Fictive Subsidiary: Alderaan Digital Banking (ADB)

Alderaan Digital Banking (ADB) is a wholly online neobank subsidiary of IBC, drawing its name from the Star Wars universe. Unlike traditional banking models, ADB conducts nearly all its operations electronically, from account opening and loan origination to complex treasury actions. Below is an overview of the organizational structure, the major processes driving ADB's day-to-day activities, and the **key IT applications** (internal or external) supporting each process.

Organizational Structure

1. **Executive Leadership**
2. **CEO (Alderaan Digital Banking):** Sets strategic vision, manages partnerships, and ensures alignment with IBC's group objectives.

3. **COO (Alderaan Digital Banking):** Oversees all operational pillars, monitoring KPIs and resource allocation across technology, customer-facing services, and compliance execution.

4. **Core Business Units**

5. **Online Transactions & Payments Division:** Handles real-time payments, P2P transfers, and card transactions.
6. **Loans & Credit Division:** Manages digital loan applications, credit assessments, and advanced underwriting procedures.

7. **Support & Back-Office Operations Division:** Addresses dispute resolution, AML reviews, and daily transaction reconciliations.

8. **Support Functions**

9. **IT & Security Department:** Responsible for infrastructure, network security, application development, DevOps, and cybersecurity.
10. **Compliance & Legal Department:** Ensures regulatory compliance for local and cross-jurisdictional operations.
11. **Finance & Accounting Department:** Maintains financial reporting, treasury management, and liquidity oversight.
12. **HR & Administration Department:** Manages staffing, role-based access controls, and employee training programs.

13. **Enterprise Architecture & Security Architecture Office:** Defines and monitors architectural standards, including secure designs and risk-based controls.

14. **Vendor Management & Procurement**

15. Oversees relationships with external providers that supply software, hardware, or specialized services (e.g., cloud hosting, identity verification, credit scoring).

16. **Marketing & Customer Engagement**

17. Conducts campaigns, analyses customer behavior, and orchestrates user onboarding journeys.

Overview of Major Processes and Key IT Applications

Below is a consolidated view of the central processes that power ADB's banking ecosystem, each tied to a specific function or department, along with **key internal or external IT applications** supporting them.

1. Online Account Opening

- **Owner:** Head of UX and Customer Onboarding
- **Key Activities:** eKYC checks, automatic identity verification, account credential creation
- **Dependencies:** Third-party verification APIs, HR for policy alignment, legal for data privacy
- **Key IT Applications:**
- **Customer Onboarding Portal** (internal web application for user registration)
- **eKYC Verification System** (external vendor's API for identity checks)
- **ID Scan & OCR Tool** (third-party service integrated into the portal)
- **HR Access Control Database** (internal system for policy references)

---

2. Digital Payments & Transfers

- **Owner:** Head of Online Transactions
- **Key Activities:** Real-time payment processing, P2P transfers, external clearinghouse interactions
- **Dependencies:** Payment gateways, card networks, AML/fraud checks
- **Key IT Applications:**
- **Payment Gateway Platform** (external service for card and online payments)
- **Real-Time Settlement Engine** (internal application to route or confirm transactions)
- **Fraud Detection Module** (internal or third-party AML solution)
- **Clearinghouse Connector** (external API or interface to national/interbank clearing network)

---

3. Core Banking Operations

- **Owner:** IT Manager (in synergy with the Infrastructure Lead)
- **Key Activities:** Maintaining account ledgers, transaction integrity, ensuring performance and resiliency
- **Dependencies:** Database systems, DevOps pipelines, patch management processes

- **Key IT Applications:**
- **Core Banking System** (internal, main ledger management software)
- **Database Cluster** (internal, high-availability storage for transaction data)
- **DevOps Pipeline** (CI/CD environment for updates to the core system)
- **Patch Management Console** (internal tool for distributing software updates)

---

4. Mobile and Web Application Management

- **Owner:** Mobile Banking Product Manager
- **Key Activities:** Designing user journeys, pushing new features, coordinating with the DevOps Engineer for releases
- **Dependencies:** QA testing, static code analysis tools, vulnerability scans
- **Key IT Applications:**
- **Mobile Banking App** (internal application for iOS/Android)
- **Web Front-End** (internal React/Angular or similar framework)
- **Static Code Analysis Tool** (external or on-prem for scanning code)
- **Vulnerability Scanner** (internal/external solution integrated into DevOps pipeline)

---

5. Loan Origination and Underwriting

- **Owner:** Loan Origination and Underwriting Manager
- **Key Activities:** Digital form submissions, credit scoring, integration with external data providers
- **Dependencies:** Risk assessment modules, compliance checks for local lending regulations
- **Key IT Applications:**
- **Loan Application Portal** (internal front-end for customer data intake)
- **Credit Scoring Engine** (could be external or internal advanced analytics tool)
- **Underwriting Workflow System** (manages approvals, flags anomalies)
- **Compliance Check Module** (AML/KYC checks for lending)

---

6. Accounting & Finance Reporting

- **Owner:** Accounting and Finance Manager
- **Key Activities:** Monthly closures, transaction reconciliations, financial statement preparation
- **Dependencies:** Core banking data exports, treasury data, advanced reporting modules
- **Key IT Applications:**
- **Finance & GL System** (internal general ledger application)
- **Reporting & BI Platform** (tableau, power BI, or custom internal analytics)
- **Reconciliation Tool** (internal or external software for matching transaction data)
- **Treasury Module** (manages liquidity, short-term investments)

---

7. ATM Network & Card Services

- **Owner:** Card Services Manager
- **Key Activities:** Card issuance, real-time transaction authorization, vendor relationships with card schemes
- **Dependencies:** Payment networks, vendor security reviews, security keys for card transactions
- **Key IT Applications:**
- **Card Issuance Portal** (internal system or external vendor for card creation)
- **Authorization Switch** (internal or external platform that handles card transaction approvals)
- **Key Management Server** (manages cryptographic keys for card transactions)
- **Card Scheme Integration Layer** (API connector for major card networks)

---

8. Threat Intelligence & Vulnerability Management

- **Owner:** Cybersecurity Manager (part of ADB)
- **Key Activities:** System scanning, third-party threat feeds, triaging vulnerabilities for patching
- **Dependencies:** IT Infrastructure team for patch deployment, limited budget hamper automation
- **Key IT Applications:**
- **Threat Intelligence Feeds** (external subscription for new exploits, IOC data)
- **Vulnerability Scanner** (internal or external tool scanning servers/apps)
- **Ticketing or SIEM Integration** (internal platform to track vulnerability triage)
- **Patch Deployment Console** (ties to the patch management system in core infrastructure)

---

9. Compliance & Regulatory Audits

- **Owner:** Compliance and Regulatory Officer
- **Key Activities:** Gathering evidence of compliance, responding to external regulators, verifying alignment with local banking laws
- **Dependencies:** Legal guidelines, internal auditors, departmental heads
- **Key IT Applications:**
- **Compliance Tracking System** (internal software for storing & organizing compliance docs)
- **Regulatory Audit Portal** (external or government-provided portal for filings)
- **Document Repository** (internal, for official forms and evidence)
- **Workflow for Internal Auditors** (could be integrated or separate tool)

---

10. Vendor Access & Oversight

- **Owner:** Procurement Manager

- **Key Activities:** Enforcing vendor security assessments, verifying SLAs, scheduling compliance checks
- **Dependencies:** Cloud providers, card printing vendors, specialized consultancies
- **Key IT Applications:**
- **Vendor Management Portal** (internal or external tool for tracking vendor contracts)
- **SLAs & Compliance Dashboard** (custom or third-party to monitor contract KPI)
- **Procurement Workflow** (internal process for new vendor onboarding & access requests)

---

11. Incident Response & Forensics

- **Owner:** Security Manager (part of the ADB structure)
- **Key Activities:** Triaging reported incidents, containing breaches, and producing incident reports
- **Dependencies:** DevOps and IT teams for data capture, incomplete documentation due to limited resources
- **Key IT Applications:**
- **Incident Response Platform** (internal or external solution that centralizes IR tasks)
- **Forensic Analysis Tools** (licenses for disk or memory analysis, e.g. EnCase or open-source alternatives)
- **SIEM** (Security Information & Event Management) for logs & alert correlation
- **Ticketing System** (tracks incidents from detection to closure)

---

12. DevOps & Deployment Pipelines

- **Owner:** DevOps Engineer
- **Key Activities:** Automating code builds, container orchestration, facilitating CI/CD for all internal software
- **Dependencies:** Security code scanning, QA sign-offs, post-deployment checks
- **Key IT Applications:**
- **CI/CD Server** (Jenkins, GitLab CI, or similar)
- **Container Orchestration Platform** (Kubernetes, Docker Swarm, etc.)
- **Source Control (Git)** (internal or external repository hosting)
- **Artifact Repository** (storage for build artifacts, images)

---

13. UI/UX Enhancement & Customer Journeys

- **Owner:** Marketing Campaigns Director
- **Key Activities:** Customer engagement analysis, AB testing, cross-selling opportunities
- **Dependencies:** Data analytics platforms, compliance considerations for tracking user interactions
- **Key IT Applications:**

- **A/B Testing Suite** (could be external, e.g. Optimizely)
- **Marketing Automation Tool** (HubSpot, Marketo, or in-house)
- **Analytics Platform** (Google Analytics, or custom events tracking)
- **CRM** (customer relationship management tool)

---

14. Data Privacy & Retention

- **Owner:** Data Protection Officer (Subsidiary-Level)
- **Key Activities:** Ensuring privacy by design, implementing retention schedules, responding to data subject requests
- **Dependencies:** Coordinating with DevOps for data disposal scripts, external regulatory constraints
- **Key IT Applications:**
- **Data Retention Policy Engine** (internal rules for archiving or deleting PII)
- **Privacy Request Portal** (front-end for data subject requests)
- **Secure Deletion / Anonymization Tools** (scripts or vendor solutions)
- **Regulatory Constraint Tracker** (possible shared compliance dashboard)

---

15. Cross-Border Transaction & Clearing

- **Owner:** Payment Clearing and Settlement Lead
- **Key Activities:** Aligning with SWIFT, national clearinghouses, settlement runs in multiple currencies
- **Dependencies:** IT Manager, compliance checks for anti-money laundering, potential brand damage if delayed
- **Key IT Applications:**
- **SWIFT Interface** (external or partnered solution for cross-border messaging)
- **Clearinghouse Connector** (internal service connecting to interbank networks)
- **FX Conversion Engine** (handles multi-currency transactions real-time)
- **Settlement Scheduler** (manages end-of-day or real-time settlement processes)

---

16. Collections & Recovery

- **Owner:** Collection and Recovery Team Lead
- **Key Activities:** Automated contact strategies, linking defaulted accounts with internal legal processes
- **Dependencies:** Loan underwriting data, legal oversight for escalations, CRM tools
- **Key IT Applications:**
- **Collections Management System** (tracks overdue accounts, schedules outreach)
- **Dialer / SMS Outreach** (external or internal tool for contacting customers)
- **CRM** (shared or separate from marketing, focusing on debt follow-up)
- **Legal Case Management** (internal system or module for advanced legal processes)

---

17. Treasury & Liquidity Management

- **Owner:** Treasury and Liquidity Specialist
- **Key Activities:** Monitoring daily bank positions, placing short-term investments, maintaining foreign exchange hedges
- **Dependencies:** Market data feeds, nightly batch processing, real-time updates from the ledger systems
- **Key IT Applications:**
- **Treasury Platform** (internal or external solution for liquidity tracking)
- **Market Data Feeds** (Bloomberg/Reuters or specialized aggregator)
- **FX Hedging Module** (handles currency risk management)
- **Batch Processing Scheduler** (orchestrates nightly ledger updates)

