advanced

White Paper

Guidelines for Maintaining Business Continuity For Your Organisation

Protect your organisation from disruptions and maintain workforce productivity.

This white paper presents a complete approach to keep people productive during planned or unplanned disruptions, including best practices for a complete business continuity strategy as well as technologies to provide secure access to apps and data on any device, over any network or Cloud. By ensuring seamless operations no matter what happens, Advanced's Managed Digital Workplace Services help protect your organisation from consequences such as financial losses, damaged reputation, weakened customer and partner relationships, and lost productivity.

Every organisation faces the possibility of major and minor disruptions of all kinds, from planned events such as IT maintenance and office relocations, to looming emergencies such as hurricanes, snow storms, epidemics or the threat of a pandemic, to unplanned events that strike without warning, such as earthquakes, tornadoes, terrorism, and fires. Even regional incidents from water or power outages to commute disruptions can have a major impact.

While business continuity planning has traditionally focused on planning failover and high availability of mission-critical business systems, this is only part of the picture. To keep the business up and running, organiations must take a more comprehensive approach encompassing both organisational measures and technologies to minimise disruption, maintain security, and support uninterrupted productivity for users and teams. Best practices for a complete business continuity strategy should address team structure, a formal plan, disaster recovery and business continuity testing, crisis communications, and employee safety and awareness programs. All of this should be done jointly with a trusted IT partner, to ensure all operational considerations are taken into account.

Providing users with the experience they need, a secure digital workplace from Advanced can grant users seamless access to business apps and data on any device, over any network. Contextual awareness allows just the right balance of security and flexibility for their current situation, without compromising corporate resources. However, in addition to the technology, perhaps the most important asset to an organisation is having an experienced, trusted advisor like Advanced that knows exactly how to engage in uncertain times.

The Importance of Business Continuity—and the Challenges it Poses

Whether planned or unplanned, business disruptions that aren't managed effectively come at a high cost. Lost revenue, missed sales opportunities, and broken service level agreements can have a devastating financial impact. Disrupted partner relationships and supply chains can delay time-to-market, derail important initiatives, and weaken competitive advantage. An inadequate response can harm the company's public image, as well as the confidence of its customers and investors. Following the disruption, people can find it difficult to regain full productivity due to lost data, interrupted work in progress, and lost collaborative

"The safety and security of our students, staff and community members are paramount. To enable our staff to deliver high-quality education that the University of Sydney is known for, we need to lean on technology that allows us to facilitate the sharing and consumption of knowledge in ways that are safe and secure."

Jordan Catling | Associate Director, Client Technology
ICT University of Sydney

cohesion with teammates and management—not to mention the personal impact the event may have had on them.

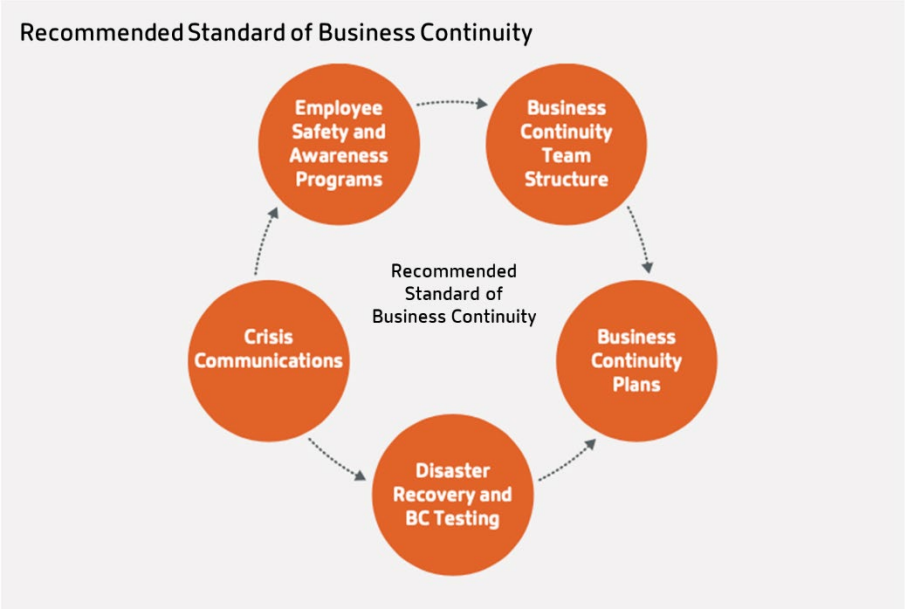
For organisations that run their IT in-house, recovering from a business disruption can be a complex and time-consuming process:

