

# World Bank - Backup and Disaster Recovery (BDR) Policy

## Section 1: Policy Statement, Objectives, and Scope

- **1.1 Policy Statement** World Bank is committed to ensuring the confidentiality, integrity, and availability of its critical information assets and business operations through a comprehensive Backup and Disaster Recovery (BDR) program. This program is designed to recover from disruptions in a timely and effective manner, minimizing impact to our customers, operations, and regulatory obligations. The BDR program is an integral component of the Bank's overall risk management framework and business continuity strategy.
- **1.2 Objectives** The primary objectives of this BDR Policy are to:
  - Define clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical banking systems and data, ensuring these are understood and achievable.
  - Ensure the timely and orderly restoration of critical banking functions and services following a disruptive incident, thereby maintaining operational resilience.
  - Protect customer data and sensitive financial information from loss, corruption, or unauthorized disclosure during and after a disruptive event.
  - Maintain continuous compliance with all applicable legal, statutory, and regulatory requirements, including those mandated by the FFIEC, FDIC, and other relevant supervisory bodies.
  - Minimize financial losses, operational disruptions, and potential reputational damage resulting from disasters or significant outages.
  - Establish clear procedures for regular testing, maintenance, and updating of BDR plans to ensure their ongoing effectiveness and relevance.
- **1.3 Scope**
  - This policy applies to all World Bank information systems, applications, databases, network infrastructure, and data deemed critical for the continuous operation of banking services and business functions. This includes systems hosted on-premise and those utilizing cloud-based services.
  - This policy covers all World Bank personnel across all departments, as well as third-party vendors and service providers who have a role in the backup, recovery, or continuity of World Bank's operations. The inclusion of third-party vendors is of particular importance, as the Bank relies on numerous external

entities for critical services. A failure at a key vendor can have an impact equivalent to an internal system failure. Therefore, this BDR policy necessitates robust due diligence, contractual agreements specifying BDR capabilities and SLAs, and contingency plans for critical vendor services. For instance, if World Bank's core banking service provider experiences a major outage, our ability to process transactions and serve customers is directly compromised. Our BDR strategy must therefore account for such vendor failures, potentially involving alternative processing arrangements or heightened internal preparedness.

## Section 2: Roles and Responsibilities

- **2.1 Board of Directors and Senior Management:**

- Hold ultimate responsibility for the governance of the BDR program.
- Approve the BDR Policy and associated plans.
- Ensure adequate allocation of resources (financial, personnel, technological) for the effective implementation and maintenance of the BDR program.
- Regularly review reports on BDR readiness, test results, and risk assessments.

- **2.2 Security Manager:**

- Responsible for the development, implementation, ongoing maintenance, and regular review of this BDR Policy and the detailed Disaster Recovery Plan.
- Coordinates all BDR activities across the Bank, including BIAs, risk assessments, plan development, testing, and training.
- Serves as a primary point of contact for BDR-related matters.

- **2.3 IT Department:**

- Executes routine backup procedures according to established schedules and standards.
- Maintains and manages backup systems, software, and media.
- Responsible for the restoration of IT infrastructure, systems, applications, and data during DR testing and actual disaster events.
- Manages DR site infrastructure and ensures its readiness.

- **2.4 Business Unit Managers:**

- Identify and document critical business processes and associated IT dependencies within their respective units.
- Actively participate in Business Impact Analysis (BIA) activities to define RTOs and RPOs for their processes.

- Develop and maintain business-level recovery procedures and workarounds for their specific functions.
- Ensure their staff are trained on relevant BDR procedures.
- **2.5 Disaster Recovery (DR) Team / Business Continuity Team:**
  - A designated team comprising representatives from IT, key business units, security, and communications, responsible for executing the DR plan during a declared disaster.
  - Coordinates response and recovery efforts, making critical decisions under the guidance of Senior Management and the Security Manager.
  - The effectiveness of these roles is not solely based on individual assignments but heavily relies on practiced, cross-departmental collaboration and clear communication channels, especially during high-stress disaster scenarios. Siloed operations during a crisis can lead to critical delays and missteps. For example, IT might successfully restore a database, but if the relevant business unit is unaware or unprepared to validate the data and resume operations, or if management has not clearly communicated the recovery priorities, the overall RTO for a critical service can be missed. This policy, therefore, emphasizes the need for joint planning sessions and regular, integrated DR tests involving all key personnel to foster this collaborative capability.
- **2.6 All Employees:**
  - Maintain awareness of the BDR policy and procedures relevant to their specific roles and responsibilities.
  - Participate in BDR training sessions and awareness programs as required.
  - Report any incidents or conditions that could potentially impact business continuity or data integrity.