---

18. Legacy Systems & Migration Projects

- **Owner:** Head of Back-Office Processing
- **Key Activities:** Handling older transaction modules pending phased retirement, ensuring minimal backlog
- **Dependencies:** Network segmentation, manual patchwork solutions, vendor relationships for obsolete technologies
- **Key IT Applications:**
- **Legacy Transaction Module** (old mainframe or older software)
- **Migration Toolkit** (scripts or vendor-based solution for data migration)
- **Obsolete OS Patching** (special arrangements for EOL systems)
- **Vendor-Specific Connectors** (bridging old modules with new ones)

---

19. Governance & Executive Oversight

- **Owner:** CEO and CFO (ADB)
- **Key Activities:** Setting overall direction, budget approvals, deciding on expansions or strategic partnerships
- **Dependencies:** Accurate reporting from all process owners, risk dashboards, compliance insights
- **Key IT Applications:**
- **Executive Dashboard** (internal platform aggregating KPIs from various systems)
- **Risk/Compliance Reporting Tool** (pulls data from SIEM or compliance logs)
- **Board Meeting Portal** (external or internal solution for secure board-level docs)

---

20. Legal Advisory (Subsidiary-Level)

- **Owner:** Legal Advisor (Subsidiary-Level)
- **Key Activities:** Reviewing local contract terms, ensuring synergy with IBC group legal, addressing any new laws impacting digital banking operations
- **Dependencies:** Regulatory bulletins, internal policy alignment, departmental consultations

- **Key IT Applications:**
- **Legal Case Tracking** (internal tool or shared with compliance)
- **Regulatory Bulletin Board** (portal for newly published laws/regulations)
- **Contract Repository** (secure doc storage for referencing legal terms)
- **Policy Management System** (coordinating internal policy changes)

By weaving these departments, roles, and processes together, **Alderaan Digital Banking (ADB)** functions as a swift, cloud-centric neobank under IBC's umbrella, yet faces challenges such as resource-limited security reviews, friction in vendor management, and tight operational schedules that can overshadow recommended security controls. The list of **key IT applications** (both internal and external) tied to each business process provides a clear snapshot of the technology enabling ADB's day-to-day operations.

ROLE CARD: Compliance and Regulatory Officer

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Compliance & Legal Department

Position Description:
As the Compliance and Regulatory Officer, you oversee all compliance-related efforts within Alderaan Digital Banking (ADB). You manage the collection of documentation for audits, respond to inquiries from regulators, and ensure that every ADB process aligns with applicable banking laws, AML/KYC rules, and data privacy regulations. Your role is pivotal in preventing non-compliance penalties and preserving ADB's license to operate.

Primary Objective:
Maintain full regulatory adherence by coordinating internal audit evidence, managing official filings, and collaborating with departmental heads so that ADB can confidently pass external audits and inspections without disruptions or fines.

---

2. Single Business Process Details

2.1 Process Name

Compliance & Regulatory Audits

2.2 Key Process Activities

1. **Compliance Evidence Gathering**
    - Collect relevant documentation from each department (e.g., AML checks, transaction logs, security measures).
    - Manage a **Compliance Tracking System** where all proofs and records are stored.
2. **Regulator Filings & Audit Coordination**
    - Use the **Regulatory Audit Portal** to submit required filings or respond to official inquiries.
    - Coordinate on-site or virtual audits, ensuring each business unit (IT, Loans, Payments) provides timely responses.

3. **Verification & Follow-Up**

    ◦ Validate that all items comply with local/national regulations and standards.
    ◦ Conduct follow-ups with departmental heads if any evidence is missing or insufficient, addressing potential gaps before final submission.

Note: Timely completion and accurate documentation are essential to avoid fines or brand-damaging official censures.

2.3 Dependencies

- **Internal Dependencies:**

    ◦ **Legal & Policy** references from the Legal Advisory (Subsidiary-Level).
    ◦ **Departmental Heads** (e.g., Online Transactions, Loans & Credit) for process-specific data.
    ◦ **IT & Security Department** for logs, security configurations, and incident documentation.

- **External Dependencies:**

    ◦ **Regulatory Bodies/Auditors** (government portals, central bank inspectors).
    ◦ **Document Repository Vendors** (if outsourced) or shared corporate systems for official forms.
    ◦ **Potential Industry or Government Mandates** requiring new compliance measures.

2.4 Peak Operational Periods

- **Quarterly & Annual Audit Cycles**: High pressure around Q1 and Q4, or as determined by local regulators.
- **Post-Incident Follow-Ups**: If a security or AML incident occurs, additional audit scrutiny may spike.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Compliance & Regulatory Audits	1 Day	A prolonged inability to manage compliance tasks beyond 1 day could risk missing deadlines, incurring severe penalties or legal consequences.

---

4. IT Applications

Application	RTO	RPO
Compliance Tracking System	1 Day	4 Hours
Regulatory Audit Portal	1 Day	4 Hours
Document Repository	1 Day	12 Hours
Workflow for Internal Auditors	1 Day	12 Hours

---

5. Financial Impact

- **Annual Revenue Attributable**:
  - Not directly revenue-generating, but majorly protects ADB from huge compliance breaches.
- **Penalties & Costs**:
  - Potential for significant fines if audits are missed or compliance failures are unaddressed.
  - Repeated non-compliance can lead to license threats, restricting ADB's operations.
- **Total Financial Impact (Tier)**:
  - **Tier 4** (High) – Non-compliance can lead to massive legal penalties, brand damage, or forced operational changes.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Severe Official Criticism & Fines	Failing an audit or ignoring compliance mandates can yield major sanctions from regulators.

---

7. Brand Impact

Tier	Impact Value	Rationale
3-4	Moderate to High Brand Damage	Public regulatory actions undermine trust in ADB's legitimacy as a secure neobank.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Notable Operational Disruption	Staff must scramble to recreate or locate missing data, slowing other processes.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2-3	Mild to Moderate Impact	Clients could lose faith in ADB’s reliability if regulatory mishaps become public, but direct customer friction is less immediate.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Compliance & Regulatory Audits	Threat Intelligence & Vulnerability Mgmt	Evidence of scans, patch compliance	Medium	Yes
2	Input	Compliance & Regulatory Audits	Incident Response & Forensics	Incident records, final IR reports	High	Yes
3	Output	Compliance & Regulatory Audits	Executive Leadership (CEO/ CFO)	Summaries of audit results, compliance dashboards	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input/Output	Compliance & Regulatory Audits	Finance & Accounting Department	Transaction logs for reconciliation, financial records for audits	Medium	Yes
2	Input/Output	Compliance & Regulatory Audits	Loans & Credit Division	Loan files, underwriting details for compliance checks	High	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Output	Compliance & Regulatory Audits	Government Regulators	Audit documentation, official filings	High	Yes
2	Output	Compliance & Regulatory Audits	External Auditors/Inspectors	Evidence of controls, on-site or remote reviews	High	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Compliance & Regulatory Audits	*	*	*	*	*							Q1		Q1	Q2/ Q3	Q2/ Q3	Q2/ Q3	Q2/ Q3	Q3	Q4	Q4	Q4	

- **Legend:**
  - Daily tasks from Mon–Fri, but **Quarterly** (Q1, Q2/Q3, Q4) are major push points for official audits or filings.

---

12. Additional Observations

- **Automation Gaps / Manual Steps**:
  - Gathering evidence can be partly manual if some departments don't have updated data in the Document Repository.
- **Budget or Resource Constraints**:
  - Potential new modules for real-time compliance tracking are awaiting corporate budget sign-off.
- **Known Historical Incidents**:
  - A scramble last year to meet an updated AML directive cost ADB fines due to late filing. Exposed the need for more integrated compliance reporting.

---

13. Summary for Role-Play

1. **Key Talking Points**:
   - Risk of missed deadlines or incomplete evidence leading to monetary fines.
   - Heavy reliance on correct departmental data (Loans, Payments, etc.) and timely aggregator of logs.
   - Government portal uptime or changes in filing requirements can be unexpected external stressors.

2. **Process Criticality**:

    - While not direct revenue, compliance is mandatory for ADB's legal operation. Failing audits can threaten the bank's license or result in large penalties.

3. **Data Provided**:

    - **RTO**: 1 Day
    - **Financial Scale**: Potentially large if major non-compliance leads to multi-million credit fines.
    - **Dependencies**: Internal logs, external regulators, departmental heads.
    - **Peak Load**: Quarterly/annual audits, or post-incident follow-ups.

ROLE CARD: Procurement Manager (Vendor Access & Oversight)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Vendor Management & Procurement

Position Description:
As the Procurement Manager overseeing **Vendor Access & Oversight** at ADB, you manage the entire lifecycle of third-party engagements, from initial contract negotiations to monitoring ongoing vendor compliance. You ensure that all suppliers (e.g., cloud providers, card printing services, specialized consultants) align with ADB's security standards, contractual obligations, and regulatory expectations.

Primary Objective:
Maintain robust and compliant vendor relationships by enforcing security assessments, verifying adherence to service-level agreements (SLAs), and scheduling regular audits or compliance checks.

---

2. Single Business Process Details

2.1 Process Name

Vendor Access & Oversight

2.2 Key Process Activities

1. **Security Assessments & Onboarding**
    - Conduct thorough vetting of potential vendors, verifying background checks, security certifications, and any relevant financial stability indicators.
    - Coordinate with IT and Compliance departments to ensure that vendors meet internal security thresholds (e.g., data handling, encryption protocols).
2. **SLA Management & Monitoring**
    - Negotiate key performance metrics with vendors (e.g., uptime percentages, response times).
    - Track compliance with these metrics through dashboards or logs, escalating issues if vendors fall short.

3. **Compliance Checks & Renewals**
    - Oversee periodic vendor audits, whether internal or third-party, to confirm continuous adherence to contract terms and regulatory mandates.
    - Manage contract renewals or terminations, adjusting agreements as technology evolves or as new security requirements arise.

Note: Failure to track vendor performance can expose ADB to security breaches, missed SLA penalties, and regulatory scrutiny.

2.3 Dependencies

- **Internal Dependencies:**
    - **IT & Security Department** for security baseline enforcement, vendor risk assessments.
    - **Finance & Accounting** for budget approvals and invoice validations.
    - **Legal & Compliance** for contract reviews and audits.
- **External Dependencies:**
    - **Cloud Providers** hosting core banking or support services.
    - **Card Printing Vendors** for physical/virtual card issuance.
    - **Specialized Consultancies** providing niche technical or security functions.

2.4 Peak Operational Periods

- **Contract Renewal Cycles:** Especially busy near end-of-year when multiple vendors' agreements may expire simultaneously.
- **New Project Launches:** Additional vendor onboarding for specialized tools or consulting.
- **Periodic Compliance Audits:** Surge in documentation requests to demonstrate vendor alignment with internal policies.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Vendor Access & Oversight	2 Days	Extended downtime halts vendor approvals and SLA monitoring, risking security gaps and potential regulatory non-compliance.

---

4. IT Applications

Application	RTO	RPO
Vendor Management Portal	2 Days	24 Hours
SLAs & Compliance Dashboard	1 Day	12 Hours
Procurement Workflow	2 Days	24 Hours

(These platforms collectively handle the tracking of contract statuses, KPI metrics, and on/offboarding tasks for vendors.)