- Bringing the systems back online and restoring any lost data
- Replacing lost or inaccessible devices and ensuring that each can run the user's required software
- Provisioning and configuring applications
- Designing new ways of working and communicating them to users, from alternate network access methods to workarounds for applications which can no longer be accessed
- Accomplishing all of these tasks in the middle of an emergency

Advanced helps organisations develop effective IT business continuity plans, which greatly simplifies and accelerates this process. Powered by Citrix technologies, Advanced's Digital Workplace offering can restore and maintain service to the organisation while getting people back to work as quickly as possible. In events with some advance warning, like a planned office move or anticipated weather emergency, Advanced can even help prevent work in the organisation from being interrupted in the first place.

A Global Approach for Your Business Continuity Strategy

Although each emergency is unique and many decisions will always have to be made on-the-fly, a business continuity plan provides a framework and preparation to guide these decisions as well as a clear indication of who will make them. Successful business continuity programs require executives to play an active role in both developing the plan and ensuring buy-in from the rest of company leadership. With this support, the executives can lead the development of a comprehensive business continuity strategy that encompasses all of the following essential elements.



Team Structure

One of the top considerations for a business continuity plan is the development of a clear decision-making hierarchy. In an emergency, people shouldn't have to wonder who has the responsibility or authority to make a given decision.

The organisation should be able to address all business continuity tasks in every location in which it operates, both to respond to local events and to coordinate the organisation-wide response for both local and broader-based emergencies. Key members of the business continuity team must remain involved in planning and testing throughout the year to ensure that the plan is effective and up-to- date, and to build the familiarity needed to perform under the pressure of an actual emergency.

An organisation's core business continuity team should include executive leaders, a trusted IT service provider or team, facilities, and real estate, as well as physical security, communications, human resources, finance, and other service departments. Individual teams can be dedicated to:

- Emergency response–leads business continuity planning efforts; makes final recommendations to the executive management committee; provides overall direction for preparation, response, and recovery
- Communications–provides communication to all parties including employees, vendors, public service agencies, and customers
- Campus response–prepares property and equipment for the impending disaster event; performs post-event assessment of damage and its impact on continuing operations; assists with insurance claims; secures buildings and grounds
- Business readiness–acts as a liaison with individual business unit teams; makes arrangements to implement disaster business operations for each unit; provides tactical response and business direction

"We try and make it so it doesn't matter if they [employees] are sitting in their office or in their home or in a hotel or on an airplane, as much as possible, to be able to feel like it walks and talks and it feels like their desktop."

Sarah Vogt | Remote Systems Engineer
Greenberg Traurig, LLC

Each of these teams should report into the executive management committee.

Business Continuity Planning

At a high level, a business continuity plan should identify potential business disruptions that can affect any of an organisation's locations, such as power outages, epidemics, pandemics, and fires, as well as those that are specific to individual locations, such as earthquakes and tsunamis in a seismically active region or civil unrest in politically unstable areas. Planning extends throughout the supply chain as well, including reviewing the business continuity strategies for key vendors, identifying potential risks of operational outages, and evaluating alternatives. To keep the number of scenarios manageable, planning should be based on worst- case scenarios, rather than multiple graduated versions of each incident.

