# Business Continuity Planning

## Best practices to weather any storm

# Business Continuity Planning Provides Organizational Resilience

Unplanned disruptions can adversely affect the operations of any organization, no matter the size, putting it and its stakeholders at significant risk. Fortunately, strategic investments and scenario planning can give your organization a competitive advantage over those who are unprepared for a variety of contingencies. Business Continuity Plans (BCP) are an important part of risk management and can include scenarios such as pandemics (like COVID-19), government shutdowns, natural disasters and cyberattacks. In an era of devastating cyber breaches and unprecedented political rancor, the financial health and mission success of any organization depends on its preparation to weather almost any storm.

## Is Your Organization Risk Ready?

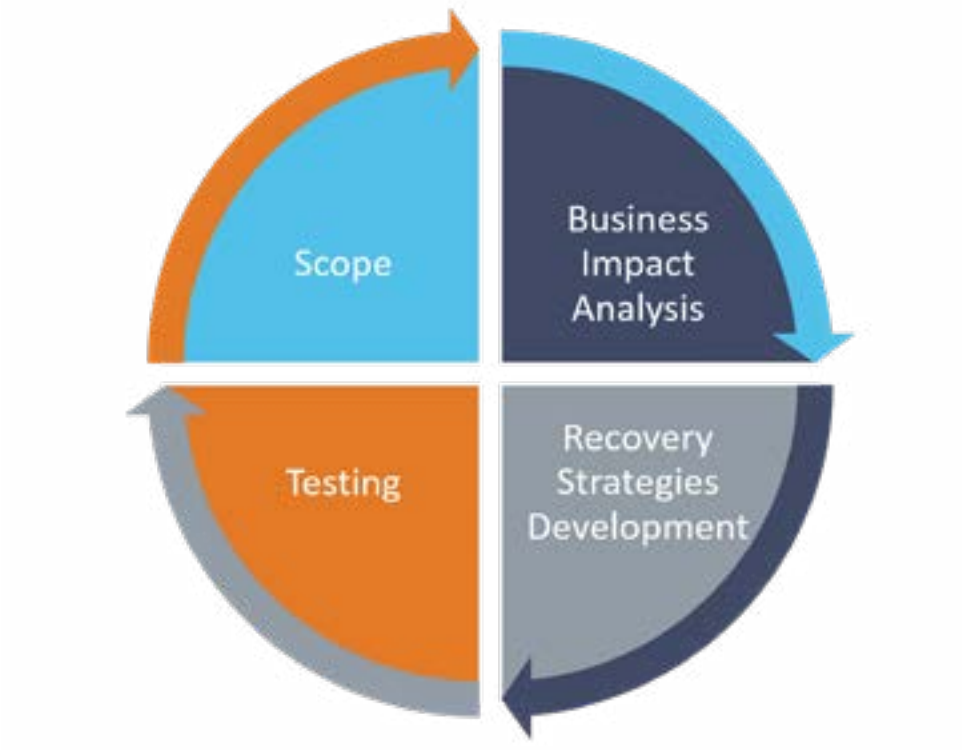
The BCP helps organizations determine the best course of action when a business disruption occurs. When well thought-out and readily available, a BCP allows an organization to continue operations and avoid situations that could potentially bring operations to a screeching halt. Even small organizations should form a team responsible for overseeing the BCP plan and meet at least quarterly to plan for significant risk events and the appropriate responses.

### Example Emergency Planning and Response Policies

- Salary Continuation
- Crisis Counseling
- Travel Policy
- Key Staff Succession Policy
- Natural Disaster Business Continuity Plan
- Pandemic Continuity of Operations Plan
- Emergency Lockbox
- Communication Policy
- Evacuation Policy

## Components of Business Continuity Planning

When properly developed, BCPs have four equally important components:




### Scope

When scoping the BCP, it is important that the organization has all stakeholders provide their operational requirements for the organization. Having stakeholders engaging in the BCP requirements allows them to identify aspects of the organization that need to continue to operate at a high level during a disaster scenario. In addition to those identified by stakeholders, the BCP or risk team should also identify which critical products and/or services the organization provides.