---

5. Financial Impact

- **Annual Revenue Attributable**: Indirect; more about avoiding service disruption or penalty fees if vendors fail contractual obligations.
- **Penalties & Costs**: SLA breaches can result in monetary penalties. ADB may incur financial damages if critical vendor services go offline or if new vendor onboarding is delayed.
- **Total Financial Impact (Tier)**: Medium-tier, since vendor failings can cascade into lost revenue or fines, but the process itself isn't directly revenue-generating.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism/Some Fines	Failure to ensure vendor compliance can lead to data mishandling, prompting regulatory warnings or fines.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	Vendor breaches or repeated SLA failures reflect poorly on ADB's diligence in vendor oversight.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Some internal processes can be resolved from others	In some cases, alternate vendors or internal teams can fill gaps if one vendor fails, but not for all.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	Little Impact	Most customers do not directly deal with vendor oversight; only visible if a vendor outage cripples ADB’s services.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Vendor Access & Oversight	IT Security (Threat Mgmt)	Vendor risk reports, security baselines	High	Yes
2	Input	Vendor Access & Oversight	Legal Advisory (Subsidiary)	Contract clauses, compliance changes	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Vendor Access & Oversight	Finance & Accounting	Invoices, cost breakdowns	Medium	Yes
2	Input	Vendor Access & Oversight	Operations Divisions	Requirements for new vendor services, SLA needs	High	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Both	Vendor Access & Oversight	Cloud Providers, Card Printers	Contract updates, KPI or SLA metrics	High	Yes
2	Output	Vendor Access & Oversight	Specialized Consultancies	Security assessment protocols	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Vendor Access & Oversight					X	-	-	-	-	-	X	-	-	-	X	-	-	-	X	-	-	X	X

(*Contract renewals often cluster near quarter-end or year-end. New project vendor onboarding surges could occur at the start of major development cycles.*)

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Some vendor screening or SLA verification remain manual, reliant on spreadsheets or email sign-offs.
- **Budget or Resource Constraints**: Proposed expansions for advanced vendor security scanning or more robust SLA monitoring dashboards are pending.
- **Known Historical Incidents**: In the prior year, an unvetted vendor's data breach forced a compliance investigation, revealing weaknesses in the current vendor oversight model.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Vendor onboarding heavily depends on security checks and compliance sign-offs.
    - SLA compliance is crucial; repeated vendor shortfalls can cause financial or reputational hits.
2. **Process Criticality**:
    - Ensures all external partners meet ADB's operational standards.

- Lax oversight can lead to service disruptions, data breaches, or non-compliance.

3. **Data Provided**:

   - RTO of 2 Days (if the oversight tool is offline, new vendors can’t be approved, existing relationships can’t be monitored).
   - Potential Tier 2 regulatory risk if external partner fails compliance.
   - Peaking around quarter-end or new major project launches requiring fresh vendor onboarding.

ROLE CARD: Treasury and Liquidity Specialist

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Finance & Accounting Department (in close coordination with Executive Leadership)

Position Description:
As the Treasury and Liquidity Specialist, you manage ADB's daily cash flow positions, short-term investments, and currency hedges. Your role ensures that sufficient liquidity is available to meet operational obligations, while optimizing the bank's excess funds through secure yet profitable instruments. You also oversee risk mitigation strategies for foreign exchange fluctuations.

Primary Objective:
Maintain stable liquidity and protect ADB's financial health by actively monitoring market conditions, placing short-term investments, and executing FX hedges to minimize currency exposure.

---

2. Single Business Process Details

2.1 Process Name

Treasury & Liquidity Management

2.2 Key Process Activities

1. **Daily Position Monitoring**
    - Gather real-time data from the **Treasury Platform** and the **Core Banking System** ledger.
    - Determine if there's surplus or deficit in daily cash positions across various accounts and currencies.
2. **Short-Term Investments & FX Hedging**
    - Place excess funds into money market instruments or short-term deposits for incremental interest gains.
    - Use the **FX Hedging Module** to lock in exchange rates and mitigate currency risk for international transactions.

3. **Nightly Batch Reconciliation**
    - The **Batch Processing Scheduler** initiates end-of-day updates, reflecting all transactions processed.
    - Validate any discrepancies or capital adequacy requirements, producing final daily position reports.

Note: Quick, accurate decisions are critical to avoid liquidity shortfalls or unhedged currency exposures that could incur losses or regulatory scrutiny.

2.3 Dependencies

- **Internal Dependencies:**
    - **Core Banking System** for up-to-date ledger balances.
    - **Finance & Accounting Department** for reporting and compliance on capital adequacy.
    - **IT & Security Department** for stable system connectivity and nighttime batch processes.
- **External Dependencies:**
    - **Market Data Feeds** (Bloomberg/Reuters or aggregator) for current FX rates, interest rates.
    - **External Platforms** (if part of the Treasury Platform is outsourced) or partner financial institutions for short-term placements.

2.4 Peak Operational Periods

- **Daily Monitoring**: Typically early morning to confirm positions and late afternoon to adjust them.
- **Month-End/Quarter-End**: Higher complexity around financial reporting and rebalancing.
- **Volatile Market Conditions**: Spikes in currency hedging activity if global events impact exchange rates.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Treasury & Liquidity Management	6 Hours	Prolonged downtime beyond 6 hours can leave ADB vulnerable to liquidity shortfalls, missed investment windows, or unhedged FX risk.

---

4. IT Applications

Application	RTO	RPO
Treasury Platform	6 Hours	1 Hour
Market Data Feeds	2 Hours	0*
FX Hedging Module	6 Hours	1 Hour
Batch Processing Scheduler	6 Hours	2 Hours

* Some real-time FX data must not be lost (0 RPO) to ensure accurate hedging decisions.

---

5. Financial Impact

- **Annual Revenue Attributable**:
  - Treasury operations can yield interest/FX gains, impacting millions of credits annually. Liquidity management also prevents overdraft or penalty fees.
- **Penalties & Costs**:
  - Inadequate liquidity or missed margin calls may cause heavy financial losses or forced borrowing at high rates.
  - Delayed hedging can incur FX losses in volatile markets.
- **Total Financial Impact (Tier)**:
  - **Tier 4** (High) – A critical function; mismanagement can produce substantial losses or undermine ADB's solvency.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Serious Regulatory Sanctions or License Risk	Central bank or financial authorities can penalize banks for not meeting liquidity or capital standards.

---

7. Brand Impact

Tier	Impact Value	Rationale
3-4	Moderate to High Brand Damage	A liquidity crisis or inability to fund withdrawals can severely damage ADB's reputation.

8. Operational Impact

Tier	Impact Value	Rationale
3-4	High Operational Strain	Without real-time data or functional systems, staff scramble to track positions manually, risking errors.

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2-3	Some to Significant Dissatisfaction	If liquidity constraints cause delays or service disruptions, customers lose trust; however, direct customer friction is somewhat indirect.

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Treasury & Liquidity Management	Accounting & Finance Reporting	End-of-day balances, interest calculations	High	Yes
2	Output	Treasury & Liquidity Management	Core Banking Operations	Updated ledger data after short-term investments	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Treasury & Liquidity Management	Executive Leadership	Liquidity risk summaries, market outlooks	High	Yes
2	Input	Treasury & Liquidity Management	IT & Security Department	Connectivity, real-time updates, scheduling	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Treasury & Liquidity Management	Market Data Providers (Bloomberg/Reuters)	FX rates, interest rates, market indicators	High	Yes
2	Output	Treasury & Liquidity Management	External Banks/Funds	Short-term placements, confirmations	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Treasury & Liquidity Management	X	X	X	X	X							*			*					*		*	*

- **Legend:**
  - **X** = Daily monitoring (Mon-Fri).
  - ***** = Month/Quarter ends when positions and regulatory capital reporting intensify.

---

12. Additional Observations

- **Automation Gaps / Manual Steps**:
  - In exceptional volatility, the specialist might do manual overrides or consult ad-hoc data sources.
- **Budget or Resource Constraints**:
  - Enhanced real-time predictive analytics for liquidity are pending budget decisions.
- **Known Historical Incidents**:
  - A partial outage of the Market Data Feed last year resulted in delayed currency trades, minor losses, and urgent manual references to third-party websites.

---

13. Summary for Role-Play

1. **Key Talking Points**:
   - Reliance on real-time data from external feeds for correct FX/interest decisions.
   - RTO of 6 hours—longer outages risk immediate financial or regulatory repercussions.
   - High-tier financial impact if mismanaged.

2. **Process Criticality**:
    - Crucial for maintaining operational liquidity, avoiding unexpected overdrafts or currency exposures.
    - Directly tied to compliance with capital/liquidity mandates.
3. **Data Provided**:
    - **RTO**: 6 Hours
    - **Financial Scale**: Multi-million credit losses possible from FX or missed investment windows.
    - **Dependencies**: Market data providers, internal ledger data, nightly batch.
    - **Peak Load**: Daily (morning/evening checks), with more intensity at month/quarter ends.

ROLE CARD: Head of Back-Office Processing

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Support & Back-Office Operations Division (focusing on **Legacy Systems & Migration Projects**)

Position Description:
As the Head of Back-Office Processing, you oversee the maintenance and gradual retirement of older transaction modules still in production, ensuring minimal operational backlogs and continuity of legacy services. This role also involves planning and executing migration projects toward newer platforms, coordinating with vendors for outdated technologies, and managing any manual patchwork or network segmentation strategies to keep these systems functioning securely until full decommissioning.

Primary Objective:
Maintain **business continuity** for legacy systems while **progressively migrating** them to modern equivalents, minimizing downtime and the risk of data inconsistencies.

---

2. Single Business Process Details

2.1 Process Name

Legacy Systems & Migration Projects

2.2 Key Process Activities

1. **Legacy Transaction Module Maintenance**
    - Oversee daily operations of older mainframe or outdated software.
    - Ensure minimal backlog of queued transactions or operations.
2. **Migration Planning & Execution**
    - Use the **Migration Toolkit** to transfer data from legacy systems to modern platforms.
    - Coordinate with vendor specialists for any proprietary connectors or patch solutions.

3. **EOL (End-of-Life) Patchwork & Vendor Collaboration**
    - Address **Obsolete OS Patching** requirements (special support arrangements).
    - Maintain relationships with vendors providing last-mile fixes for otherwise unsupported environments.

Note: There can be partial manual tasks for each step—these are time-consuming and rely on specialized knowledge of legacy code or configurations.

2.3 Dependencies

- **Internal Dependencies:**
    - **IT & Security Department** (network segmentation, security patches).
    - **Core Banking Operations** (ensuring data consistency between old and new modules).
    - **Enterprise Architecture Office** (alignment with future architecture standards).
- **External Dependencies:**
    - **Vendors** (providing specialized support or connectors).
    - **Obsolete OS Providers** or specialized consultancies (for custom patch creation).
    - **Migration Toolkit** vendor for ongoing updates.

2.4 Peak Operational Periods

- No strict cyclical peaks, but **migration cutover windows** (e.g., weekends or after business hours) are risk-prone.
- End-of-quarter or year-end might see heavier historical data retrieval from legacy systems.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Legacy Systems & Migration Projects	8 hours	Extended downtime is sometimes tolerated (planned migrations), but surpassing 1 business day can cause transaction backlog and data misalignment.

---

4. IT Applications

Application	RTO	RPO
Legacy Transaction Module	8 hrs	4 hrs
Migration Toolkit	8 hrs	4 hrs
Obsolete OS Patching Scripts	12 hrs	12 hrs
Vendor-Specific Connectors	8 hrs	4 hrs

---

5. Financial Impact

- **Annual Revenue Attributable**: Minimal direct revenue from the legacy channel, but some processes (like older corporate clients) still funnel transactions here.
- **Penalties & Costs**: Potential operational costs or compliance issues if data is not migrated properly; downtime can lead to extended backlog or brand harm for any stuck transactions.
- **Total Financial Impact (Tier)**: **Medium**—While not the main revenue driver, a backlog or data corruption in legacy systems can create reputational and operational headaches.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism / Some Fines Possible	If data integrity is compromised during migration, regulators may question accuracy of transaction records.

---

7. Brand Impact

Tier	Impact Value	Rationale
2	Some Temporary Brand Damage	Extended issues with older systems rarely hit headlines, but existing clients might lose trust if legacy modules fail.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Significant Additional Manual Work	If the legacy module is down, staff must manually reprocess transactions or rely on complex migration steps.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2	Moderate Concern for Specific Clients	Mostly affects older or corporate customers using legacy channels. Mainstream users may be unaffected.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Legacy Systems & Migration Projects	Core Banking Operations	Old transaction data synchronization	High	Yes
2	Output	Legacy Systems & Migration Projects	Accounting & Finance Reporting	Historical data for statements	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	Legacy Systems & Migration Projects	IT & Security Dept	Patching schedules, network rules	High	Yes
2	Output	Legacy Systems & Migration Projects	Enterprise Architecture Office	Migration roadmap, new platform standards	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Legacy Systems & Migration Projects	Vendor for Obsolete OS	Patch scripts, manual updates	Medium	Yes
2	Output	Legacy Systems & Migration Projects	Migration Toolkit Vendor	Data transfer solutions, bug fixes	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Legacy Systems & Migration Projects	-	-	-	*	*	***	***	*	*	*	***	*	*	*	*	***	*	*	*	*	***	***	***

Legend: *** indicates typical weekends or scheduled downtimes for migrations. Month/quarter ends can be avoided for major cutovers.