## Section 3: Backup Strategy and Procedures

- **3.1 Critical Systems Identification and Prioritization:**
  - A comprehensive inventory of all World Bank information systems and their criticality has been established and is maintained. Critical systems include, but are not limited to:
    - Core Banking System (CBS)
    - Online Banking Platform and Mobile Banking Application
    - Automated Teller Machine (ATM) Network and associated transaction processing systems

- Payment Processing Systems (e.g., SWIFT, ACH, Fedwire gateways)
  - Customer Relationship Management (CRM) System
  - Loan Origination and Servicing Systems
  - Financial Accounting and Reporting Systems
  - Regulatory Reporting Systems
  - Email and Internal Communication Systems
  - Identity and Access Management (IAM) Systems, including Privileged Access Management (PAM)
  - Security Infrastructure (Firewalls, IDS/IPS, SIEM)
- The identification and prioritization of these systems are determined through a formal Business Impact Analysis (BIA) process, conducted at least annually or upon significant business or system changes. The BIA assesses the impact of an outage on bank operations, financial stability, customer service, legal and regulatory compliance, and reputation.
- **3.2 Backup Types, Frequency, and Retention Schedules:**
    - World Bank employs a combination of backup types (full, incremental, differential, continuous data protection/replication) tailored to the RPO and RTO requirements of each system. The specific RTOs, RPOs, backup types, frequencies, and retention periods for critical systems are documented in the "World Bank RTO/RPO for Critical Systems" table. This table is a critical internal document, reviewed and approved by management, and serves as the authoritative source for these metrics. The selection of backup technologies and frequencies is directly linked to these defined objectives; for example, systems with near-zero RPOs, such as the Core Banking System, necessitate advanced solutions like synchronous replication, which carry different cost and complexity implications compared to traditional nightly backups. This understanding ensures that resource allocation for backup infrastructure is aligned with business continuity needs.

**TABLE: World Bank RTO/RPO for Critical Systems (Illustrative Extract)**

System Name	Criticality	RPO	RTO	Backup Type(s)	Backup Frequency	Retention (Online/Hot)	Retention (Archive/Cold)	Regulatory Driver(s)
Core Banking System (CBS)	Tier 0	Near Zero	< 30 minutes	Continuous Replication, Snapshots	Real-time/Continuous	7 days (snapshots)	7+ years	FFIEC, SOX, Local Regs

Online Banking Platform	Tier 1	< 15 minutes	< 1 hour	Full Daily, Incremental Hourly, Replication	Hourly	30 days	7 years	FFIEC, Customer Expectation
ATM Network Transaction Logs	Tier 1	< 30 minutes	< 2 hours	Incremental Backups, Log Shipping	Every 15-30 mins	90 days	7 years	PCI DSS (if applicable), FFIEC
Payment Processing (SWIFT)	Tier 0	Near Zero	< 15 minutes	Real-time Replication, Transaction Logging	Real-time/Continuous	Per SWIFT/Regulator	5-10 years	SWIFT CSP, AML, FFIEC
Customer Transaction Database	Tier 0	< 5 minutes	< 30 minutes	Continuous Data Protection, Frequent Snapshots	Every 5 mins	90 days	7+ years	FFIEC, SOX, GLBA
Email & Communication	Tier 2	< 4 hours	< 24 hours	Full Daily, Incremental Intra-day	Every 4 hours	30 days	1-7 years (as per data)	E-discovery, SOX
Privileged Access Mgt (PAM)	Tier 0	< 1 hour	< 2 hours	Full Daily, Config Backup after change	Daily & Event-driven	30 days	3 years	FFIEC, SOX

\* \*This table is crucial as it codifies the bank's tolerance for data loss and downtime for its most vital services. It directly informs the technical backup solutions, resource allocation, and DR planning. It's a key document for auditors and regulators [4] and serves as a clear objective for IT and business units. Without clearly defined and agreed-upon RTOs/RPOs, recovery efforts can be misaligned with business needs, leading to excessive financial loss, customer dissatisfaction, or regulatory penalties. This table translates business requirements into actionable IT objectives.\*

\* Backup media (tapes, disks, cloud storage) lifecycle management, including secure rotation, storage, and eventual destruction, will be strictly followed.

