**Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP) Based on the Provided Document**

**(a) Disaster Recovery Plan (DRP)**

The **East West Bank (EWB) Digital Banking Disaster Recovery Plan (DRP)** defines procedures for restoring IT systems, data, and infrastructure following a disruption. The DRP focuses on minimizing downtime and ensuring that critical banking services are restored promptly.

The DRP includes specific **Recovery Time Objectives (RTOs)** for different systems, with Tier 1 systems requiring recovery within **4 hours**, Tier 2 within **1 day**, Tier 3 within **3 days**, and Tier 4 exceeding **3 days**.

Key aspects of the DRP include:

* **Application Recovery**: The IT team assesses system disruptions, identifies affected applications, and coordinates recovery efforts. Tier 1 systems, including customer-facing websites and fraud detection tools, are prioritized for rapid restoration.
* **Data Backup and Restoration**: Digital banking applications rely on AWS, Azure, and on-premise data centers. Backups are maintained, and recovery plans include procedures for data restoration and loss mitigation.
* **Failover Mechanisms**: Critical applications have **automatic failover** to backup systems or alternative cloud environments. AWS and Azure services can be redeployed in different locations if needed.
* **Incident Response & Communication**: The **Network Operations Center (NOC)** monitors IT systems 24/7, troubleshoots issues, and coordinates with subject matter experts. Disruptions are escalated based on severity, and affected departments are notified through the **Business Continuity Incident Hotline**.
* **Third-Party Dependencies**: The DRP addresses recovery strategies for third-party services such as **LexisNexis, FIS, and Alipay**, which support fraud detection and payment processing. If a third-party service is disrupted, EWB escalates issues with vendors and applies manual workarounds when applicable.

**(b) Business Continuity Plan (BCP)**

The **EWB Digital Banking Business Continuity Plan (BCP)** provides a structured approach to maintaining essential business functions before, during, and after a disruption. The BCP is designed to **protect critical banking operations, minimize risk exposure, and ensure compliance with regulatory requirements**.

The plan outlines specific strategies for:

* **Incident Response & Reporting**: Employees must report business continuity incidents through the **BCP Hotline**. The **Crisis Management Team (CMT)** is activated for significant disruptions. Life safety measures take priority in emergencies.
* **Workforce Recovery**: If critical personnel become unavailable, staffing priorities are reassessed. **HR is notified to initiate the replacement process** in case of extended workforce disruptions. This may involve internal role reassignments or external hiring. HR receives details on **role descriptions, required experience, and system access needs**.
* **Technology & Location Dependencies**: Digital banking services depend on **AWS, Azure, and on-premise data centers**. If a location becomes inaccessible, employees **work remotely or relocate to an alternate EWB facility**.
* **Third-Party Dependencies**: The BCP acknowledges reliance on external vendors, including **Alipay, LexisNexis, and Salesforce**, for fraud detection, identity verification, and customer service. If a vendor service is disrupted, EWB applies alternative solutions or escalates the issue.
* **Return to Business as Usual (BAU)**: Once recovery objectives are met, the **Department Recovery Team** conducts an after-action review to document lessons learned and improve the BCP for future incidents.

This **BCP and DRP framework ensures that East West Bank’s digital banking services, including fraud detection models like Alipay, remain resilient and operational in the face of disruptions**.