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Complex data mapping and manual verification frequently required during migrations.
- **Budget or Resource Constraints**: Approval for advanced migration tooling is delayed, staff reliant on partial scripts.
- **Known Historical Incidents**: Past migrations faced partial data corruption, requiring days to reconcile.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Balancing ongoing maintenance with planned retirement.
    - Danger of partial data corruption or backlog if the legacy module goes down.
    - Vendor reliance for obsolete OS patches.
2. **Process Criticality**:
    - While not front-facing for mainstream, it underpins many back-office functions. Extended downtime can hamper finance and accounting or hamper historical data access.

3. **Data Provided**:

    - RTO: 8 hours (exceeding 1 business day of downtime can cause extensive backlogs).
    - Financial Tier: Medium, but brand/operational risk if data is lost or corrupted.
    - Peak periods revolve around weekend migrations, avoiding month-end closings.

ROLE CARD: Security Manager (Incident Response & Forensics)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
IT & Security Department (specializing in **Incident Response & Forensics**)

Position Description:
As the Security Manager overseeing Incident Response and Forensics, you lead the core process of detecting and containing breaches or suspicious activities at Alderaan Digital Banking. This role ensures timely triage of reported incidents, coordinates technical investigation, and prepares formal incident reports for management. You also collaborate closely with DevOps and IT teams to capture relevant system logs and images, though limited documentation resources can impede swift response in certain scenarios.

Primary Objective:
Maintain a **swift and effective** incident response capability, minimizing damage from cyber threats, while producing **forensic** and **compliance-ready** documentation of each event.

---

2. Single Business Process Details

2.1 Process Name

Incident Response & Forensics

2.2 Key Process Activities

1. **Triage & Logging**
    - Receive incident alerts (from SIEM, employee reports, or threat intelligence).
    - Classify incidents by priority, open tickets in the **Ticketing System**.
2. **Containment & Investigation**
    - Engage relevant teams (DevOps, Infrastructure) for swift containment.
    - Use **Forensic Analysis Tools** (e.g., EnCase, open-source) to gather evidence from compromised hosts.

3. **Reporting & Recovery**
    - Draft a formal incident report for management, highlighting root causes, impacted systems, recommended remediation.
    - Ensure post-incident forensics data is archived for compliance.

Note: Time is critical: the quicker containment is done, the less reputational or financial damage ADB faces.

2.3 Dependencies

- **Internal Dependencies:**
    - **DevOps** (log data, system snapshots)
    - **IT & Security Department** (network security, patching vulnerabilities)
    - **Compliance & Legal** (if a breach triggers regulatory notifications)
- **External Dependencies:**
    - **External IR Platform** (cloud-based or vendor solution if used)
    - **Threat Intelligence Feeds** (to correlate new IOCs or potential attacks)
    - **Third-party Forensic Specialists** (in extreme cases of advanced persistent threats)

2.4 Peak Operational Periods

- **No strict cyclical peak** but incidents may spike around:
    - Large-scale deployments or product launches (when new code might introduce vulnerabilities).
    - Public holidays (hackers may exploit minimal staffing).
    - Marketing campaigns drawing heavier traffic.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Incident Response & Forensics	2 hours	Delays beyond 2 hours in incident handling can lead to major breach spread, increased financial/brand damage, and regulatory scrutiny.

---

4. IT Applications

Application	RTO	RPO
Incident Response Platform	2 hrs	1 hr
Forensic Analysis Tools	4 hrs	2 hrs
SIEM	2 hrs	1 hr
Ticketing System	4 hrs	2 hrs

(RTO/RPO values reflect how quickly these tools must be available to investigate and respond to incidents.)

---

5. Financial Impact

- **Annual Revenue Attributable**: While not directly revenue-generating, delayed or ineffective incident response could result in significant financial losses due to prolonged breaches or data theft.
- **Penalties & Costs**: Fines (GDPR or other data protection regulations), potential lawsuits, or brand damage compensation.
- **Total Financial Impact (Tier)**: **High** – The indirect risk of an uncontained breach can cause extensive financial harm.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Possible Major Fines / Enforcement Actions	A delayed or mishandled incident can violate data protection, leading to severe regulatory consequences.

---

7. Brand Impact

Tier	Impact Value	Rationale
4	Major Brand Damage	High-profile breaches or incompetent IR handling can drastically erode customer trust.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Severe Strain on Staff / Potential Overload	The IR team might work 24/7 if a big breach occurs; lack of standardized procedures intensifies stress.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Noticeable Concern / Fear	News of a breach or slow IR can make customers worry about data theft, possibly leading to churn.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Incident Response & Forensics	DevOps & Deployment	Logs, server access credentials, code details	High	Yes
2	Output	Incident Response & Forensics	IT & Security Management	Incident reports, patch requirements	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Incident Response & Forensics	Compliance & Regulatory	Breach notifications, formal IR findings	High	Yes
2	Input	Incident Response & Forensics	HR & Administration	Employee rosters if insider threat suspected	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Incident Response & Forensics	Threat Intelligence Feeds	IOC data, vulnerability advisories	Medium	Yes
2	Output	Incident Response & Forensics	Possibly External Forensics Vendor	Forensic images, log analysis details	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Incident Response & Forensics	-	-	-	-	-	-	-	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-

Legend: Typically no cyclical “peak,” but spikes might occur after major deployments or security announcements.

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Many IR procedures remain manual (collecting logs, scanning memory dumps).
- **Budget or Resource Constraints**: Additional forensics licensing or specialized staff not always funded.
- **Known Historical Incidents**: Last year, a major phishing campaign tested IR capacity; partial success but delayed patching introduced vulnerability window.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Quick response crucial to minimize damage; 2-hour RTO is strict for containing threats.
    - Some manual tasks hamper speedy forensics—lack of dedicated automation tools or staff might worsen large incidents.
    - Must coordinate with DevOps, compliance, and external vendors for thorough investigations.
2. **Process Criticality**:
    - A failed IR process can lead to extended breaches, major brand damage, and severe regulatory penalties.

3. **Data Provided**:

    - RTO: 2 hours for IR platform availability.
    - High-level brand and regulatory impact if compromised data remains uncontained.
    - Dependencies on DevOps logs, SIEM, and external threat feeds.

ROLE CARD: Data Protection Officer (Subsidiary-Level)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Compliance & Legal Department (collaborating closely with IT & Security)

Position Description:
As the Data Protection Officer (Subsidiary-Level) for Alderaan Digital Banking (ADB), you ensure that data privacy regulations are integrated into all ADB processes. You oversee the lifecycle of personal data—from collection and retention through to destruction—and respond to data subject requests or external regulatory inquiries regarding privacy.

Primary Objective:
Uphold comprehensive data protection standards (privacy by design) and ensure proper data retention schedules, preventing breaches or non-compliance with galactic and local data laws.

---

2. Single Business Process Details

2.1 Process Name

Data Privacy & Retention

2.2 Key Process Activities

1. **Policy Creation & Management**
    - Draft or update data retention policies, ensuring alignment with legal requirements and corporate standards.
    - Educate relevant teams about these policies, clarifying how and when to archive or delete sensitive data.
2. **Data Subject Requests**
    - Operate the Privacy Request Portal for individuals seeking to view, correct, or remove their personal data.
    - Coordinate with IT and relevant business units to fulfill requests within mandated timelines.

3. **Data Deletion / Anonymization**
    - Monitor scheduled data disposal tasks, ensuring that personal data is securely erased or anonymized upon the end of retention periods.
    - Oversee the application of secure deletion tools to prevent residual traces of PII in backups or archives.

Note: Failure to enforce the correct retention schedules or promptly address data subject requests can lead to major compliance infractions and reputational harm.

2.3 Dependencies

- **Internal Dependencies:**
    - **DevOps Team** for implementing automated data disposal scripts in production systems.
    - **Legal & Compliance** for guidelines on new or evolving privacy regulations.
    - **IT & Security** to ensure secure archiving and disposal methods.
- **External Dependencies:**
    - **Regulatory Entities** requiring compliance with specific data protection frameworks.
    - **Vendor Solutions** (if certain data processing or storage tasks are outsourced).

2.4 Peak Operational Periods

- **Quarterly or Annual Audits**: Heightened reviews of data retention practices.
- **New Privacy Legislation**: Surges when external regulators introduce or update privacy regulations, requiring immediate policy adaptation.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Data Privacy & Retention	1 Day	Extended downtime halts data subject requests and data destruction tasks, risking non-compliance with strict privacy deadlines.

---

4. IT Applications

Application	RTO	RPO
Data Retention Policy Engine	1 Day	4 Hours
Privacy Request Portal	1 Day	1 Hour
Secure Deletion/Anonymization Tools	1 Day	4 Hours
Regulatory Constraint Tracker	1 Day	4 Hours

---

5. Financial Impact

- **Annual Revenue Attributable**: Indirect. Mistakes could lead to heavy privacy-related fines or damage trust, eventually impacting revenue.
- **Penalties & Costs**: Non-compliance with data privacy laws can trigger significant fines or legal settlements (multi-million credit range).
- **Total Financial Impact (Tier)**: Typically Tier 2 or Tier 3, reflecting notable fines but not as directly revenue-generating as transaction processes.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism/Some Fines	Missed data deletion deadlines or improper data handling attract official notices.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	Data privacy failures spark strong consumer backlash, though short-lived if swiftly resolved.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Some internal processes can be resolved from others	Alternate staff or manual fallback methods exist to handle data requests, albeit not indefinitely.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Some Impact	Privacy issues can erode consumer trust, but not all customers track privacy policies closely.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Data Privacy & Retention	DevOps & IT Sec.	Implementation scripts for data disposal, new compliance logs	High	Yes
2	Output	Data Privacy & Retention	Legal Advisory	Status of compliance with privacy laws, updated disclaimers	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	Data Privacy & Retention	HR & Administration	Employee data retention guidelines	Medium	Yes
2	Output	Data Privacy & Retention	Marketing & Engagement	Rules for storing or anonymizing campaign data	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Output	Data Privacy & Retention	Regulators (local/galactic)	Evidence of compliance, privacy audits	High	Yes
2	Output	Data Privacy & Retention	External Vendors	Data disposal requirements, privacy standards	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Data Privacy & Retention	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	X	-	-	X	X

(*Spikes may occur when new privacy laws or large data subject request campaigns come in, often at quarter-end or after major marketing pushes.*)

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Some data retention enforcement is manual, relying on departmental sign-offs for older records.
- **Budget or Resource Constraints**: Upgrades to advanced policy engines for real-time data subject requests remain postponed.
- **Known Historical Incidents**: Last year's compliance checks discovered overlooked backup tapes containing older personal data; took weeks to rectify.

---

13. Summary for Role-Play

1. **Key Talking Points**
    - Potential fines from privacy breaches or delayed data subject requests.
    - Collaboration with DevOps to script automated data disposal or anonymization.
    - Regulatory deadlines can come swiftly, forcing quick updates to retention policies.
2. **Process Criticality**
    - Ensures ADB's compliance posture, protecting brand reputation and avoiding legal entanglements.

- Overlooked or stale data quickly becomes a liability if discovered by regulators.

3. **Data Provided**

   - RTO of 1 Day, signifying urgent need to respond to privacy-related tasks even if broader systems fail.
   - Medium-tier financial/regulatory risk but can escalate with repeated non-compliance.
   - Spikes triggered by new regulations or large data subject request waves.

