Disaster Recovery Strategy

– Amazon Warehouse Fire Scenario

Strategic Activities

We maintain a frequent backup schedule, taking incremental database and system-state snapshots every 15 minutes, alongside a weekly full backup and AMI snapshots, all securely stored in multiple AWS regions to ensure rapid recovery and redundancy. Our failover orchestration uses automated scripts that detect system failures and launch Tier 1 services—such as the warehouse management and order systems—in a secondary region while notifying stakeholders. After failover, we validate data accuracy, integrity, and performance in a sandbox environment before handing over operations. Meanwhile, we engage our emergency partner, like BMS CAT, within 30 minutes to contain fire damage and prepare the site for recovery. We also conduct quarterly DR simulations, performing full system cutover, measuring recovery time, debriefing staff, and improving the process. After the site is cleared, we perform post-incident synchronization and reintegration, reconciling data and switching operations back without impacting customers.

Tier 1 Critical systems like order processing and WMS must recover within 2 hours with minimal data loss (15 minutes) to ensure fulfillment.

Tier 2 Critical support systems like communication tools and safety monitoring must be recovered within 4 hours, with a maximum of 1 hour of data loss.

Tier 3 Less vital systems like reporting and back-office functions can tolerate up to 24 hours of downtime and 4 hours of data loss.

- Vision: Keep warehouse operations running or quickly recovered so customers are not affected by disruptions.
- Mission: Create a fast, reliable, and affordable disaster recovery system that protects operations and staff.
- Drivers: Fire risk, delivery demands, compliance needs, and the opportunity to use cloud-based recovery tools.

Goals

Our disaster recovery plan is designed to minimize downtime by the recovery of Tier-1 systems within **2 hours** (the RTO Recovery Time Objective) and minimize data loss by a maximum exposure of **15 minutes** of potential loss (the RPO Recovery Point Objective). By rapidly transferring operations to an alternate facility or cloud configuration, we can maintain uninterrupted fulfillment and avoid order backlogging. In the process, we also support employee safety and regulatory compliance through structured evacuation processes, health initiatives, and adherence to legal requirements.

Building Principles

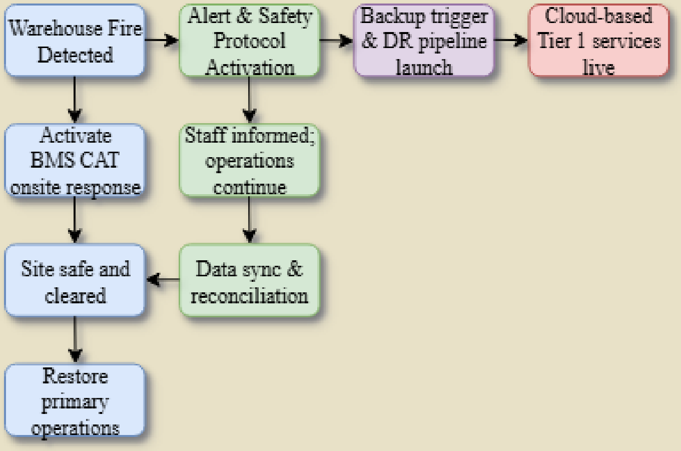
Our DR strategy uses hybrid redundancy, combining AWS multi-region backups with on-prem system replication for fast and reliable recovery. We follow an automation-first approach, using tools like CloudFormation or Terraform to quickly set up recovery environments when systems fail. Systems are restored based on priority through a tiered structure (Tier 1 to Tier 3) to meet recovery time and data loss targets. We also work with partners like BMS CAT to manage fire response and site safety. To stay ready, we run regular drills and tests, including quarterly fire and failover simulations.

261
Xuanyu Zhu
July.27th, 2025

Success Factors

Our disaster recovery readiness is based on clearly defined and regularly tested **RTO and RPO targets** for each system tier. We have **24/7 access to an emergency partner** who can quickly secure the site and support recovery. Our **cloud backups** use versioning, encryption (in-transit and at-rest), and **cross-region replication** to keep data safe and quickly recoverable. Our team is trained with clear roles, communication protocols, and **regular evacuation drills**. We also use a **DR readiness scoreboard** to track drill results, recovery times, data loss, and overall progress for continuous improvement.

Incident Flow



Warehouse Fire Detected → Alert & Safety Protocol Activation → Backup trigger & DR pipeline launch → Cloud-based Tier 1 services live

Warehouse Fire Detected → Activate BMS CAT onsite response → Site safe and cleared → Restore primary operations

Alert & Safety Protocol Activation → Staff informed; operations continue → Data sync & reconciliation → Site safe and cleared

BIA: Business Impact Analysis determined the vital systems and established recovery time and data loss objectives according to their significance.

BCP: Business Continuity Plan established fallback arrangements such as backup warehouses, third-party logistics, and relocation of staff to continue operations in the event of disruption.