- **3.3 The 3-2-1 Backup Rule Implementation:**

- World Bank adheres to the 3-2-1 backup rule globally recognized as a best practice :
  - At least **three** copies of all critical data will be maintained.
  - These copies will be stored on at least **two** different types of storage media (e.g., primary disk, backup appliance, tape, cloud storage).

- At least **one** copy will be stored off-site, in a geographically separate location.
  - *Example Scenario:* For the Core Banking System, one copy resides on the primary high-availability SAN storage. A second copy is backed up to an on-premise dedicated backup appliance (utilizing different disk technology or architecture). A third copy is replicated to a secure, immutable cloud storage vault or our designated DR facility, ensuring geographical separation.
- **3.4 Backup Encryption and Media Security:**
  - All backup data, both at rest on backup media and in transit to offsite locations or cloud storage, must be encrypted using strong, industry-standard encryption algorithms (e.g., AES-256 or higher).
  - Encryption keys will be managed securely, with strict access controls and regular rotation, separate from the backup data itself.
  - Physical backup media (e.g., tapes) transported offsite will be stored in locked, tamper-evident containers, and a chain-of-custody log will be maintained for all media movements.
  - Access to backup systems, software, and repositories will be strictly controlled based on the principle of least privilege and require multi-factor authentication.
- **3.5 Offsite Backup Storage and Vaulting:**
  - Procedures are established for the secure storage of backup media at an offsite location. This location will be geographically distant from the primary data center to mitigate risks from localized disasters.
  - The offsite storage facility (whether a third-party vault or World Bank's DR site) must meet stringent physical and environmental security standards (e.g., fire suppression, climate control, access control).
  - For cloud-based offsite backups, immutable storage options will be utilized where appropriate to protect against ransomware and accidental deletion.
  - The integrity and restorability of offsite backups will be verified regularly as part of the DR testing schedule.

## Section 4: Disaster Recovery (DR) Planning

- **4.1 Business Impact Analysis (BIA) Summary:**
  - A comprehensive BIA is conducted and reviewed annually (or as significant changes occur) to identify critical business processes, their dependencies on IT systems, and the potential impact of disruptions.

- The BIA quantifies potential impacts across financial, operational, regulatory, legal, reputational, and customer service domains.
- Maximum Tolerable Period of Disruption (MTPD) is defined for each critical business process, informing the RTOs for supporting IT systems. A summary of the BIA findings is available in the internal BIA Report.
- **4.2 DR Scenarios:** The DR plan addresses a range of potential disaster scenarios, including but not limited to:
  - **Data Center Outage:** Complete or partial loss of the primary data center due to power failure, HVAC malfunction, fire, flood, or physical security breach.
  - **Cyberattack:**
    - Ransomware attack encrypting critical systems, databases, and potentially backups.
    - Destructive malware targeting critical infrastructure.
    - Compromise of Core Banking System or other critical financial applications.
    - Sustained Distributed Denial of Service (DDoS) attack affecting online services.
  - **Natural Disasters:** Earthquakes, hurricanes, widespread flooding, or other severe weather events impacting the primary operational region.
  - **Pandemic or Workforce Unavailability:** Events leading to a significant reduction in available staff to operate critical functions.
  - **Critical Third-Party Vendor Failure:** Extended outage of a critical service provider (e.g., core banking SaaS provider, primary network provider, cloud service provider).
  - **Major Software/Hardware Failure:** Unrecoverable failure of critical server hardware, storage systems, or network components.
  - **Data Corruption:** Logical or physical corruption of critical databases or file systems.
- **4.3 DR Site and Infrastructure:**
  - World Bank maintains a designated secondary disaster recovery (DR) site, geographically separated from the primary data center to ensure it is not affected by the same localized disaster.

- The DR site is equipped as a **hot site** for Tier 0 and Tier 1 systems, meaning it has fully redundant infrastructure (servers, storage, networking) and near real-time data replication, allowing for rapid failover.
- For Tier 2 systems, a **warm site** capability may be utilized, with pre-staged hardware and more periodic data replication.
- Data replication mechanisms (e.g., synchronous/asynchronous storage replication, database log shipping, application-level replication) are implemented to ensure data at the DR site is consistent with defined RPOs.
- The DR site has resilient network connectivity with sufficient bandwidth to support critical operations and user access during a disaster.
- Physical and logical security controls at the DR site are equivalent to or exceed those at the primary data center.