It won't always be possible to maintain normal operations in an emergency situation. To mitigate the impact of reduced capacity, the team should identify which operations are most essential, who will perform them, and how work will be redirected if necessary. We recommend that this is handled by a team of business

unit owners with a business continuity analyst. This group would work together to rank the criticality of various business processes in terms of revenue, customer-facing and brand image concerns, regulatory implications, and other business considerations, then map dependencies onto these processes in terms of the applications, people, facilities, and equipment required to support them. Based on this analysis, the group can identify recovery strategies and costs around continuing each process. For your IT provider like Advanced, this data provides a framework for making sure that critical applications will be available to the business within an established recovery time objective (RTO) and recovery point objective (RPO).

Testing

A business continuity plan is only as good as you keep it. Without an ongoing focus on preparedness, an organisation can find that when emergency strikes, its plan is no longer relevant to its business or operations, which will cause it to grapple with an ad hoc response made worse by a false sense of security.

"We want to get to a stage where employees understand that everything they need to carry out their work can be accessed."

Kyle Edgeworth | Deputy CIO
City of Corona

Best practices call for annual updates of a business continuity plan to reflect changes in the criticality and dependency of applications, business priorities, risk management, business locations, operations, and other considerations. We recommend that business continuity personnel track and note such changes throughout the year to supplement this annual review. Full emergency simulations should be conducted at least annually as well. These guidelines, along with an annual review of all plans and crisis communication testing, should be considered the minimum baseline. Ideally, organisations and their IT service providers should perform quarterly business continuity and recoverability testing for all mission-critical applications. Tabletop exercises introduce new twists to ensure the flexibility of the plans in place and give team members experience responding to the unexpected.

Crisis Communications

A formal crisis communications program can make the difference between panic and smooth emergency response. The plan should identify all the stakeholders for emergency communications, including employees, contractors, clients, vendors, media, and executive management. The organisation's communications tool kit should include internal and external resources such as telecom, email, public address, intranet, IM, texting, and the company website. The communications team should work to convey a consistent message on the company's behalf via external channels such as press releases, social media updates, and interviews with spokespeople. Sample emergency messages can be drafted in advance, tailored to specific audiences and modes of communication; these can be updated quickly during an actual emergency to reflect current conditions.

Employee Safety

Keeping people safe should be the top priority in any emergency response. There are many ways to develop an employee safety program. Local agencies such as the Red Cross, fire department, and police department, as well as federal entities, can provide training and guidance for your program. Tabletop exercises can help you develop and refine the right procedures to fit your workforce, facilities, and locations. Once your program is in place, it should be included in new employee orientation and reviewed regularly with all employees. Emergency evacuation procedures should be reviewed and tested frequently, and employees should know where to find business continuity documentation. During an emergency, pay careful attention to peoples' stress levels and make sure they are allowed ample time to sleep, eat, and relax.

Table 1	Business Continuity Planning Checklist
Business continuity team structure	• Secure executive buy-in • Form core business continuity team
Business continuity planning	• Create business analysis team • Develop disaster scenarios • Define decision-making hierarchies • Prioritise recovery per business considerations • Map recovery goals to dependencies • Develop data center continuity strategy • Develop workforce continuity strategy • Scaling up/out based on the severity of the situation
Disaster recovery/business continuity testing	• Update plans regularly* • Test recoverability of mission-critical applications* • Perform tabletop exercises and walkthroughs*
Crisis communications	• Establish formal crisis communication program • Identify stakeholders for emergency communications • Identify key internal communications channels • Draft sample communications
Employee safety and awareness programs	• Develop programs through tabletop exercises and emergency response training by local agencies • Incorporate safety and awareness into new employee orientation • Review and test emergency evacuation procedures

Workforce Continuity: Enabling Uninterrupted Access to Business Resources

High availability infrastructure design between on-premises and Cloud can keep IT operations up and running—but what if people have been displaced from their usual workplace, or have lost access to their usual devices or systems? A complete and effective business continuity program has to encompass not only the data center, but the workforce as well. If people can't do their jobs, the business can't function.

While business continuity has traditionally revolved around a designated alternate workplace or recovery unit, organisations increasingly use business mobility tools to enable people to work wherever it's most convenient and effective. People who need to work at the disaster site itself, such as business continuity team members, emergency response workers, critical service workers, and others such as insurance adjusters, can be housed in any available structure or mobile unit, without the need for special infrastructure or complex connectivity.

