

# Business Continuity Plan (BCP)

## Policy Statement

World Bank is unequivocally committed to establishing, maintaining, and regularly testing a comprehensive, enterprise-wide Business Continuity Plan (BCP). The BCP is designed to ensure the timely and orderly resumption of critical business operations and essential services in the event of a significant disruption, thereby safeguarding the Bank's assets, personnel, and reputation, while upholding its commitments to member countries and stakeholders.

## Scope

This BCP encompasses all critical business processes identified by World Bank, along with the supporting IT systems, applications, data, personnel, physical facilities, and critical third-party dependencies that are essential for the Bank's core operations and service delivery on a global scale.

## Objectives

The primary objectives of World Bank's BCP are :

- To minimize the financial, operational, legal, and reputational impact resulting from any disruptive event.
- To ensure the safety, security, and well-being of all World Bank staff during and after a crisis.
- To meet all pertinent legal and regulatory obligations concerning business continuity and disaster recovery, particularly those stipulated by financial industry regulators like the FFIEC and international standards such as ISO 22301.
- To maintain the trust and confidence of member countries, clients, partners, and the public by demonstrating a robust capability to continue essential operations.
- To facilitate a structured and efficient recovery process, returning to normal business operations as swiftly and safely as possible.

## Roles and Responsibilities

Clearly defined roles and responsibilities are crucial for the effective execution of the BCP :

- **Board of Directors & Senior Management:** Provide ultimate oversight and governance for the BCM program, approve the BCP and associated policies, ensure adequate resources are allocated for BCP activities, and champion a culture of resilience across the Bank.

- **Business Continuity Manager (BCM):** The designated BCM is responsible for the overall development, implementation, ongoing maintenance, and regular testing of the World Bank BCP. The BCM coordinates all BCP-related activities across departments and serves as the primary subject matter expert on business continuity.
- **Security Manager:** Plays a pivotal role by contributing to the BCP development with a specific focus on integrating information security considerations, ensuring alignment with the Incident Response Plan (IRP), defining secure recovery procedures, and validating the security of alternate operating environments.
- **Business Unit Leaders/Department Heads:** Responsible for identifying critical business processes within their respective areas, participating actively in the Business Impact Analysis (BIA), developing and maintaining departmental-level recovery plans, and ensuring their staff are trained on BCP procedures.
- **IT Department:** Accountable for the recovery and restoration of all critical IT systems, applications, and data in accordance with defined RTOs and RPOs. This includes managing data backups, operating alternate IT sites, and restoring network connectivity.
- **Crisis Management Team (CMT):** A pre-designated team of senior leaders and key functional heads responsible for strategic decision-making, overall coordination of the Bank's response, and high-level communication during a major disruptive event.
- **Recovery Teams:** Specific teams assigned responsibilities for executing recovery procedures for particular business functions or IT systems.

## BCP Lifecycle & Components

World Bank's BCP follows a structured lifecycle consistent with leading industry practices and standards :

- **1. Risk Assessment:**
  - Systematically identify potential threats and vulnerabilities that could disrupt World Bank's operations. This includes natural disasters (earthquakes, floods, hurricanes relevant to global office locations), technological failures (system crashes, data corruption, power outages), cyberattacks (ransomware, DDoS, data breaches), pandemics, geopolitical instability, and critical supplier failures.
  - Assess the likelihood and potential impact of each identified threat.
  - *Security Manager's Perspective:* World Bank's BCP risk assessment specifically models scenarios such as sophisticated, state-sponsored cyberattacks targeting core financial transaction systems and prolonged denial-of-service (DDoS) attacks against its public-facing platforms and member country portals.

This reflects the unique threat landscape faced by an international financial institution and aligns with FFIEC concerns regarding cybersecurity resilience.

- **2. Business Impact Analysis (BIA):** A cornerstone of the BCP process.
  - Identify and document all critical business functions and processes across World Bank's diverse operations (e.g., loan disbursement, fund management, economic research, policy advice, IT support for global offices).
  - For each critical function, determine the quantitative and qualitative impacts of its disruption over incremental time periods (e.g., financial loss, operational paralysis, legal/regulatory non-compliance, reputational damage, impact on member countries).
  - Establish **Recovery Time Objectives (RTOs)**: The maximum acceptable period of downtime for each critical business function before unacceptable consequences arise.
  - Establish **Recovery Point Objectives (RPOs)**: The maximum acceptable amount of data loss (measured in time) for each critical function that the Bank can tolerate.
  - Identify all dependencies for each critical function, including upstream and downstream processes, internal IT systems, data requirements, key personnel, and essential third-party service providers.
  - *Use Case (BIA for World Bank's Development Project Database)*: The BIA for the central database tracking all ongoing development projects and associated funding for member countries identifies an RTO of 24 hours (to ensure project monitoring and financial oversight can resume) and an RPO of 4 hours (to minimize loss of recently updated project status or financial commitment data). This reflects the database's critical role in the Bank's mission delivery.
- **3. Recovery Strategies Development:** Based on the BIA and risk assessment, develop and document viable recovery strategies to restore critical functions and IT systems within their defined RTOs and RPOs.
  - **Personnel Strategies:** Implement cross-training programs for critical roles, maintain clear succession plans, establish robust remote work capabilities (secure VPNs, collaboration tools, endpoint security), and identify alternate work locations if primary offices become untenable.
  - **Process Strategies:** Develop documented manual workarounds for critical processes where feasible, and streamline recovery processes to prioritize essential activities.
  - **Technology Strategies:**