- **4.4 Failover and Failback Procedures for Critical Applications:**

- Detailed, step-by-step failover procedures are documented for all critical applications and systems, outlining the process to switch operations from the primary site to the DR site.
- Failover triggers are defined, including criteria for automatic failover (where technically feasible and appropriate) and manual failover initiation by the DR Team.
- Specific roles and responsibilities for personnel involved in the failover process are clearly assigned within the DR plan.
- Procedures include steps for verifying the functionality and data integrity of systems and applications after failover to the DR site.
- Detailed, step-by-step failback procedures are documented for restoring operations to the primary data center once it has been repaired, secured, and declared safe for production use.
- Failback procedures include strategies for data synchronization from the DR site back to the primary site to ensure no data loss and maintain consistency.
- The decision to fail back will be made by Senior Management based on a thorough assessment of the primary site's stability and readiness.
- Effective DR planning extends beyond simple data restoration; it ensures the *entire operational ecosystem*—including applications, data dependencies, network configurations, essential security controls (like firewalls, IAM, PAM), and trained personnel—can be fully reconstituted and operated effectively from the DR site within the established RTOs. This demands a holistic perspective that acknowledges the interconnectedness of banking systems. Therefore, DR



plans must meticulously detail the recovery sequence and operationalization of the complete service stack, accounting for all inter-system dependencies. This necessitates regular, comprehensive DR tests that simulate full-site failovers, rather than isolated component-level recovery drills, to truly validate the bank's resilience.

## Section 5: Testing, Maintenance, and Training

- **5.1 DR Test Plan and Schedule:**

- A formal DR test plan is maintained and executed according to a defined schedule.
- **Types of Tests:**
  - **Walkthroughs/Plan Reviews:** (At least Annually) Reviewing the DR plan documentation for accuracy, completeness, and clarity with the DR Team and key stakeholders.
  - **Tabletop Exercises:** (At least Semi-Annually) Simulating disaster scenarios in a discussion-based format to validate decision-making processes, communication channels, and roles/responsibilities. Scenarios will include those listed in Section 4.2.
  - **Functional Tests/Component Recovery Tests:** (At least Quarterly for Tier 0/1 systems) Testing the recovery of specific systems, applications, or infrastructure components (e.g., restoring a database, failing over a specific application).
  - **Full-Scale Simulations/Failover Tests:** (At least Annually for Tier 0/1 systems) Simulating a major disaster requiring failover of critical systems to the DR site and operating from the DR site for a defined period.
- Success criteria for each test are predefined and aligned with the RTOs and RPOs for the systems being tested.
- All DR tests will be documented, including objectives, scope, participants, actions taken, and outcomes.

- **5.2 Post-Test Review and Plan Updates:**

- Following each DR test, a formal post-test review meeting will be conducted with all participants and relevant stakeholders.
- The review will analyze test performance against objectives, identify any deviations from the plan, highlight successes, and document deficiencies or gaps.

- Lessons learned will be documented, and an action plan with assigned responsibilities and timelines will be created to address any identified issues.
  - The BDR Policy and associated DR plans will be updated promptly based on test findings, changes in the IT environment, business process modifications, or new regulatory requirements. The FFIEC places significant emphasis on such testing and iterative improvement. Testing is not merely a compliance formality but the primary mechanism for validating the plan's viability and uncovering weaknesses before an actual disaster strikes. An untested plan is likely to fail under real-world pressures due to overlooked dependencies, flawed procedures, or outdated contact information. Consistent, rigorous testing builds institutional muscle memory, refines operational procedures, and ensures the BDR program remains effective as the Bank's systems, personnel, and the threat landscape evolve. This necessitates dedicated resources and unwavering management commitment to the testing schedule and subsequent remediation efforts.
- **5.3 Employee Training and Awareness:**
    - All World Bank employees will receive regular training on general BDR awareness and their specific roles and responsibilities during a disaster, as applicable.
    - Members of the DR Team and other key personnel involved in recovery efforts will receive specialized, in-depth training on DR procedures, tools, and technologies.
    - Training records will be maintained.
    - BDR awareness will be promoted through internal communications and incorporated into new employee onboarding.

