

## A Collaborative Approach to Business Continuity Planning

Written by: Gus Morales, Principal Analyst, Security and Safety, Gannett Fleming

### STRATEGIES FOR RISK MANAGEMENT FOR INFRASTRUCTURE

Cybercrimes cost more than \$9.5 trillion in 2024, underscoring the urgent need for business continuity planning. Can your enterprise survive an attack? Do you have plans and policies in place to maintain your critical infrastructure?

In today's ever-changing world, organizations must be prepared to maintain business operations in the face of unpredictable events. Natural disasters, cyberattacks, and business disruptions are constant threats. Critical infrastructure business continuity planning (BCP) prepares organizations to restore services swiftly to meet public needs despite disruptions. Let's explore critical infrastructure BCP components and actionable strategies to enhance your organization's resilience.

### Understanding Business Continuity Planning

BCP establishes a framework that enables organizations to continue or quickly resume operations after disruptions. The goal is to maintain uninterrupted services by safeguarding critical systems and preparing effective recovery strategies.

A well-executed BCP involves three primary stages:

- » **Stage 1:** Start by recognizing critical business functions, such as emergency communications, road maintenance



systems, and utility delivery. These systems are vital for public safety and daily operations.

- » **Stage 2:** Conduct a thorough risk analysis to pinpoint potential vulnerabilities, including examining physical and cyber threats.
- » **Stage 3:** Formulate clear, actionable strategies, including identifying alternative sites and backup systems and defining procedures.

### Key BCP Components

BCP involves four sequential components, each integral to maintaining infrastructure resilience. The National Institute

of Standards and Technology (NIST) provides comprehensive guidelines for developing, implementing, and maintaining effective contingency plans for critical infrastructure in its NIST SP 800-34 resource.

### **BUSINESS IMPACT ANALYSIS**

A business impact analysis (BIA) helps organizations assess risks, identify critical systems, and establish acceptable downtime limits. The BIA also defines recovery time objectives (RTO) and recovery point objectives (RPO) to determine how quickly and in what quantity data can be restored after an incident.

### **BUSINESS CONTINUITY PLAN**

A business continuity plan outlines strategies and procedures for determining how critical business functions will continue during and after disruptions. Focus areas include maintaining operations, protecting essential systems, and minimizing downtime.

### **CONTINUITY OF OPERATIONS PLAN**

A continuity of operations plan, using input from either the business continuity and/or disaster recovery plans, provides a detailed framework for maintaining essential functions during emergencies, emphasizing operational resilience.

### **DISASTER RECOVERY PLAN**

Disaster recovery plans establish procedures for restoring services after an incident, articulating recovery steps, identifying team responsibilities, and defining communication protocols. Key elements include data backup and restoration plans, alternative operational sites, and recovery strategies that align with RTO and RPO.

---

## **Seven Steps to Comprehensive BCP Development**

---

Creating an effective BCP requires a structured approach that addresses preparation, response, and recovery, and involves seven key steps:

- 1. Develop a Contingency Planning Policy:** Begin with a contingency planning policy that aligns with statutory and regulatory requirements. This groundwork helps organizations meet federal, state, and local guidelines.
- 2. Conduct a BIA:** Identify critical functions and determine acceptable downtimes. By analyzing operational impacts, enterprises can prioritize which systems require immediate attention.
- 3. Implement Preventative Controls:** Deploy preventative controls to mitigate identified risks, including network security measures, physical safeguards, and/or backup generators.
- 4. Establish Recovery Strategies:** Define clear recovery strategies and assign roles, including primary and alternative recovery locations, providing continuity of operations in the event of a disaster.
- 5. Develop Contingency Plans:** Document contingency strategies and develop a comprehensive recovery plan.
- 6. Conduct Regular Testing and Training:** Test the plan through exercises and simulations so personnel understand their roles; verify the effectiveness of failover procedures.
- 7. Maintain the Plan:** Regularly update the BCP to incorporate changes. Documentation, including vendor and emergency contact information, is essential.

---

## **Collaboration and Continuous Improvement**

---

Effective BCP is a collaborative effort that requires input from all relevant stakeholders. One benefit is fostering collaboration across departments, providing alignment and shared BCP ownership.


BCP is not a one-time effort. Organizations should treat it similarly to budget planning – an ongoing exercise that requires frequent reassessment and improvement.

---

## **Key Takeaways**

---

To strengthen your organization's resilience, here are key insights and actionable steps to developing a BCP.

- » It's not a question of "if" but "when." An effective BCP enables swift recovery, minimizing service disruption.
- » Cyber resilience testing measures are vital as cyber threats grow. Organizations must incorporate cybersecurity into continuity planning.
- » Actively involve stakeholders at all levels to meet diverse needs and include various perspectives. Collaboration fosters ownership, strengthens communication, and enhances BCP effectiveness.
- » Regular updates and testing are vital to maintaining an effective BCP, facilitating agility and adaptability. 



---

## About the Author

---

Gus Morales is the principal analyst for security and safety at Gannett Fleming. Gus is an information technology professional with a Master's degree focused in Information Assurance and Cybersecurity and he can be reached at [gmorales@gfnet.com](mailto:gmorales@gfnet.com).

---

## About the Article

---

This article was written for the online [Gannett Fleming Blog](#). Founded in 1915, [Gannett Fleming](#) has been a driving force in shaping infrastructure and improving communities in more than 65 countries, specializing in natural resources, transportation, water, power, and facility-related projects. The company embraces sustainability and innovation in projects and internal activities and achieves results while being responsible stewards of the environment. A results-driven firm, Gannett Fleming is consistently ranked in the top one percent of engineering firms worldwide..

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.