ROLE CARD: Card Services Manager

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Online Transactions & Payments Division (focusing on **ATM Network & Card Services**)

Position Description:
Oversees the life cycle of ADB's card products—from card issuance to real-time transaction authorization. Manages relationships with external card schemes (e.g., Visa/Mastercard) and ensures ADB's ATM operations run smoothly. Collaborates with vendor security reviews, maintains cryptographic keys, and monitors any service-level agreements tied to card services.

Primary Objective:
Ensure **continuous card and ATM operations**, preserving user access to cash, card payments, and a frictionless experience at any card acceptance channel.

---

2. Single Business Process Details

2.1 Process Name

ATM Network & Card Services

2.2 Key Process Activities

1. **Card Issuance & Configuration**
   - Manage new card requests, personalizing details (cardholder name, account linkage).
   - Use the **Card Issuance Portal** for order processing and secure personalization.
2. **Real-Time Transaction Authorization**
   - Reroute card-based transactions to the **Authorization Switch**, verifying available funds and confirming identity (PIN, chip data).
   - Coordinate cryptographic checks with the **Key Management Server**.
3. **Card Scheme Integration**
   - Connect with major card networks (Visa, MasterCard, etc.) via the **Card Scheme Integration Layer**, exchanging authorization messages for cross-network transactions.
4. **ATM Operations**
   - Oversee ATM management for ADB's small ATM network, ensuring they connect securely to the same authorization switch or relevant vendor software.

Note: Timely updates are essential—configuration errors can block user access to ATMs or cause transaction declines.

2.3 Dependencies

- **Internal Dependencies:**
- **IT & Security Department** (patching the Key Management Server, ensuring secure comms).
- **Core Banking Operations** (syncing ledger balances in real time).

- **Back-Office** (dispute resolution, AML checks on suspect transactions).

- **External Dependencies:**

- **Card Scheme Integration** (Visa/Mastercard or local networks).
- **Vendor Security Reviews** (periodic audits from the card associations).
- **ATM Hardware Supplier** (maintenance, security patches for ATM OS).

2.4 Peak Operational Periods

- **Weekday Mornings & Evenings**: Typical surge times for ATM usage.
- **End-of-Month**: Salary credits often lead to increased withdrawal/transfer activity.
- **Holidays & Festive Seasons**: Higher card usage for shopping, potential vendor overload.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
ATM Network & Card Services	2 hours	Customers expect near-instant access to funds. Downtime >2 hours leads to major brand/financial damage, potential SLA breaches with card schemes.

---

4. IT Applications

Application	RTO	RPO
Card Issuance Portal	4 hrs	2 hrs
Authorization Switch	2 hrs	1 hr
Key Management Server	2 hrs	1 hr
Card Scheme Integration Layer	2 hrs	2 hrs

(RTO/RPO values reflect this process's tolerance. Other processes may differ.)

5. Financial Impact

- **Annual Revenue Attributable**: Card fees and ATM usage generate moderate direct income, but they strongly support overall customer satisfaction.
- **Penalties & Costs**: If transactions fail, card networks can impose fines; brand loyalty damage is likely if outages persist.
- **Total Financial Impact (Tier)**: **High**—While immediate revenue hits may be moderate, the intangible brand/reputation impact is critical given user reliance on 24/7 card access.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Criticism / Some Potential Fines	Card schemes (Visa/Mastercard) can levy penalties for repeated SLA failures. Certain consumer protection laws also apply.

---

7. Brand Impact

Tier	Impact Value	Rationale
4	Major Brand Damage	Outages at ATMs or card declines quickly erode trust in a digital-first bank. Headline risk is high.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Severe Strain on Operations	Staff must handle a flood of support calls, manual verification, or alternative processes if automation fails.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	Major Customer Dissatisfaction	Customers rely heavily on ATM/card access. Repeated failures lead to rapid churn or negative social media uproar.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	ATM & Card Services	Core Banking Operations	Real-time ledger checks for balances	High	Yes
2	Output	ATM & Card Services	Accounting & Finance Reporting	Summaries of card usage, daily settlement	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	ATM & Card Services	Compliance & Regulatory	Transaction logs for AML/fraud checks	High	Yes
2	Input	ATM & Card Services	Vendor Management & Procurement	Maintenance schedules, security audits	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	ATM & Card Services	Card Schemes (Visa/ Mastercard)	Auth messages, scheme compliance	High	Yes
2	Input/Output	ATM & Card Services	ATM Hardware Supplier	Updates, OS patches, support tickets	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
ATM Network & Card Services	*	*	*	**	***	***	**	*	*	*	**	*	*	*	*	***	*	*	**	*	*	***	***

Legend: *** indicates highest usage (weekends/holiday shopping).

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Certain special card personalization tasks remain manual, risking delays if staff are absent.
- **Budget or Resource Constraints**: Upgrading older ATM OS requires separate funding, currently pending CFO approval.
- **Known Historical Incidents**: A major card scheme threatened fines last year due to slow real-time authorization responses over two weekends.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Real-time transaction approvals are critical; downtime >2 hours is unacceptable.
    - Card scheme compliance is strict, leading to potential brand or financial hits if SLAs fail.
    - Legacy ATM OS upgrades are partially unfunded.
2. **Process Criticality**:
    - Card and ATM services serve as the **public face** of ADB’s financial accessibility. Prolonged failures tarnish credibility.

3. **Data Provided**:

    - **RTO**: 2 hours maximum.
    - **Financial Impact**: High (brand & fines).
    - **Peak**: Weekends, end-of-month salary times, holiday seasons.

ROLE CARD: Cybersecurity Manager (Threat Intelligence & Vulnerability Management)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
IT & Security Department

Position Description:
As the Cybersecurity Manager overseeing Threat Intelligence & Vulnerability Management, you are responsible for continuously scanning ADB's systems for weaknesses, consuming external threat feeds, and coordinating patching efforts. This role ensures that vulnerabilities are identified, triaged, and remediated quickly to protect ADB's digital banking platforms and maintain regulatory compliance.

Primary Objective: - Proactively identify and mitigate cybersecurity threats and vulnerabilities. - Coordinate with IT Infrastructure and other teams to reduce risk and maintain secure banking operations.

---

2. Single Business Process Details

2.1 Process Name

Threat Intelligence & Vulnerability Management

2.2 Key Process Activities

1. **Threat Monitoring & Analysis**
    - Subscribe to external threat feeds and gather emerging attack indicators (IOCs).
    - Correlate threat information with ADB's environment to identify potential exposures.
2. **Vulnerability Scanning & Assessment**
    - Run automated scans on servers, applications, and endpoints.
    - Analyze scan reports, prioritize vulnerabilities based on criticality, and document findings in the ticketing/SIEM system.

3. **Remediation & Patch Coordination**

    ◦ Partner with the IT Infrastructure team for timely patch deployment.
    ◦ Validate patches, retest vulnerabilities, and track progress until closure.

Note: These steps begin with receiving threat intel, move through scanning/triage, and conclude with confirmed remediation and continuous oversight.

2.3 Dependencies

- **Internal Dependencies:**

    ◦ **IT Infrastructure Team:** Deploying patches, reconfiguring systems.
    ◦ **SIEM & Ticketing Platform:** Tracking vulnerabilities and remediation tasks.
    ◦ **Core Banking / DevOps Teams:** Coordinating application security fixes.

- **External Dependencies:**

    ◦ **Threat Intelligence Feeds:** Third-party subscriptions providing updated exploit data, IOCs.
    ◦ **Vulnerability Scanner Vendor:** Ensuring scan engine updates, plugin patches for newly discovered CVEs.
    ◦ **Patch Deployment Console** (tied to internal tooling, but reliant on vendor updates for OS/application patches).

2.4 Peak Operational Periods

- **After Major Security Bulletins or Zero-Day Announcements:** Rapid scanning and remediation often spike here.
- **Monthly Patch Cycles:** Typically around vendor patch Tuesday or scheduled patch releases.
- **Post-Incident Investigation:** If a breach is detected, scanning and threat intelligence ramp up substantially.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Threat Intelligence & Vulnerability Management	12 hours	Delayed or suspended vulnerability management for more than half a day could expose ADB to critical exploits, risking compliance, financial, and reputational damage.

---

4. IT Applications

Application	RTO	RPO
Threat Intelligence Feeds (external)	12 hours	24 hours
Vulnerability Scanner	12 hours	24 hours
Ticketing / SIEM Platform	4 hours	1 hour
Patch Deployment Console	24 hours	24 hours

> **Note:** The SIEM/ticketing system requires faster recovery (4 hours) to ensure immediate tracking of active vulnerabilities and threats.

---

5. Financial Impact

- **Annual Revenue Attributable:**
  While not a direct revenue generator, strong vulnerability management underpins secure banking operations. If compromised, ADB's ability to conduct business or earn fees from transactions could be severely impacted.

- **Penalties & Costs:**
  - Potential regulatory fines for inadequate cybersecurity controls.
  - Incident response costs, breach notifications, legal liabilities.

- **Total Financial Impact (Tier):**
  High – A single unpatched critical vulnerability could lead to unauthorized transactions, data breaches, and large-scale financial loss.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Severe Official Criticism / Significant Fines	Regulatory bodies often penalize financial institutions that fail to maintain robust security, especially around known vulnerabilities.

---

7. Brand Impact

Tier	Impact Value	Rationale
4	Substantial Brand Damage	Public breaches or exploit incidents can erode trust in ADB’s neobank services, severely affecting reputation.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Moderate Operational Disruption	Staff must conduct extra manual checks and incident response if threat scanning or remediation is delayed.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Medium Impact	While direct customer interaction is limited, major unmitigated vulnerabilities lead to potential security incidents that could erode customer trust if disclosed.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Threat Intelligence & Vulnerability Management	Core Banking Operations	Vulnerability reports, required patch details	High	Yes
2	Output	Threat Intelligence & Vulnerability Management	DevOps & Deployment Pipelines	Security findings, recommended code fixes	Medium	Yes
3	Both	Threat Intelligence & Vulnerability Management	Incident Response & Forensics	Active threat data, post-incident scans, root cause analysis	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Threat Intelligence & Vulnerability Management	Compliance & Legal Department	Security posture updates, vulnerability disclosures	Medium	Yes
2	Input	Threat Intelligence & Vulnerability Management	Finance & Accounting	Budget approvals for security tools	Low	Yes
3	Both	Threat Intelligence & Vulnerability Management	Vendor Management & Procurement	SLA terms for scanning tools, security add-ons	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Threat Intelligence & Vulnerability Management	Threat Intelligence Feeds Provider	IOCs, daily/weekly threat updates	High	Yes
2	Input	Threat Intelligence & Vulnerability Management	Vulnerability Scanner Vendor	Scanner engine updates, new CVE plugins	High	Yes
3	Output	Threat Intelligence & Vulnerability Management	External Patch Providers	Patch requests, coordination with OS/app vendors	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Threat Intelligence & Vulnerability Management					X				X														

Legend - **Fridays:** Often a target for patch releases or scanning windows (since major vendor patch cycles may release mid-week). - **2nd Week of Each Month:** Commonly aligns with “Patch Tuesday” for many vendors.

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
  - Patch processes still rely on manual approvals and staging, causing delays.
  - Some vulnerability scanners lack automation hooks to auto-remediate or roll out patches instantly.
- **Budget or Resource Constraints:**
  - Limited funds for advanced real-time threat intelligence feeds or continuous scanning solutions.
  - Additional staff training or specialized certifications are pending budget approval.
- **Known Historical Incidents:**
  - A critical vulnerability remained unpatched for over a week due to incomplete scanning coverage.
  - Several near-miss phishing campaigns highlight the need for faster detection and response.

