CITRIX®

White Paper

Guidelines for Maintaining Business Continuity For Your Organization

Protect your business from disruptions and keep your 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, Citrix Workspace solutions help protect your business from consequences such as financial losses, damaged reputation, weakened customer and partner relationships, and lost productivity.

Every organization 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 and epidemics, to unplanned events that strike completely without warning, such as earthquakes, tornados, terrorism and fires. Even relatively small incidents like a water or power outage, commute delays and the seasonal flu 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, organizations must take a more comprehensive approach encompassing both organizational measures and technologies to minimize disruption, maintain security, and support uninterrupted productivity for users and teams. Best practices for a complete business continuity strategy should address business continuity team structure, business continuity planning, disaster recovery and business continuity testing, crisis communications, and employee safety and awareness programs.

Providing users with the experience they need, a secure digital workspace can grant seamless access to business apps and data on any device, over any network, hosted on-premises or in a public cloud. Contextual awareness allows just the right balance of security and flexibility for their current situation, without compromising corporate resources. Analytics and insights help IT maintain security, compliance, and threat protection wherever and however people work

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

"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."

Stan Black | **Chief Security and Information Officer** | **Citrix**

For IT, 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

An effective business continuity plan greatly simplifies and accelerates this process, helping IT restore and maintain service to the organization 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, the organization can even prevent their work 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, security and IT teams can lead the development of a comprehensive business continuity strategy that encompasses all of the following essential elements

.

"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

Citrix Standard of Business Continuity

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 organization 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 organization-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.

At Citrix, a core business continuity team for each region includes executive leaders, IT, facilities, and real estate, as well as physical security, communications, human resources, finance, and other service departments. Individual teams are 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

Each of these teams reports into the Citrix 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 organization'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.

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

Kyle Edgeworth | Deputy CIO
City of Corona

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. At Citrix, this is handled by a team of business unit owners with a business continuity analyst. This group works 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 IT, 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 organization 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.

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. At Citrix, 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. Citrix performs 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 organization'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 such as the FEMA Community Emergency Response Teams (CERT) in the United States, 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 analysisteam • Develop disasterscenarios • Define decision-making hierarchies • Prioritize recovery per business considerations • Map recovery goals to dependencies • Develop data center continuity strategy • Develop workforce continuitystrategy • 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, organizations 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.

At Citrix, the same secure digital workspace 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, we 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. IT doesn't have to worry about imaging dozens or hundreds of machines, then guide people through a long list of changed processes.

This approach yields important benefits, including:

Efficiency and cost savings. Making mobility and remote access core elements of business continuity planning lets you 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 IT controlled hybrid cloud infrastructure, where automation and centralized 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 IT to maintain complete control, tracking, reporting, and auditability to aid security and compliance. Data delivered to mobile devices is secured and controlled through mobile device management (MDM), while applications are 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. Organizations can invoke their business continuity plan with less disruption to users and the business. As a result, the organization 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.

Headquartered in Ft. Lauderdale, Florida, Citrix has ample firsthand experience with business continuity events. Citrix has relocated individuals to hotel conference rooms, shifted workloads around the world based on closed facilities, and rapidly increased capacity in other areas based on potential disasters. Citrix has done this it many times, especially during the Florida hurricane season. The services provided both internally and

externally to customers have never been affected due to the workforce flexibility enabled by Citrix technologies.

Ensuring Workforce Continuity with Citrix Technologies

With a secure digital workspace, Citrix helps organizations ensure continuity of operations during business disruptions. Industry-leading Citrix Workspace solutions enable IT 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 supports 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, IT can allow people to access their secure digital workspace 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. Citrix Gateway (formerly NetScaler Gateway) provides a unified management framework for IT to secure, control, and optimize access to apps and data on any device, using any network or cloud.

People who have lost access to their usual work device can connect to their secure digital workspace, including all their familiar business apps, using any available device. Download Workspace app onto 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. Inside Citrix Workspace, users have single-click access to enterprise mobile, web, SaaS, custom and Windows apps, including integrated file sharing and productivity apps.

Application Security

Windows app and desktop virtualization powered by Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) lets IT transform Windows apps and complete desktops into on-demand services delivered securely to digital workspaces on any device, in any location. Because apps and data are managed within the data center or cloud, IT maintains centralized data protection, compliance, access control, and user administration as easily on personally owned, borrowed, or newly purchased devices as on corporate-owned endpoints—within the same unified environment.