With Advanced's Managed Services, the same secure digital workplace technology lets people connect with apps and data in both routine operations and emergency situations, using any device, network, or Cloud. This makes it simple for people to do whatever their priorities dictate—whether to continue working normally, perform new tasks required by the event, or focus on the needs of their families and themselves, then resume work as circumstances allow. Instead of having to get PCs that meet certain specifications, configure them, provide access to the applications, organisations are able to shut down an office, move people to another location and get them back to work in the same familiar environment quickly. This allows for the exact same user experience. With Advanced's Managed Services, an in-house IT team doesn't have to worry about imaging dozens or hundreds of machines, then guiding people through a long list of changed processes.

Staying engaged with an expert IT service provider, even outside of emergency situations, yields important benefits, including:

Efficiency and cost savings. Making mobility and remote access core elements of business continuity planning lets an organisation increase the value of these investments while eliminating many separate business continuity processes and costs.

A seamless experience for people. Because people access and use their resources the same way they always have, with the same secure digital workspace experience in any scenario, there is no need for alternate procedures to be learned or remembered.

Security and compliance. During a business continuity event, data and apps are delivered using the same infrastructure as for routine operations, with the same inherent security. Windows applications remain under the IT provider's on-premises, Cloud, or hybrid Cloud infrastructure, where automation and centralised management enhance policy enforcement, regulatory compliance, and antivirus protection. Similarly, users can securely access sensitive business apps and data from any device in any location while enabling the IT service provider to maintain complete control, tracking, reporting, and auditability to aid security and compliance. Data delivered to mobile devices can be secured and controlled through mobile device management (MDM), while applications can be secured and controlled through mobile application management (MAM). End-to-end encryption provides an additional layer of protection as people access business apps and data over any network, from any location.

More practical, lower-risk execution. Organisations can invoke their business continuity plan with less disruption to users and the business. As a result, the

organisation is often more willing to take this measure proactively—to move people offsite in advance of a hurricane or snowstorm, to have them work at home during an epidemic, or even to evacuate to a different city in the case of an especially large-scale impending disruption—rather than taking its chances and hoping the disaster will pass without impacting the business. The plan becomes much more effective when it is seen as an acceptable adjustment to circumstances rather than a last resort to be invoked only in the most desperate times, or at the last possible moment.

Ensuring Workforce Continuity with Citrix Technologies

With a secure digital workplace, Advanced's Digital Workplace offering powered by Citrix helps organisations ensure continuity of operations during business disruptions. Industry-leading Citrix Workspace technologies enable Advanced to securely deliver all apps—Windows, web, SaaS, and mobile— as well as data and services from any device, over any network or Cloud. Citrix and Advanced support workforce continuity through comprehensive technologies that simplify security operations and reduce risk in the following key areas.

Contextual Access

Instead of worrying about special access methods, Advanced can allow users to access their secure digital workplace the usual way over any available connection. Users can connect from company LAN or WAN, consumer broadband, satellite, public hotspot or mobile with full security, access control, and compliance monitoring and tracking.

People who have lost access to their usual work device can connect to a secure digital workspace, including all their familiar business apps, using any available device - even newly purchased devices or an old personal device, including Windows and Mac desktops and laptops, iOS, Android and Windows-based mobile products, and Google Chromebooks.

Application Security

Because apps and data are managed within Advanced's data centres or Cloud, data protection, compliance, access control, and user administration is centralised, and can be just as easily applied on personally owned, borrowed, or newly purchased devices as on corporate-owned endpoints—within the same unified environment.

Data Security

Advanced's and Citrix's Content Collaboration enables users, teams, and customers to access sync and securely share files from anywhere, on any device. Routine document workflows such as approval chains and electronic signatures can be automated to keep business processes running smoothly even in unusual circumstances. Policy-based control, reporting, data encryption, remote wipe, information rights management (IRM support), and data loss prevention (DLP) integration help keep business content secure when business disruptions occur.