With the requirements and critical products and/or services established, it is also important to understand the organization's risk appetite (the level of risk an organization is willing to take on). The risk appetite for top-level stakeholders may differ from department specific stakeholders. The organization's overall risk appetite may significantly increase or decrease the costs of a disaster recovery plan.

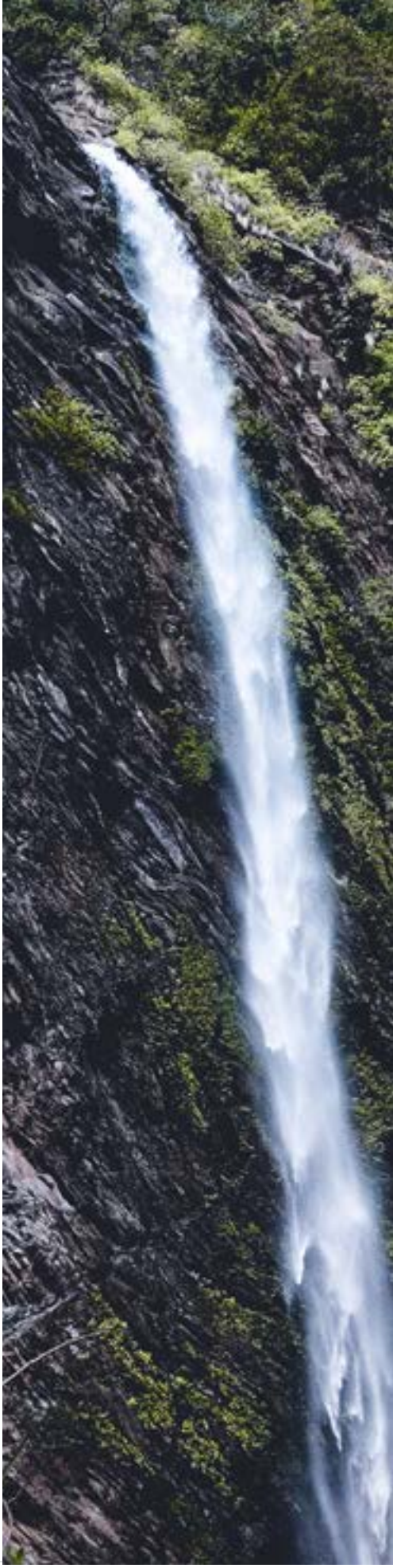
For example, consider preparation for an unplanned office closure due to a water main break. The affected organization should speak with each department head during BCP scoping to be sure the organization is fully operational while employees work remotely. During this process, the organization may discover that the organization's sales software is only accessible while employees are physically logging in from the office. With this information, the organization can proactively expand the number of VPN licenses to provide access to employees who utilize the sales software.

## Business Impact Analysis (BIA)

The BIA is broken down into three components:


Identifying Critical Assets/Processes involves elaborating on the products/services that were identified in the scope of the BCP at a more granular level. With critical assets and processes identified, the risk assessment lists the threats and vulnerabilities related to those assets/processes, assess the impact and likelihood for each combination of assets/threats/vulnerabilities, and calculate the level of risk. Following the risk assessment, the organization can determine its maximum tolerable downtime (MTD). MTDs can vary by asset or process, or the organization can adopt one MTD standard, determined by the risk assessment and the organization's risk appetite.

Continuing with the VPN license example, the organization should calculate the cost associated with the additional licenses as well as the cost of lost productivity from failure to access the sales software. As part of the analysis, the organization may also want to consider the cost of reallocating some of the existing VPN licenses from other employees.



## Recovering Strategies Development

The development of recovery strategies is where the rubber meets the road. The BCP or risk team brainstorms and identifies specific recovery strategies for business disruption events based on the results of the risk assessment. Team composition is important because it should include participants from different departments within the organization. Their job is to provide insights on the impact of adverse events on the assets and processes identified and help develop appropriate business continuity and IT disaster recovery procedures. Once the plan and procedures are developed, the team should share the BCP with management for buy-in prior to testing.