- **Data Backup and Restoration:** Implement comprehensive data backup and restoration procedures (as detailed in the Backup and Disaster Recovery Policy), ensuring backups are regularly performed, tested, and stored securely offsite or in a separate cloud region.
  - **Redundant Systems:** Deploy redundant hardware, software, and network components for critical systems to provide failover capabilities.
  - **Alternate IT Infrastructure:** Establish alternate IT processing sites (e.g., hot sites with real-time data replication, warm sites, or cold sites) or leverage cloud-based disaster recovery (DRaaS) solutions for rapid system recovery.
- **Facilities Strategies:** Identify and equip alternate physical office locations (if applicable), and formalize work-from-home (WFH) arrangements with necessary security and logistical support.
- **Third-Party Dependency Strategies:** Identify all critical third-party vendors and service providers. Review their BCPs to ensure alignment with World Bank's requirements. Establish contingency plans, which may include identifying alternative vendors or developing in-house capabilities for essential services.
- **4. Plan Development:** Document the BCP comprehensively.
  - **Master BCP Document:** An overarching document detailing the BCM program, governance, policies, and general procedures.
  - **Departmental Recovery Plans:** Specific plans for each business unit and support function, outlining detailed procedures to recover their critical processes.
  - **IT Disaster Recovery Plan (IT DRP):** A detailed technical plan for recovering critical IT infrastructure, systems, applications, and data (see Backup and Disaster Recovery Policy).
  - **Activation Criteria:** Clearly defined triggers and thresholds for activating the BCP and specific recovery plans.
  - **Recovery Teams and Responsibilities:** Documented roles, responsibilities, and contact information for all personnel involved in the recovery effort, including the Crisis Management Team and specialized recovery teams.
  - **Crisis Management Plan:** Procedures for overall strategic coordination, executive decision-making, resource allocation, and managing the broader implications of a crisis.
  - **Communication Plan:** Detailed internal and external communication protocols, including methods, target audiences (employees, member

countries, media, regulators, partners), designated spokespersons, and pre-drafted communication templates for various scenarios.

- **5. Training and Awareness:**

- Conduct regular, role-specific training for all employees on their responsibilities under the BCP and in the event of a disruption.
- Implement ongoing awareness programs to promote a culture of preparedness and resilience throughout World Bank.

- **6. Testing and Exercises:** The BCP must be regularly tested to validate its effectiveness and identify areas for improvement.

- **Types of Tests:** Conduct a variety of tests, including:
  - **Tabletop Exercises/Walkthroughs:** Discussion-based sessions to review plans and roles.
  - **Functional Tests:** Testing specific components or functions of the BCP (e.g., data restoration, alternate site activation for a single department).
  - **Full-Scale Simulations:** Comprehensive, live exercises simulating a realistic disaster scenario, involving multiple departments, recovery teams, and potentially external parties.
- **Testing Objectives:** Tests should validate the achievability of RTOs and RPOs, the effectiveness of recovery strategies, the clarity of communication plans, and the preparedness of recovery teams.
- **Frequency:** The testing schedule should be risk-based, with critical functions and systems tested more frequently. Full-scale simulations are typically conducted annually or biennially.
- **Third-Party Involvement:** Where critical services are outsourced, TSPs should be included in relevant BCP tests, or their own test results should be reviewed.
- *Security Manager's Perspective:* World Bank mandates annual full-scale BCP simulation exercises. These exercises often involve complex scenarios, such as a major cyberattack disabling primary data centers in one region, coupled with a natural disaster impacting a key international office. These simulations rigorously test our ability to recover critical global financial services, inter-office communication, and secure remote operations across different continents simultaneously.

- **7. Maintenance and Improvement:** The BCP is a living document and requires continuous maintenance and improvement.

- **Regular Review:** The BCP and all its components (BIA, risk assessment, recovery plans) must be reviewed and updated at least annually, or more frequently if there are significant changes to World Bank's business operations, IT environment, threat landscape, or regulatory requirements.
- **Lessons Learned:** Incorporate findings and lessons learned from all tests, exercises, and actual disruptive incidents into plan revisions.
- **Alignment:** Ensure the BCP remains aligned with the current risk assessment, BIA, and the Bank's overall strategic objectives.

## Framework Alignment

World Bank's BCP is developed and maintained in alignment with:

- **ISO 22301 (Business Continuity Management Systems):** This international standard provides the overarching framework for our BCMS, including requirements for policy, planning, implementation, operation, monitoring, review, maintenance, and continual improvement.
- **FFIEC Business Continuity Management Booklet:** As a financial institution, World Bank adheres to the comprehensive guidance provided by the FFIEC, which details expectations for BCM governance, risk management, BIA, resilience strategies, plan development, testing, and third-party considerations.
- **NIST Special Publication 800-34 (Contingency Planning Guide for Federal Information Systems):** While geared towards federal systems, the principles and methodologies for contingency planning, BIA, and recovery strategy development are highly relevant and incorporated.

