blackbaud

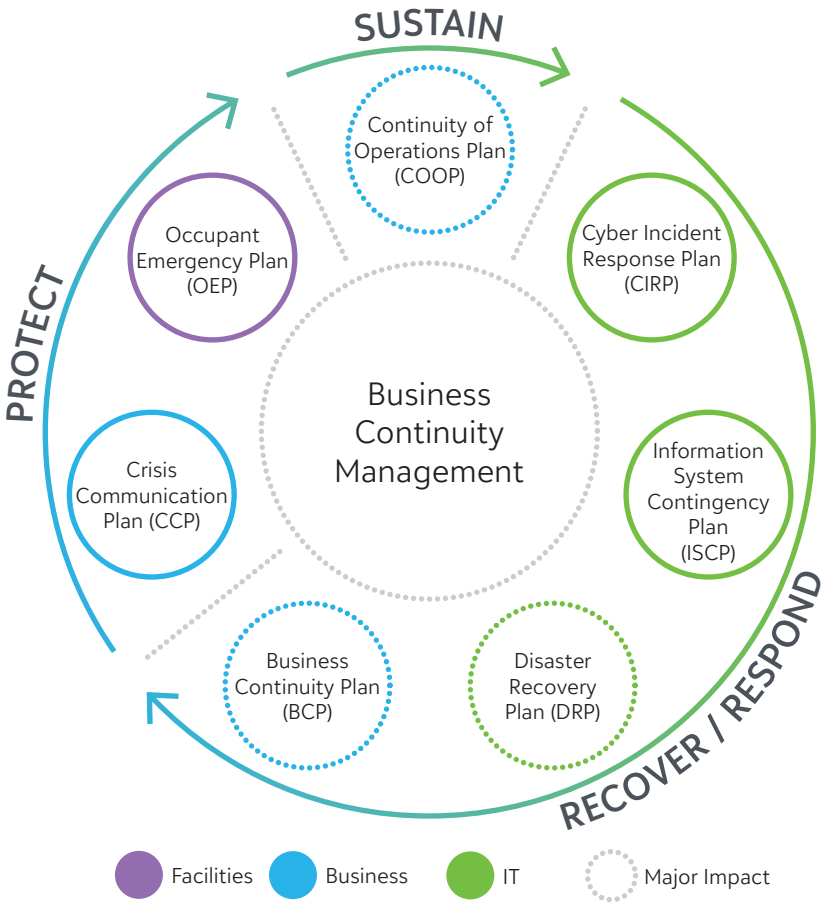
# Blackbaud Business Continuity Management

Blackbaud's Business Continuity Management (BCM) program equips internal teams with the information needed to protect, sustain, and recover their managed operations in the event of a disruption to the business. These plans strengthen our capabilities and enable Blackbaud to better serve our customers.

## Corporate Policy

In addition to helping organizations and individuals after catastrophic events such as natural disasters, pandemics, and public safety incidents, Blackbaud maintains policies and procedures to protect against any potential impacts that could negatively affect our ability to provide excellent customer service and drive social good. These strategies serve to identify, respond, monitor, manage, and restore normal business operations in a timely manner with minimal, or no, business interruption.

With the Blackbaud BCM program—modeled after NIST 800-34—we can assure customers that we have the most efficient and functional plans in place to continue serving their needs, even in the event of a crisis.




## Business Continuity and Disaster Recovery Planning

Effective BCM relies on strong and resilient business continuity planning (BCP) and disaster recovery planning (DRP). These plans at Blackbaud are driven by internal teams managing core business functions: IT, Cyber Security, Human Resources, Facilities, Research, Delivery & Operations (RDO). The BCP and DRP coordinate and consolidate strategies to best enable these teams to support one another without negating or duplicating efforts.

## COOP, OEP, CIRP, CCP, ISCP

Rounding out the BCM are supplemental plans that can be activated independently of or in conjunction with one another, depending on the risk(s) and the estimated severity of the potential threat(s). These determinations are made as part of the readiness and preparation development efforts for the BCM program.

- **Continuity of Operations Plan (COOP):** Ensuring mission essential functions sustain before return to normal.
- **Occupant Emergency Plan (OEP):** Procedures to minimize damages from physical threats.
- **Cyber Incident Response Plan (CIRP):** Prioritized response processes performed in event of cyber-attack.
- **Crisis Communication Plan (CCP):** Internal & external communication plans in event of BCM plan(s) being activated.
- **Information System Contingency Plan (ISCP):** Contingency plan for recovering an information system(s) at same or alternative site/location.

This Knowledgebase article provides details on Blackbaud's Information System Contingency Plans as they relate to specific products.

**Learn more**

Blackbaud's response plans also help customers navigate the impacts of COVID-19.

**Learn more**

## Commitment to Best Practices and Industry Standards

Blackbaud's Compliance, IT, RDO and Cyber Security operations jointly serve to ensure our organization adheres to regulatory requirements so that we may continually execute tactical strategies that best protect our valued resources.

These functions undergo annual Service Organization Control (SOC) and Payment Card Industry Data Security Standard (PCI DSS) assessments that include control reviews of BCM procedures (SOC CC5.0, PCI DSS 12.10). It is our objective to continually satisfy these control requirements to maintain best practices and standards for all BCM operations as we evolve as a business leader in the social good community.

In August 2021, the Risk Management team led a tabletop exercise to simulate a hurricane response plan that would require the activation of Blackbaud's Business Continuity and Disaster Recovery Plans.

## Supply Chain Risk Monitoring

Many of the threats or disruptions that pose a risk to Blackbaud incur reliance on third party service providers, such as data centers, telecommunication services, and ISP and DNS providers. The ongoing availability of such services are vital for Blackbaud to successfully execute recovery plans to achieve a continuity of operations.

Blackbaud maintains a third-party risk management (TPRM) program that identifies, reviews, manages, and monitors any potential risks from these dependent relationships. BCM and TPRM serve one another to promote a more robust strategy for comprehensive efforts to sustain core business operations. Furthermore, it serves to prioritize essential services that can be tied into Blackbaud's BCM strategies for more resilient recovery plans.