Considering the scenario again, the organization deliberating the expansion of VPN access may decide that they will not purchase additional licenses. Their recovery strategy would involve identifying who among existing VPN license holders will lose their access and who will receive the reallocated licenses.

### In The News

Risk management planning for a possible pandemic involves identifying risks, assessing their impact and developing mitigation strategies to manage them. Most organizations refer to preparedness standards and guidelines like the FEMA Pandemic Influenza Continuity of Operations Template to assist them in developing a Pandemic Influenza Continuity of Operations Plan.

## Testing

Testing the BCP not only determines if everything works as designed, but also allows the organization to train staff on their roles and duties as described in the BCP and disaster recovery procedures. It can include simple tabletop exercises to full-blown planned outages to determine how staff will react and respond. The testing phase will determine whether the implemented strategy for the specific event is a success. If successful, the strategy should be monitored over time to keep pace with any changes in staff or processes. Failed strategies may require minor adjustments or a complete replacement.

It may be difficult to identify all possible scenarios for a BCP without prior experience on behalf of individual team members or the organization. Without direct experience with business disruption, the organization should dedicate time and resources to researching best practices for addressing possible scenarios and implementing mitigating tactics. Third party companies who specialize in this area are also an option. Many have experience in a broad range of industries and help organizations develop BCP and mitigation plans to avoid business disruption based on proven methodologies.

### Testing (Continued)

In the example, once a decision is made regarding the purchase or reallocation of VPN licenses, the employees receiving the new licenses must be trained, especially if they have not logged into a VPN software in the past.

## Key Takeaways

To enhance your organization's operational resilience, consider these key activities at a minimum:

- Identify your organization's core services
- Compile a list of the essential tasks necessary to keep your operations going
- Identify staffing arrangements such as telecommuting and succession planning
- Perform an analysis of organizational threats
- Assemble and provide easily accessible contact and resource information for employees
- Develop instructions for employees detailing where they should go in the event of a disaster
- Outline the steps necessary to protect the health of your employees
- Delineate how the plan will be tested and updated
- Understand your regulatory and reporting compliance requirements

## GRF CPAs & Advisors' Risk and Advisory Services

GRF CPAs & Advisors (GRF) offers clients valuable industry experience combined with proven best practices to help organizations identify risk scenarios and provide guidance for effective mitigation strategies. With GRF's industry insights and deep bench of resources, our Risk and Advisory Services (RAS) practice helps clients protect their critical assets and safeguard their mission.

## Additional Resources

- Best Practices in Enterprise Risk Management
- Why Associations are Implementing Enterprise Risk Management
- Enterprise Risk Management for Nonprofits & Associations: Where Strategy Meets Risk
- Be Prepared: Why Enterprise Risk Management is Essential for Nonprofits
- Internal Audit is a Critical Investment for Nonprofit Organizations
- Vulnerability Scanning and Penetration Testing Offer Tools for a Strong Security Posture

## Authors


### Melissa Musser, CPA, CITP, CISA

Principal

mmusser@grfcpa.com
O: 301-951-9090
T: 877-437-4771



### Darren Hulem, CISA, Security +, PCIP

Network Adminstrator Auditor

dhulem@grfcpa.com
O: 301-951-9090
T: 877-437-4771


## About GRF CPAs & Advisors

Our risk experts work with organizations to provide support for complex decision-making over a wide range of business and financial issues.

Services include Enterprise Risk Management (ERM), third-party risk assessment, internal audit, cybersecurity, privacy, fraud support, compliance consulting, and financial systems optimization. For more information on how our experts can support your organization, visit our website at **https://www.grfcpa.com/accounting-services/advisory-services/**.

Headquartered in the Washington, DC metropolitan region serving clients locally, nationally and around the world. GRF CPAs & Advisors is a full-service professional services firm providing clients with audit, accounting,