Together with Citrix technologies, Advanced helps business continuity planners address the two essential considerations for users:

- Can I still access my applications, data, and files, and collaborate effectively with others inside and outside the organisation?
- Does everything still work the same way as usual, or do I need to adjust to an unfamiliar device, network access method, and set of tools?

Operational Continuity: Maintaining Continuous Access

Organisations that revolve around traditional desktop PCs for primary access to data and resources are often at a disadvantage when it comes to responding to unexpected events. With remote PC access, Advanced's customers can rapidly access individual machines inside their physical workplace. In an unexpected event, Advanced can quickly deploy an MSI package to desktop PCs and give users secure access to those devices from anywhere.

Automation and Recovery

Citrix solutions help Advanced ensure that resources remain available with tools for managing comprehensive site-wide disaster recovery, including live migration to move workloads from one physical server to another, and automated high availability, which redistributes virtual machines from a failed host to other physical hosts and restarts them to protect critical workloads from localised events.

Conclusion

The essence of business continuity is to minimise the impact of disruptions on people and the technologies they rely on. In the past, organisations have had to rely on alternate work methods and locations in such situations, forcing people to adapt to unfamiliar ways of working at the same time they're coping with the stress and uncertainty of the event itself. Advanced advises and helps organisations implement a more seamless and holistic approach, allowing people to work exactly the same way during an emergency as they would on any other day. Comprehensive technologies for contextual access to network, application, and data security enable people to become fully productive on any device, over any network or Cloud, in any location, while helping IT ensure uninterrupted security and control. On the back end, automation and recovery keep IT resources available, while real-time monitoring, detection, and analytics help ensure a good user experience, maintain compliance, and prevent breaches. By leveraging everyday infrastructure, this approach also eliminates the need for separate business continuity access tools and devices, reducing the cost and complexity of business continuity planning.

Advanced assess, advise, assist, secure and operate your digital workplace, wherever you are in your journey. Our Managed Digital Workplace Services are dedicated to helping to modernise and optimise the workplace while improving security and compliance. We provide expert advice, navigating the breadth of

vendor offerings to design, migrate, support and manage your solution's lifecycle. We're committed to unburdening our customers to get the best for your workforce. We support the needs of your diverse digital workplace via a portfolio of flexible, standard services. Our experts help the creation of a secure and innovative workplace that better enables your workforce to evolve.

This is not a one-time technology implementation; it is an introduction of ongoing management and change in leadership, process, practices, systems, culture, education and behaviours. Our customers are in a range of sectors including Health & Care, Government, Legal and Financial Services. This means that we understand how to manage these changes in a range of different areas, ensuring success for all.

Secure digital workplaces are transforming the way organisations around the world enable users and empower the business. By incorporating Advanced's Managed Services and advice into your business continuity strategy, you can protect your organisation far more effectively against the risks posed by planned and unplanned disruptions.

To learn more visit Advanced's website and fill in a contact form.

About Advanced

From desktop to data centre, our experts can securely manage your IT needs. Our comprehensive range of Managed Services can be tailored to your requirements. We can support individual applications through to your entire infrastructure environment, utilising a choice of platforms including Cloud. Adopting our Managed Services provides an efficient way to stay up-to-date on technology, have access to expert skills, dedicate more time to your business aligned IT strategy and address issues related to IT cost.

Our Managed Digital Workplace Services allow IT leaders to focus on strategic activities, while improving security, agility and innovation. We follow four key principles: provide security and end user focused services that can be trusted; 'as-a-Service' delivery with modern lifecycles management that enables you to stay current, compatible and secure; support the UK Government Code of Practice; provide innovative solutions with a high quality managed service experience.

Our operations are aligned to ITIL and PRINCE2 best practices, as well as accredited to ISO 14001, 9001 and 27001 standards. The 24x7 management and monitoring that we have provided to a variety of organisations across numerous sectors for more than 15 years, has seen us achieve a 96% customer satisifcation rate with more to come.

We're committed to delivering value through operational services, optimisation consultancy and transformative digitisation.

We're here to help.

Powered by