategies identified that are consistent with the minimum availability requirements?				IT Gov Institute 8
Has the business impact assessment process been validated by senior management?				ANAO BPG—BCM, APRA APS 232
3. Communication				
Is there a formal communication plan in place?				ANAO BPG—BCM
Have the business continuity policies and procedures been effectively communicated to all relevant parties:				KPMG
Does the communication plan incorporate a list of contact names and numbers, including, but not limited to, staff, regulators, customers, counterparties, service providers, market authorities and media? Out-of-hours numbers (including primary/alternate contacts) should be included for all staff with BCP responsibility. The contact list should be reviewed regularly to ensure it is kept up-to-date.				APRA AGN 232.1, HB 221:2004
Does the communication plan clearly identify the staff authorised to deal with the media if the BCP is invoked?				ANAO BPG—BCM, APRA AGN 232.1

Does the communication plan contain a pre-defined message for release, and the means by which messages will be released to each of the stakeholders?				HB 221:2004
Is the contact list related to BCP available to all staff and incorporated in off-site storage arrangements?				APRA APS 232
4. Roles/responsibilities				
Have key roles and responsibilities for business continuity been identified?				ITIL SD7, ANAO BPG—BCM
Senior management must establish clear lines of accountability and reporting for individuals with BCM responsibility that include escalation/notification procedures.				APRA APS 232, ANAO BPG—BCM
Off-site copies of the BCP must be kept by a number of responsible managers who have designated responsibilities in terms of the BCP and should be available at the alternate site(s), if applicable.				APRA APS 232
The composition and responsibilities of the business continuity or crisis management team, or other group that has the authority to invoke the BCP or a separate crisis management plan, must be clearly identified in the BCP and/or crisis management plan. This would include, but is not limited to, an assessment of the impact of the disruption, determining the appropriate response, implementing the communications plan, evacuating staff and activating the alternate site(s), if required.				APRA APS 232

5. Content/framework				
Is there a current, documented BCP?				KPMG, CobiT DS04
Is the BCP part of the emergency management plan?				ANAO BPG—BCM
Is there a single framework for BCPs in place to ensure that all plans are consistent and to identify priorities for testing and maintenance?				ISO/IEC 17799:2000, HB 221:2004
Are procedures developed that are based on applicable business continuity policies?				KPMG
Have plausible disruption scenarios that may lead to short, medium and long-term disruptions to critical business functions been identified and the likelihood of these scenarios occurring, been assessed?				APRA APS 232, ISO/IEC 17799:2000, HB 221:2004
The worst-case disruption scenario that should be considered by an organisation includes, but is not limited to: • loss of precinct • loss of building • denial of access to building for a limited time • loss of IT (data) • loss of IT (voice) • loss of vital (non-electronic) records • loss of key staff (temporary or permanent) • loss of key dependencies.				APRA AGN 232.1

Does the BCP contain the procedures to respond to a material disruption to normal business operations? The procedures should enable the organisation to manage the initial business disruption, recover and resume the critical business functions, resources and infrastructure outlined in the BCP within the nominated time frame.				ISO/IEC 17799:2000, APRA APS 232, HB 221:2004

6. External interdependencies (customers, suppliers, strategic partners, contractors, regulators and competitors)—if applicable				
Does the contract between the organisation and the external party include a requirement that the external party have a BCP and testing program in place and provide for regular, and no less than annual, reporting to the organisation?				APRA AGN 232.1, HB 221:2004
Does the organisation's BCP consider the operational links and interdependencies with the external party's BCP and include arrangements for managing disruptions with the external party?				APRA AGN 232.1, HB 221:2004
7. Alternate sites (if applicable)				
Is the alternate site/sites located at sufficient distance from the primary operational site/sites to minimise the risk of both sites being unavailable simultaneously?				APRA AGN 232.1
Has the organisation ensured that the alternate sites are not on the same power grid or telecommunications network as the primary operational sites?				APRA AGN 232.1
Have transportation arrangements to the alternate site/sites been contained in the BCP? Alternate modes of transport to the alternate site/sites should be considered as a particular mode of transport may be unavailable as a result of the disruption.				APRA AGN 232.1

Where the alternate site/sites have contracted arrangements with a number of other organisations, including other parts of the organisation or its parent's business; the contract between the organisation and the alternate site provider should clearly state the dedicated and shared functional and seating capacity available to the organisation.				APRA AGN 232.1
8. Infrastructure/disaster recovery				
Is there a formal disaster recovery plan in place for critical infrastructure?				APRA APS 232
Has the disaster recovery plan been approved by appropriate personnel?				ANAO BPG—BCM
Does the BCP contain a list of all resources needed to run operations in the event the primary operational site is unavailable? This would include, but is not limited to, computer hardware and software, printers, faxes, telephones, standard stationery and forms. Additional resources include suitably-trained staff and relevant documentation such as insurance policies and contracts.				APRA APS 232; ITIL SD7
Are the technical activities necessary to invoke the contingency measures fully documented, so that personnel can undertake recovery actions?				ITIL SD7
Are backups for major IT facilities performed regularly?				ANAO BPG—BCM
Are the procedures for IT backup documented and approved by appropriate personnel?				ANAO BPG—BCM

9. Training				
Has the organisation’s staff, responsible for disaster recovery continuity plans, been trained in the procedures to be followed in case of an incident or disaster?				IT Gov Institute 8, ITIL SD7, CobiT DS04, HB 221:2004
Have the remaining staff been informed of the actions to take and procedures to follow in the event of the disaster/emergency?				ISO/IEC 17799:2000; CobiT DS04, HB 221:2004
Is business continuity management training organised according to a documented procedure?				KPMG
10. Testing				
Is there a strategy in place to test the relevant plans?				ANAO BPG—BCM, HB 221:2004
Does the organisation ensure that the BCPs are adequately tested, at least annually, and that any deficiencies are addressed within a reasonable period of time?				IT Gov Institute 8; ISO/IEC 17799:2000, HB 221:2004
Are off-site storage and recovery facilities periodically assessed, at least annually, for viability, adequacy and security mechanisms?				IT Gov Institute 8
The results of the testing must be formally documented and reported to responsible senior management and the board or the committee, respectively. Subsequently, the BCP must be amended to reflect any enhancements as a result of the tests.				APRA APS 232, ANAO BPG—BCM, HB 221:2004

11. Update/review				
If so, what are the procedures for reviewing/updating the BCP?				ANAO BPG—BCM
When new requirements are identified are the continuity plans updated as appropriate?				ISO/IEC 17799:2000
Who is responsible for review/update of the BCP?				ANAO BPG—BCM