## Real-World Example: Regional Office Power Outage

A major power outage affects the city where one of World Bank's key regional offices is located, with an estimated restoration time of 48-72 hours. This office is responsible for processing time-sensitive loan applications for its region.

- **Risk Assessment & BIA:** This scenario (prolonged power outage) was identified in the risk assessment. The BIA determined that loan application processing is a critical function with an RTO of 8 business hours.
- **Recovery Strategies Activated:**
  - **Personnel:** Staff from the affected office are instructed to work remotely, utilizing pre-configured secure laptops and VPN access. A small contingent of essential staff may relocate to a pre-identified nearby partner institution with reciprocal space agreements if home connectivity is also impacted.
  - **Technology:** Critical loan processing applications are hosted in World Bank's primary data center (or a resilient cloud environment), accessible remotely.

Local data that might have been in process is minimal due to centralized systems, and RPO for critical data is 1 hour (achieved via continuous replication or frequent backups).

- **Facilities:** The physical office is closed.
- **Plan Development & Execution:** The departmental recovery plan for the regional office is activated. The Crisis Management Team is notified. The Communication Plan is initiated to inform staff, relevant headquarters departments, and potentially impacted clients about the situation and alternative processing arrangements. IT support provides assistance to remote workers.
- **Testing & Maintenance:** This type of scenario (loss of a regional office) is tested annually via a functional exercise where staff simulate working remotely and processing transactions using alternate systems. The BCP was updated last quarter to reflect new VPN capacity.

**Table: BCP Testing Schedule and Scenarios**

Test Type	Scenario Example	Frequency	Key Participants	Key Objectives	Last Test Date	Next Test Date
<b>Tabletop Exercise</b>	Ransomware attack encrypting critical shared drives	Quarterly	IRT, IT Ops, Security, Key Business Unit Reps	Validate IRP integration, decision-making, communication protocols.	2024-Q4	2025-Q1
<b>Functional Test: Data Restoration</b>	Simulate corruption of a critical financial database	Semi-Annually	IT Ops (DBA, Backup Admins), Application Owner	Verify ability to restore data within RPO/RTO; test integrity of restored data.	2024-H2	2025-H1
<b>Functional Test: Alternate Site</b>	Activate alternate data center for a specific critical application (e.g., Payments)	Annually	IT Ops, Application Team, Network Team	Test failover mechanisms, connectivity, application functionality at alternate site.	2024-09-15	2025-09-15
<b>Functional Test: Remote Access Scalability</b>	Simulate sudden need for 80% of HQ staff to work remotely	Annually	IT Ops (Network, Security), HR, Key Business Units	Test VPN capacity, remote access security, collaboration tool performance under load.	2025-01-20	2026-01-20
<b>Full-Scale Simulation</b>	Major earthquake impacting HQ, requiring evacuation and activation of full BCP	Biennially	CMT, All Recovery Teams, IT, HR, Communications, selected Regional Offices	Test end-to-end recovery of all critical functions, crisis management, inter-departmental coordination, external communication, RTO/RPO achievement.	2023-10-05	2025-10-05
<b>Third-Party Service Test (Joint)</b>	Simulate outage of a critical cloud service provider (e.g., core SaaS platform)	Annually	IT Ops, Security, Business Owner of service, Vendor's BCP/Technical Team	Validate vendor's recovery capability, communication, data synchronization post-recovery,	2024-11-10	2025-11-10

				alignment with contractual RTOs/RPOs.		
--	--	--	--	--	--	--

- **Value of Table:** This BCP Testing Schedule and Scenarios table is indispensable for World Bank as it operationalizes the commitment to regular validation of its business continuity capabilities. For a global financial institution, demonstrating a mature and rigorous testing program is paramount for several reasons:
  1. **Regulatory Compliance:** It directly addresses FFIEC mandates and ISO 22301 requirements for regular BCP testing, providing auditable evidence of due diligence.
  2. **Risk Mitigation:** Proactive testing uncovers weaknesses in plans, strategies, and team preparedness before a real crisis occurs, allowing for corrective actions that significantly reduce the potential impact of disruptions.
  3. **Stakeholder Confidence:** A well-documented and executed testing program reassures member countries, financial partners, and regulatory bodies of World Bank's resilience and ability to maintain critical operations under adverse conditions.
  4. **Continuous Improvement:** Each test provides valuable lessons learned, feeding into a cycle of continuous improvement for the BCP, ensuring it remains relevant and effective against an evolving threat landscape.
  5. **Operational Readiness:** Regular exercises ensure that recovery teams are familiar with their roles and procedures, improving response times and coordination during an actual incident. By systematically testing diverse scenarios, including those involving third-party dependencies, World Bank ensures its BCP is not merely a document but a practical and effective framework for resilience.