## Section 6: Policy Review and Exceptions

- **6.1 Review Cycle:** This BDR Policy and all associated DR plans will be reviewed, updated as necessary, and formally approved by Senior Management and the Board of Directors at least annually, or more frequently if significant changes occur to World Bank's business operations, IT infrastructure, risk posture, or regulatory requirements.
  - **6.2 Exception Process:** Any requests for exceptions to this BDR Policy must be submitted in writing to the Security Manager. Exceptions will only be granted after a formal risk assessment has been conducted to evaluate the potential impact of the deviation, and appropriate mitigating controls have been documented and approved by Senior Management. All approved exceptions will be documented and reviewed periodically.
-

# Appendix A: Backup and Disaster Recovery Simulation

## Items/Scenarios for World Bank

1. **Scenario Trigger:** Primary data center experiences a complete power outage lasting more than 4 hours.
  - **Action:** Activate the full Disaster Recovery Plan.
2. **System Recovery Test:** Restore the Core Banking System (CBS) from the latest replicated data at the DR site.
  - **Metric:** Measure time taken against the defined RTO of < 30 minutes.
3. **Data Integrity Test:** Simulate corruption of the primary Customer Transaction Database. Restore from the most recent valid backup.
  - **Metric:** Verify data loss is within the RPO of < 5 minutes.
4. **Application Failover:** Execute documented failover procedures for the Online Banking Platform to the DR site.
  - **Action:** Confirm functionality and accessibility for simulated users.
5. **Application Failback:** After a simulated successful recovery at the DR site, execute failback procedures for the Online Banking Platform to the (simulated) restored primary site.
  - **Action:** Ensure data synchronization and full functionality.
6. **3-2-1 Rule Verification:** Select three critical systems (e.g., CBS, Payment Gateway, CRM).
  - **Action:** Verify the existence and accessibility of three distinct copies of their data, on two different media, with one copy verifiably offsite.
7. **Ransomware Attack Simulation:** Critical servers (excluding primary CBS replica to avoid full disruption in simulation) are "encrypted."
  - **Action:** Attempt to restore affected servers from designated immutable backups or clean snapshots. Evaluate time to restore.
8. **Backup Encryption Key Management Test:** Attempt to restore an encrypted backup of a Tier 2 system.
  - **Action:** Verify that authorized personnel can securely access and utilize the necessary decryption keys.
9. **Third-Party Vendor Communication Test:** Simulate an outage at a critical third-party payment processor.

- **Action:** Execute the communication plan to contact the vendor, escalate internally, and inform relevant stakeholders as per the DR plan.
10. **DR Team Role-Play Exercise:** Assign specific DR team members roles (e.g., DR Coordinator, Network Recovery Lead, Database Admin Lead).
- **Action:** Have them walk through and verbally execute their specific tasks for a chosen DR scenario (e.g., Data Center Fire).
11. **Internal Communication Test:** During a simulated full-scale DR test.
- **Action:** The DR Team uses predefined channels (e.g., emergency conference bridge, secure chat) to provide status updates to a mock "Executive Management" group every 30 minutes.
12. **Offsite Media Retrieval Test:** Request retrieval of a specific set of (test) backup tapes from the offsite storage facility.
- **Metric:** Measure time taken for retrieval against SLA with the vault provider. Verify media integrity.
13. **Backup System Redundancy Test:** Simulate failure of the primary backup server/software.
- **Action:** Verify that backup jobs can be initiated and managed using the secondary/redundant backup system.
14. **DR Site Network Capacity Assessment:** During a failover test of the Online Banking Platform.
- **Action:** Monitor network bandwidth utilization and latency at the DR site under simulated peak load to ensure it can handle production traffic.
15. **DR Plan Documentation Review:** A key DR team member is "unavailable" (simulated).
- **Action:** Another team member must locate and use the DR plan documentation to identify contact lists and escalation procedures for the unavailable member's responsibilities.
16. **Critical Patch Failure Scenario:** A critical security patch applied to the Loan Origination System causes instability.
- **Action:** Initiate procedures to roll back the patch and restore the system from the pre-patch backup.
17. **MTPD Evaluation for a Business Process:** The internal wire transfer approval process (Tier 1) is disrupted.

- **Action:** Evaluate if the documented manual workarounds can sustain operations within the MTPD and if the RTO for system recovery aligns with this MTPD.

18. **Alternate Site Accessibility Test:** Key personnel attempt to access the DR site (physically or virtually, depending on setup).

- **Action:** Verify access credentials and procedures for DR site access.

19. **Data Synchronization Verification Post-Failback:** After a simulated failback of the CRM system.

- **Action:** Perform data validation checks to ensure data consistency between the DR site and the restored primary site.

20. **Review of Vendor SLAs for DR:** Select two critical SaaS vendors.

- **Action:** Review their stated RTO/RPO commitments and DR capabilities against World Bank's requirements. Identify any gaps.