---

13. Summary for Role-Play

1. **Key Talking Points:**
    - Delays in patch deployment due to manual processes and limited budget.
    - Dependence on external threat feeds and scanner updates to catch zero-days.
    - Coordinating across multiple teams (IT, DevOps, Incident Response) can be challenging.
2. **Process Criticality:**
    - Essential for preventing data breaches, compliance fines, and reputational damage.
    - A core safeguard of ADB's digital banking operations.
3. **Data Provided:**
    - **RTO:** 12 hours for core vulnerability management functions.
    - **Financial Scale:** High potential impact if a breach occurs due to unmitigated vulnerabilities.
    - **Major Dependencies:** SIEM/Ticketing, Infrastructure patching, external threat intel.
    - **Peak Load Times:** Patch cycles, zero-day disclosures, post-incident investigations.

ROLE CARD: Legal Advisor (Subsidiary-Level)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Compliance & Legal Department

Position Description:
As the Subsidiary-Level Legal Advisor, you oversee local contract terms, interpret and adapt new regulations for ADB's digital banking services, and ensure alignment with IBC's group legal framework. You regularly consult with business units to address evolving laws, risk considerations, and compliance demands unique to online banking operations.

Primary Objective: - Ensure ADB's legal conformity and protect the company from contract or regulatory risks. - Provide prompt legal guidance on new laws, contracts, and policy changes that might affect ADB's digital operations.

---

2. Single Business Process Details

2.1 Process Name

Legal Advisory (Subsidiary-Level)

2.2 Key Process Activities

1. **Regulatory Monitoring & Assessment**
    - Track updates from the **Regulatory Bulletin Board**.
    - Review potential impact of new financial or data protection laws.
2. **Contract & Policy Review**
    - Analyze local vendor agreements, partnership contracts, and internal policies.
    - Ensure synergy with IBC group guidelines and local legal requirements.
3. **Legal Consultation & Escalation**
    - Provide counsel to internal stakeholders (e.g., Product Managers, Compliance Officer).

    - Escalate complex issues to IBC group legal or specialized external counsel as needed.

Note: This workflow often starts with scanning new regulatory bulletins, then includes proactive or reactive contract/policy reviews, culminating in official legal advice or escalations.

2.3 Dependencies

- **Internal Dependencies:**
    - **Compliance & Regulatory Audits Team:** Coordination for official filings or audits.
    - **Policy Management System:** Implementation and updates to internal policies.
    - **Departmental Consultations:** (e.g., HR, IT, Finance) seeking legal clarity on specific initiatives.
- **External Dependencies:**
    - **Regulatory Bulletin Board (Government/Industry)** for new laws or rulings.
    - **External Counsel (if escalated)** for specialized local or cross-border legal challenges.

2.4 Peak Operational Periods

- Whenever major regulatory changes are announced (e.g., new data protection laws, financial guidelines).
- Annual or quarterly contract renewals/negotiations with vendors or partners.
- Periods of intense strategic planning (e.g., expansions, product launches).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Legal Advisory (Subsidiary-Level)	48 hours	Delays beyond 2 days in legal reviews can hinder major contracts, compliance with urgent regulations, and increase legal risk for ADB.

---

4. IT Applications

Application	RTO	RPO
Legal Case Tracking	48 hours	24 hours
Regulatory Bulletin Board	72 hours	24 hours
Contract Repository	72 hours	24 hours
Policy Management System	48 hours	12 hours

> **Note:** The Legal Case Tracking system should be restored within 48 hours to manage pending legal matters. The Regulatory Bulletin Board and Contract Repository can tolerate slightly longer downtime, though extended unavailability may slow compliance efforts.

---

5. Financial Impact

- **Annual Revenue Attributable:**
  Primarily indirect; timely legal input prevents costly contract disputes or regulatory fines, thus safeguarding revenue streams.

- **Penalties & Costs:**

  - Fines or legal damages if contracts are poorly worded or new regulations aren't promptly addressed.
  - Additional legal fees if external counsel is needed due to delays or missed deadlines.

- **Total Financial Impact (Tier):**
  Medium-High – While not generating revenue, failing to provide legal guidance can lead to expensive litigation or penalties.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Severe Official Criticism / High Fines	Missing key regulatory deadlines or failing to comply with new laws can result in significant sanctions or official criticism.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Moderate Brand Damage	News of legal missteps, contract disputes, or regulatory infractions can erode public and partner trust in ADB.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Moderate Operational Disruption	If legal reviews are delayed, new initiatives stall and staff must pause or backtrack on product rollouts, vendor signings, etc.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2	Limited Direct Impact	Most customers only feel indirect effects if legal issues cause product delays or hamper user-facing services.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Legal Advisory (Subsidiary-Level)	Compliance & Regulatory Audits	Regulatory requirements, documentation	High	Yes
2	Output	Legal Advisory (Subsidiary-Level)	HR & Administration	Employment contracts, policy clarifications	Medium	Yes
3	Both	Legal Advisory (Subsidiary-Level)	Policy Management System	Updates or new policies reflecting legal changes	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Legal Advisory (Subsidiary-Level)	Finance & Accounting	Contract terms affecting payments, vendor obligations	Low	Yes
2	Input	Legal Advisory (Subsidiary-Level)	IT & Security	Guidance on data protection laws, vendor security clauses	High	Yes
3	Both	Legal Advisory (Subsidiary-Level)	Executive Leadership	Strategic expansions, contract approvals, risk assessments	High	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Legal Advisory (Subsidiary-Level)	Regulatory Bulletin Board (Govt.)	New laws, official memos, updates	High	Yes
2	Both	Legal Advisory (Subsidiary-Level)	External Counsel	Specialized legal opinions, escalated case handling	Medium	Yes
3	Input	Legal Advisory (Subsidiary-Level)	Contract Repository Vendor	Secure storage or hosting updates, compliance checks	Low	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Legal Advisory (Subsidiary-Level)				X	X			X						X									X

Legend: - **Thursdays/Fridays:** Common days for finalizing contract reviews or addressing urgent legal inquiries before weekend. - **1st Week / March / December:** Common periods for new regulations or contract renewals (e.g., end-of-fiscal-year activities).

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
  - Some contract redlining is done manually; advanced contract lifecycle management tools are under evaluation.
  - Regulatory bulletins are sometimes only partially automated, requiring manual classification of potential legal impacts.
- **Budget or Resource Constraints:**
  - Additional external counsel might be needed if the legal team is overloaded.
  - Further integration between the Contract Repository and Policy Management System is pending.
- **Known Historical Incidents:**
  - A major contract’s renewal was delayed due to last-minute legal clarifications, causing tension with a key vendor.
  - A short-lived data protection compliance gap resulted in an official warning from a local authority.

---

13. Summary for Role-Play

1. **Key Talking Points:**
    - Timeliness of legal reviews can prevent compliance infractions or expensive contractual disputes.
    - Heavy reliance on the Regulatory Bulletin Board for updates, with potential manual classification.
    - Coordination with multiple departments for policy, contract, and risk oversight.
2. **Process Criticality:**
    - Essential for mitigating legal/regulatory risk and ensuring that ADB's digital banking initiatives adhere to local and group-level requirements.
    - Delays can jeopardize vendor relationships, compliance, or strategic decisions.
3. **Data Provided:**
    - **RTO:** 48 hours for Legal Advisory workflows.
    - **Financial Scale:** Medium-High (indirect but can prevent large penalties or litigation costs).
    - **Major Dependencies:** Regulatory updates, contract repository, internal policy management.
    - **Peak Load Times:** Major regulatory changes, contract renewal seasons, year-end compliance rush.

ROLE CARD: IT Manager (Core Banking Operations)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
IT & Security Department, collaborating closely with the Infrastructure Lead

Position Description:
As the IT Manager overseeing **Core Banking Operations**, you maintain ADB's primary ledger systems, ensure transaction integrity, and uphold performance standards essential for daily banking functions. Your duties include orchestrating DevOps pipelines for core banking software updates, managing system resiliency, and coordinating patch management across critical applications.

Primary Objective:
Safeguard the continuous operation of ADB's core ledger, preserving real-time account balances and transaction records while ensuring minimal downtime and robust data protection.

---

2. Single Business Process Details

2.1 Process Name

Core Banking Operations

2.2 Key Process Activities

1. **System Administration & Ledger Management**
    - Oversee the main ledger application, ensuring accurate debits/credits, up-to-date customer account information, and consistent transaction records.
    - Perform routine tasks (e.g., database backups, log reviews) to preserve data integrity.
2. **Performance and Resiliency Coordination**
    - Monitor system health, track throughput, and respond to alerts signaling increased loads or performance degradations.
    - Collaborate with Infrastructure Leads to maintain high availability configurations (redundancy, failover clustering).
3. **DevOps Pipeline Integration**
    - Manage CI/CD workflows for updates to the core banking software, testing patches and new features before release.

    - Communicate with DevOps teams to schedule deployments that minimize production disruptions.

Note: The process aims to keep account ledgers continuously operational. Any extended downtime affects daily banking operations, user transactions, and back-office reconciliations.

2.3 Dependencies

- **Internal Dependencies:**
    - **Database systems** (high-availability clusters for transaction data).
    - **DevOps pipelines** (CI/CD environment delivering updates/patches).
    - **Patch management processes** (internal tool distributing software updates).
    - **AML/Fraud Check Modules** (reads/writes data from the core ledger).
- **External Dependencies:**
    - **None direct** for the ledger itself, but certain clearing or cross-entity interactions rely on accurate ledger status (e.g., payment gateways or inter-bank settlement eventually query ledger data).

2.4 Peak Operational Periods

- **End-of-Day/Month Closings:** Transaction volumes often spike as daily or monthly batch jobs finalize.
- **Major System Release Windows:** Occasionally see heavier load or partial slowdowns, requiring thorough planning to avoid impacting normal operations.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Core Banking Operations	4 Hours	Extended downtime halts account updates, preventing day-to-day transactions. By 4 hours, backlog becomes critical and user trust erodes.

---

4. IT Applications

Application	RTO	RPO
Core Banking System	4 Hours	15 Min
Database Cluster	4 Hours	0 Min (real-time sync)
DevOps Pipeline	4 Hours	30 Min
Patch Management Console	4 Hours	15 Min

(RPO times reflect how quickly data changes must be captured to prevent significant transaction loss.)

---

5. Financial Impact

- **Annual Revenue Attributable**: The entire neobank's transaction base relies on this ledger; disruptions risk hundreds of millions in transaction-based fees or interest computations.
- **Penalties & Costs**: Missed transaction updates may create settlement mismatches, incurring fines or rework.
- **Total Financial Impact (Tier)**: Likely Tier 1 or Tier 2, considering major revenue and operational significance.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism/Some Fines	Prolonged downtime leads to potential scrutiny by regulatory bodies for misreporting or incomplete ledgers.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	Customers quickly lose faith if account balances fail to update, causing negative press or social media chatter.

---

8. Operational Impact

Tier	Impact Value	Rationale
2	There are only a select few who know the process	Specialized knowledge around the ledger's intricacies is concentrated in a small IT group.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2	Significant Impact	Customers depend on timely ledger updates to verify their balances; confusion arises rapidly during downtime.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Output	Core Banking Operations	AML/Fraud Modules	Transaction details and status	High	Yes
2	Output	Core Banking Operations	Accounting & Finance	Daily ledger records, reconciliation	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Core Banking Operations	Compliance & Regulatory Audits	System logs, transaction data sets	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Output	Core Banking Operations	None Direct	N/A	N/A	N/A

(Primarily an internal ledger system, though final settlement data can eventually feed external partners.)

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Core Banking Operations	X	X	X	X	X	-	-	-	-	-	-	-	-	X	-	-	-	-	X	-	-	X	X

(Business days heavily used; end-of-month or end-of-quarter produce data spikes for statements.)

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Database patching requires partial downtime and manual sign-offs.
- **Budget or Resource Constraints**: Proposed expansions to database cluster or improved high-availability approaches remain pending due to resource debates.
- **Known Historical Incidents**: A 2-hour outage last quarter disrupted thousands of in-progress transactions, resulting in customer complaints and forced manual ledger corrections.