Mobile devices can play an especially important role keeping users connected with the business during a disruption. Citrix Endpoint Management (formerly XenMobile) enables identity-based provisioning and control of apps, data, and devices, as well as automatic account de-provisioning and selective wipe of any devices that have been used

temporarily during a business continuity event. Business apps and data, whether developed by IT or a third party, and included enterprise-grade mobile productivity apps, reside in a container separated from personal apps and data on the device.

Data Security

Citrix Content Collaboration (formerly ShareFile) enables users, teams, and customers to access sync and securely share files from anywhere, on any device. IT can easily grant access to existing corporate data repositories without compromising security. Routine document workflows such as approval chains can be automated to keep business processes running smoothly even in unusual circumstances. Flexible storage options, 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, these Citrix technologies help 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 organization?
- 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?

Datacenter Continuity: Maintaining Continuous IT Operations

Most large organizations already operate in a hybrid cloud model and have more than one data center while also taking advantage of the cloud for scale and redundancy. If one data center or cloud comes offline for any reason—planned or unplanned—people should be able to access resources via another data center or cloud resource, either active or backup, until the affected data center or cloud comes back online. It's important to make sure that the associated infrastructure can support this response, from rapid, automated failover to load balancing and network capacity.

Organizations 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 Citrix Remote PC access, Citrix Virtual Apps and Desktops customers can rapidly enable access to individual machines inside their physical workplace. In an unexpected event, admins can quickly deploy an MSI package to desktop PCs and give users secure access to those devices from anywhere.

User Continuity

Ideally, your IT department has deployed a solution that offers the same end user experience regardless of physical location. Citrix Workspace with intelligent features expands the users' ability to be productive from anywhere. Having an intelligent feed of action items on any device keeps individuals moving forward, even in times of unrest.

Network Security

Citrix ADC (formerly NetScaler ADC) and Citrix SD-WAN (formerly NetScaler SD-WAN) make data center failover seamless for users. If the primary data center goes down, Citrix ADC redirects users automatically and transparently to the secondary site while continuing to perform load balancing and global load balancing. Citrix ADC also allows organizations which use a public cloud for backup to manage this outsourced infrastructure the same way they would their own backup data center. Citrix SD-WAN lets IT connect and accelerate applications, optimize bandwidth utilization across third-party public cloud and private networks, and gain visibility into application performance to optimize the user experience in any scenario.

Automation and Recovery

Citrix solutions help IT ensure that data center resources remain available. Citrix Hypervisor (formerly XenServer), the industry leading platform for cost- effective cloud, server, and desktop virtualization, provides 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 localized events.

Citrix Cloud services aid resiliency by providing a single dashboard for IT to manage resources in multiple enterprise data centers, public clouds, and private clouds. IT can easily reassign users to alternate sites as needed to reduce the load on challenged resources and ensure performance and availability. Citrix Cloud services run on a highly available, globally distributed platform designed for continuous operation regardless of local disruptions.

Analytics & Insights

A business continuity scenario can greatly alter the distribution of users and workloads across network infrastructure, making it especially important to monitor performance to ensure a good experience for every user. At the same time, IT must remain vigilant for security threats so that an ongoing disruption does not create opportunities for hackers. Citrix solutions including Citrix ADC, Citrix Application Delivery Management (formerly NetScaler Management and Analytics System), and Citrix Virtual Apps and

Desktops provide full visibility into your IT infrastructure, with real-time analytics to detect threats, misconfigurations, and performance issues.

Citrix Analytics for Performance and for Security give real time and actionable insights to ensure your environment is running as smoothly as possible. Having detailed information on what each user is experiencing gives IT the agility to offer more resources to an individual having a less than optimal experience.

Conclusion

The essence of business continuity is to minimize the impact of disruptions on people and the IT resources they rely on. In the past, organizations 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. Citrix supports 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 IT 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.

Secure digital workspaces are transforming the way IT organizations around the world enable users and empower the business. By incorporating Citrix solutions into your business continuity strategy, you can protect your organization far more effectively against the risks posed by planned and unplanned disruptions.

To learn more visit https://www.citrix.com/virtual-apps.