---

13. Summary for Role-Play

1. **Key Talking Points**
    - The ledger is the heart of day-to-day ADB operations: if it's down, all transactions are effectively on hold.
    - Only a select core team intimately understands the entire system, complicating after-hours or urgent recovery.
2. **Process Criticality**
    - Directly tied to revenue, compliance (accurate recordkeeping), and brand confidence (customers must see real-time balances).
    - Extended downtime jeopardizes daily closings, cross-department tasks, and consolidated financial statements.

3. **Data Provided**

    - RTO of 4 hours and near-real-time RPO indicates minimal tolerance for both downtime and data loss.
    - Tier 1–2 financial significance, Tier 2 for regulatory compliance (potential official criticisms/fines), Tier 3 brand damage if recurring.

ROLE CARD: CEO and CFO (Governance & Executive Oversight)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Executive Leadership

Position Description:
As the CEO and CFO team for Alderaan Digital Banking (ADB), you provide **top-level governance and executive oversight** for the entire neobank. You set strategic direction, approve major budgets, and decide on significant expansions or partnerships. Your roles demand ensuring accurate, real-time visibility into ADB's operations, assessing risk dashboards, and maintaining alignment with the parent organization, IBC.

Primary Objective:
Guide ADB's strategic growth and financial health through informed decision-making, balancing profitability, compliance, and brand reputation.

---

2. Single Business Process Details

2.1 Process Name

Governance & Executive Oversight

2.2 Key Process Activities

1. **Strategic Planning & Budget Approvals**
    - Review annual budget proposals from each department, prioritizing investments in infrastructure, security measures, or expansion.
    - Evaluate long-term business plans and propose or endorse new products or market entries.
2. **Performance & Risk Monitoring**
    - Analyze risk dashboards and compliance insights to identify threats or process bottlenecks.
    - Engage with department heads when critical KPIs underperform, intervening if necessary.

3. **Executive Decision-Making & Communication**
    - Present consolidated strategies and financial updates to IBC's board or relevant stakeholders.
    - Oversee corporate governance tasks (board meetings, top-level policy reviews, acquisitions).

Note: Failure to maintain robust governance can result in misaligned strategies, underfunded essential programs, or heightened risk exposures that threaten ADB's stability.

2.3 Dependencies

- **Internal Dependencies:**
- **Accurate Reporting from All Process Owners** (loan origination data, transaction volumes, compliance status, etc.).
- **Risk Dashboards** (pulling from SIEM, AML checks, or operational metrics).
- **Compliance Insights** (Legal & Regulatory teams).
- **External Dependencies:**
- **IBC Group Policies** (ensuring synergy with parent institution's guidelines).
- **Regulators** (periodic supervisory requirements that the executive team must satisfy).

2.4 Peak Operational Periods

- **Quarterly Board Reviews**: Preparation for board-level or stakeholder meetings.
- **Year-End Budget Finalizations**: Decision-making on budget allocations, expansions, or major acquisitions.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Governance & Executive Oversight	2 Days	Prolonged disruption means inability to approve budgets or respond to critical risks. Beyond 2 days, high-level decisions stall, risking strategic and compliance failures.

---

4. IT Applications

Application	RTO	RPO
Executive Dashboard	2 Days	6 Hours
Risk/Compliance Reporting Tool	1 Day	1 Hour
Board Meeting Portal	2 Days	6 Hours

(These solutions aggregate performance KPIs, risk alerts, and compliance findings for the executive team.)

---

5. Financial Impact

- **Annual Revenue Attributable**: Indirect. The CEO and CFO's decisions shape resource distribution and strategic expansions that eventually drive ADB's revenue.
- **Penalties & Costs**: Misguided or delayed executive approvals can lead to missed growth opportunities, compounding inefficiencies, or compliance fines if high-risk exposures go unresolved.
- **Total Financial Impact (Tier)**: Potentially Tier 2 or Tier 1 because executive paralysis might ripple across multiple revenue-generating or regulatory processes.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism/Some Fines	Prolonged oversight failures can expose ADB to official warnings or penalties if compliance is neglected.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	Leadership inaction or delayed expansions may erode confidence in ADB's direction.

---

8. Operational Impact

Tier	Impact Value	Rationale
2	There are only a select few who know the process	Top executives make cross-functional calls; few can stand in if governance is stalled.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	Little Impact	Customers rarely see direct exec decisions unless large delays cascade into operational processes.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Governance & Executive Oversight	Loan Origination, Payments	Performance data, expansions requests	High	Yes
2	Input	Governance & Executive Oversight	Compliance & Legal	Regulatory risk overviews, policy changes	Medium	Yes
3	Output	Governance & Executive Oversight	All Divisions	Budget approvals, strategic directives	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Governance & Executive Oversight	Finance & Accounting	Funding for projects, expansions	Medium	Yes
2	Input	Governance & Executive Oversight	HR & Administration	High-level staff or policy changes	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input/Output	Governance & Executive Oversight	IBC Board or Regulators	Periodic presentations, compliance documents	High	Yes
2	Input/Output	Governance & Executive Oversight	Strategic Partners	Negotiations for major partnerships or expansions	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Governance & Executive Oversight	-	-	-	-	-	-	-	X	-	X	X	-	-	-	X	-	-	-	X	-	-	X	X

(Board cycles may align with monthly or quarterly intervals, plus year-end budgeting during Q4.)

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Some strategic decisions rely heavily on manual data collation from different units, risking incomplete or outdated info.
- **Budget or Resource Constraints**: If expansions or upgrades are not prioritized, certain critical processes remain underfunded or at risk.
- **Known Historical Incidents**: In the prior fiscal year, delayed CFO sign-off on an infrastructure upgrade led to performance bottlenecks during a peak transaction surge.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Executive-level decisions shape all ADB processes, especially expansions or major risk mitigation budgets.
    - Stalled leadership approvals can exacerbate security or compliance vulnerabilities.
2. **Process Criticality**:
    - Vital for setting strategic direction, allocating resources, and meeting IBC or regulatory expectations.
    - Without timely oversight, departmental silos or budget shortfalls could cause systemic issues.

3. **Data Provided**:

    - RTO of 2 Days: Extended leadership inactivity quickly hampers cross-department workflows, risking missed strategic or regulatory deadlines.
    - Tier 2–3 financial or brand impact possible, but could escalate if critical expansions or crisis decisions are delayed.

ROLE CARD: Loan Origination and Underwriting Manager

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Loans & Credit Division

Position Description:
As the Loan Origination and Underwriting Manager, you oversee the end-to-end lending process for Alderaan Digital Banking. This includes processing digital applications, coordinating credit scores, and ensuring compliance with local lending regulations. Your role is crucial for maintaining a swift, secure, and customer-friendly lending experience while minimizing default risks.

Primary Objective:
Facilitate timely and accurate loan approvals by leveraging automated credit checks, thorough compliance reviews, and a robust underwriting workflow, ensuring ADB meets revenue targets while maintaining regulatory compliance.

---

2. Single Business Process Details

2.1 Process Name

Loan Origination and Underwriting

2.2 Key Process Activities

1. **Digital Form Submission**
    - Applicants complete an online loan application via the Loan Application Portal.
    - Basic personal and financial details are captured, and initial identity checks occur.
2. **Credit Scoring & Risk Assessment**
    - The Credit Scoring Engine evaluates applicant creditworthiness, referencing internal and external data sources.
    - Potential fraud or compliance red flags trigger more in-depth reviews.

3. **Underwriting Workflow**
    - The Underwriting Workflow System orchestrates approvals, highlighting anomalies (like high debt ratios).
    - Approved applications are passed to the Compliance Check Module for final AML/KYC validations before official disbursement.

Note: Each step must be seamless to provide a quick, positive customer experience.

2.3 Dependencies

- **Internal Dependencies:**
    - **Compliance Check Module** (for AML/KYC checks)
    - **Finance & Accounting Department** (final disbursement, interest accrual settings)
    - **IT & Security Department** (ensures system uptime, data integrity)
- **External Dependencies:**
    - **Credit Scoring Engine** (may be a third-party or advanced analytics vendor)
    - **Identity Verification Services** (if separate from the standard eKYC process)
    - **Regulatory Bodies** (local lending rules, interest caps, or data retention mandates)

2.4 Peak Operational Periods

- **Month-End**: Surge in applications as salaries arrive and people decide on personal/short-term loans.
- **Year-End Holidays**: Higher demand for consumer loans for shopping or travel.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Loan Origination and Underwriting	4 Hours	Prolonged downtime beyond 4 hours stalls loan approvals, risking customer attrition and lost revenue.

---

4. IT Applications

Application	RTO	RPO
Loan Application Portal	4 Hours	1 Hour
Credit Scoring Engine	2 Hours	30 Min
Underwriting Workflow System	4 Hours	1 Hour
Compliance Check Module	4 Hours	1 Hour

---

5. Financial Impact

- **Annual Revenue Attributable**:
  - Loan interests and associated fees represent a substantial revenue stream—potentially **tens of millions of credits** annually.
- **Penalties & Costs**:
  - If compliance checks fail or are bypassed during downtime, ADB risks fines from regulators.
  - Delayed underwriting means potential loan cancellations or customer churn.
- **Total Financial Impact (Tier)**:
  - **Tier 3-4** (Medium-High). Extended disruptions lead to lost loan opportunities and possible fines, but short disruptions may be recoverable.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Criticism & Potential Fines	Non-compliance with local lending laws or AML checks may attract regulatory attention.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Moderate Brand Damage	Customers may lose confidence if loan approvals stall, tarnishing ADB’s image of efficiency.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Moderately High Ops Disruption	Manual underwriting would be slow, staff might be overwhelmed with backlog, risking errors.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Noticeable Dissatisfaction	Applicants expect quick decisions; long delays hurt satisfaction and might prompt them to switch to competitors.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Loan Origination & Underwriting	Compliance & Regulatory Audits	AML/KYC validation records	High	Yes
2	Output	Loan Origination & Underwriting	Finance & Accounting	Approved loan data, interest details	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Loan Origination & Underwriting	Marketing & Customer Engagement	Status of loan offers/ campaign leads	Medium	Yes
2	Output	Loan Origination & Underwriting	HR & Administration	Access/permissions updates for staff	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Loan Origination & Underwriting	Credit Scoring Engine Vendor	Credit score data, risk flags	High	Yes
2	Input/Output	Loan Origination & Underwriting	External ID Verification APIs	Additional identity/fraud checks	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Loan Origination & Underwriting	X	X	X	X	X	*	*																

- **Legend:**
  - **X** = Typical daily volume (Mon-Fri)
  - ***** = Some weekend spikes if promotions or ad campaigns run

---

12. Additional Observations

- **Automation Gaps / Manual Steps**:
  - If the Credit Scoring Engine or Underwriting Workflow is down, manual underwriting is slow and prone to error.
- **Budget or Resource Constraints**:
  - Additional advanced analytics modules for credit risk are pending approval.
- **Known Historical Incidents**:
  - A 2-day engine outage last year resulted in a backlog of 3,000 applications—some potential borrowers turned to competitors.

---

13. Summary for Role-Play

1. **Key Talking Points**:
   - Ensuring swift credit scoring with minimal downtime.
   - Importance of compliance checks to avoid legal blowback.
   - External vendor reliability (Credit Scoring Engine, ID verification).

2. **Process Criticality**:

    - Loan revenue is a large portion of ADB's profits.
    - Slow or suspended approvals damage brand perception and reduce net new business.

3. **Data Provided**:

    - **RTO**: 4 Hours for the overall process.
    - **Financial Scale**: Potentially tens of millions of credits in annual loan interest revenue.
    - **Dependencies**: Credit Scoring Engine (external), AML compliance.
    - **Peak Load**: End of month and holiday campaigns see higher application volumes.

ROLE CARD: DevOps Engineer (DevOps & Deployment Pipelines)

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
IT & Security Department (DevOps & Deployment Pipelines)

Position Description:
The DevOps Engineer is responsible for automating code builds, managing container orchestration, and facilitating end-to-end CI/CD for all internal applications. This ensures fast, reliable software deployments across ADB's environment, supporting agile product releases and security updates.

Primary Objective: - Maintain efficient, secure, and scalable deployment pipelines. - Minimize downtime and deployment errors through automation and continuous integration practices.

---

2. Single Business Process Details

2.1 Process Name

DevOps & Deployment Pipelines

2.2 Key Process Activities

1. **Automated Code Builds:**
    - Integrate changes from developers into a central repository.
    - Compile, test, and package applications using CI/CD tools.
2. **Container Orchestration & Deployment:**
    - Configure and manage containers (e.g., Docker) within Kubernetes or similar orchestration platforms.
    - Scale services as needed, monitor container health, and perform rolling updates.
3. **CI/CD Pipeline Coordination:**
    - Enforce QA sign-offs, security checks, and post-deployment validations.

    - Collaborate with development and security teams to incorporate automated testing, vulnerability scanning, and rollback procedures if issues arise.

Note: These activities start with code integration, move through build/test phases, and culminate in production deployments with post-release monitoring.

2.3 Dependencies

- **Internal Dependencies:**
    - **Security Code Scanning** (cybersecurity team provides or configures scanning solutions)
    - **QA Sign-Offs** (QA team validates quality and functionality)
    - **Application Owners** (e.g., Mobile Banking Product Manager, Core Banking Manager) for release timing and acceptance criteria
- **External Dependencies:**
    - **Container Orchestration Platform** (could be cloud-managed Kubernetes)
    - **Source Control Service** (hosted Git repositories, possibly external)
    - **Artifact Repository** (could be an external hosted solution, e.g., Nexus or Artifactory)

2.4 Peak Operational Periods

- **Product Release Windows:** Weekly or bi-weekly sprints.
- **Emergency Hotfix Scenarios:** Any time a critical bug or security patch must be pushed urgently.
- **Quarterly or Seasonal High-Traffic Deployments:** (e.g., major ADB feature launches, year-end promotions).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
DevOps & Deployment Pipelines	8 hours	If this pipeline is down for more than 8 hours, critical patches and new features cannot be deployed, risking security exposures, lost revenue, and potential reputational harm.

---

4. IT Applications

Application	RTO	RPO
CI/CD Server (Jenkins, GitLab CI, etc.)	8 hours	4 hours
Container Orchestration Platform (Kubernetes)	12 hours	4 hours
Source Control (Git)	8 hours	4 hours
Artifact Repository	12 hours	8 hours

> **Note:** Continuous integration services are vital to building and testing code swiftly. Source control must be restored quickly to prevent code loss or conflicts.

---

5. Financial Impact

- **Annual Revenue Attributable:**
  While not directly generating revenue, stable and continuous deployment pipelines allow quick feature releases and security fixes—indirectly supporting all revenue streams.

- **Penalties & Costs:**

  - Delayed security patches may result in breach-related costs or fines.
  - Prolonged downtime in deployment pipelines can lead to missed market opportunities, increasing operational overhead.

- **Total Financial Impact (Tier):**
  Medium-High – Extended outages can impact multiple lines of business simultaneously, but the exact monetary loss varies based on pending releases and security fixes.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Concern / Moderate Fines Possible	If the inability to deploy critical updates leads to regulatory non-compliance (e.g., missing patches for secure banking), regulators may impose penalties.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Moderate Brand Damage	If major feature updates or security patches are delayed, customer confidence can waver, though not as visibly as a front-end outage.

---

8. Operational Impact

Tier	Impact Value	Rationale
4	High Operational Disruption	Dev, QA, and Security teams rely heavily on automated pipelines; manual workarounds are time-consuming and error-prone.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2	Low to Moderate Impact	Customers indirectly feel the impact if important updates or bug fixes are delayed. Direct dissatisfaction is lower unless widespread production issues occur.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	DevOps & Deployment Pipelines	Cybersecurity (Threat Scanning)	Vulnerability scan results, code analysis	High	Yes
2	Output	DevOps & Deployment Pipelines	Mobile & Web App Management	New app builds, updated code, release artifacts	High	Yes
3	Both	DevOps & Deployment Pipelines	Core Banking Operations	Core code updates, patches, feedback on performance	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	DevOps & Deployment Pipelines	QA / Testing Team	Test cases, sign-offs, performance metrics	High	Yes
2	Output	DevOps & Deployment Pipelines	Compliance & Legal	Verification that production environment meets compliance guidelines	Medium	Yes
3	Both	DevOps & Deployment Pipelines	Finance / Accounting	Budget requests for additional pipeline tooling or container hosts	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	DevOps & Deployment Pipelines	Source Control Provider (Git Hosting)	Repository data, commits, branch merges	High	Yes
2	Input	DevOps & Deployment Pipelines	Cloud/Hosting Provider (Kubernetes)	Container orchestration, scaling resources	Medium	Yes
3	Output	DevOps & Deployment Pipelines	Artifact Repository Vendor	Build artifacts, Docker images, versioning	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
DevOps & Deployment Pipelines	X	X			X				X					X									

Legend: - **Mondays/Tuesdays/Fridays:** Common sprint-end or mid-sprint integration days. - **2nd Week / March:** Often release windows for bigger features or quarter-end.

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
  - Some manual approvals still exist for production deployments and container scaling.
  - Regression testing occasionally requires manual oversight when automated tests fail or have false positives.
- **Budget or Resource Constraints:**
  - Additional container orchestration capacity or advanced CI/CD plugin features require more funding.
  - Considering expansion to multi-cluster setups for high availability, pending budget.
- **Known Historical Incidents:**
  - A major build pipeline outage once delayed a critical security patch for 24 hours, exposing a minor vulnerability.
  - A container registry misconfiguration led to a rollback, causing partial downtime during a high-traffic launch.

---

13. Summary for Role-Play

1. **Key Talking Points:**
    - Pipeline disruptions directly delay security patches and new features.
    - Dependencies on QA and cybersecurity scanning can create release bottlenecks.
    - Budget constraints for scaling container orchestration or advanced CI/CD functionalities.
2. **Process Criticality:**
    - Fundamental to all software deployments within ADB.
    - Any downtime hinders new service rollouts, bug fixes, and regulatory compliance updates.
3. **Data Provided:**
    - **RTO:** 8 hours for DevOps & Deployment Pipelines.
    - **Financial Scale:** Medium-High (indirectly supports multiple revenue channels).
    - **Major Dependencies:** QA sign-offs, cybersecurity scans, container orchestration environment.
    - **Peak Load Times:** Product release days, emergency patch cycles, end-of-quarter feature rollouts.

ROLE CARD: Head of UX and Customer Onboarding

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Online Transactions & Payments Division (specifically focuses on user-facing onboarding processes)

Position Description:
This role leads the **Online Account Opening** process, ensuring new customers can swiftly create accounts through ADB's digital platform. The Head of UX and Customer Onboarding supervises everything from initial identity checks (eKYC) to final credential setup, partnering with compliance and IT for secure, user-friendly experiences.

Primary Objective:
Facilitate a **seamless, compliant**, and **secure** onboarding path that meets regulatory standards for identity verification while providing an intuitive user journey.

---

2. Single Business Process Details

2.1 Process Name

Online Account Opening

2.2 Key Process Activities

1. **User Registration & Identity Capture**
    - Prospective clients input personal details, upload ID documents/photos.
    - The system cross-references the HR Access Control Database for policy alignment (ensuring correct identity fields are captured).
2. **eKYC & Automatic Verification**
    - The uploaded ID is scanned via the **ID Scan & OCR Tool**.
    - The **eKYC Verification System** checks for authenticity, verifying it against watchlists or sanction lists.

3. **Account Creation & Credential Setup**
    - On successful verification, the **Customer Onboarding Portal** generates account credentials.
    - Creates an initial user profile in the core bank environment, referencing legal for any data privacy disclaimers.

Note: Failure or delay in any step can cause friction, leading to user drop-off or compliance issues.

2.3 Dependencies

- **Internal Dependencies:**
    - **Legal** (ensuring data privacy disclaimers & T&Cs).
    - **HR** (for policy references on capturing personal details).
    - **IT Security** (ensuring secure transport and storage of ID documents).
- **External Dependencies:**
    - **eKYC Verification System** (third-party vendor's API).
    - **ID Scan & OCR Tool** (another external solution integrated into the portal).
    - **Cloud provider** (hosting the Customer Onboarding Portal).

2.4 Peak Operational Periods

- Typically during **weekday mornings** (prospective customers often open accounts early in the day).
- **Marketing campaigns** can spike registrations sporadically (e.g., promotional launch periods or ad campaign weeks).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Online Account Opening	4 hours	If new accounts cannot be opened for more than half a business day, ADB loses growth momentum and potential brand reputation as a "swift neobank". Also, regulatory concerns arise if existing eKYC verifications are left pending.

---

4. IT Applications

Application	RTO	RPO
Customer Onboarding Portal	4 hrs	2 hrs
eKYC Verification System (Vendor)	4 hrs	1 hr
ID Scan & OCR Tool	6 hrs	2 hrs
HR Access Control Database	6 hrs	4 hrs

(RTO/RPO here reflect the perspective of Online Account Opening's tolerance. Other processes might have different requirements.)

---

5. Financial Impact

- **Annual Revenue Attributable**: The bank targets 30% annual growth from new accounts. Losing 1 day of sign-ups could cost tens of thousands of credits in potential deposit inflows.
- **Penalties & Costs**: If eKYC fails or lags, there might be compliance fines (modest, but brand harming if repeated).
- **Total Financial Impact (Tier)**: **Medium**. The direct revenue from new sign-ups may be moderate, but potential brand damage can amplify long-term losses.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism / Possible Minor Fines	If eKYC or account creation fails, ADB might face warnings from regulators. Repeated non-compliance could escalate.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Substantial Temporary Brand Damage	A failed or severely delayed onboarding process can tarnish ADB's image as a "quick & digital" service provider.

---

8. Operational Impact

Tier	Impact Value	Rationale
2	Some Additional Workarounds	If the portal fails, staff can attempt manual or email-based onboarding, but it’s inefficient and prone to errors.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Noticeable Frustration / Public Complaints	Customers expect an instant account creation experience. Delays or failure may quickly push them to competitors.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Online Account Opening	Core Banking Operations	Customer details for ledger creation	High	Yes
2	Output	Online Account Opening	IT & Security Department	Logging, security checks, encryption keys	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	Online Account Opening	Compliance & Legal	eKYC guidelines, disclaimers	High	Yes
2	Output	Online Account Opening	Marketing & Customer Eng.	Customer data for onboarding campaigns	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Online Account Opening	eKYC Verification Provider	ID validation results	High	Yes
2	Input	Online Account Opening	ID Scan & OCR Vendor	OCR data + authenticity checks	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Online Account Opening	*	*	*	*	***	**	*	*	*	*	**	*	*	*	*	*	*	*	*	*	*	*	***

Legend: *** indicates peak (often end of month or promotional campaigns).

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Certain exceptions (e.g., unusual ID formats) get handled manually by a small ops team, potentially causing backlogs.
- **Budget or Resource Constraints**: Funding is available for major improvements, but depends on corporate approval from IBC.
- **Known Historical Incidents**: A short eKYC outage last quarter caused over 150 prospective accounts to drop off.
- **Security**: Minimal intrusion detection on the portal itself; relies heavily on vendor side checks.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Potential eKYC vendor downtime, manual fallback.
    - Marketing pushes can overload the system.
    - Ensuring legal disclaimers are in place.
2. **Process Criticality**:
    - Essential for ADB’s growth and brand image as an entirely digital bank.

3. **Data Provided**:

    - RTO: 4 hours (longer downtime jeopardizes new account sign-ups).
    - Financial Impact: Medium tier but crucial for expansions.
    - Dependencies: eKYC vendor is high impact.

As the **Head of UX and Customer Onboarding**, you'd emphasize that quick, frictionless onboarding is essential to Alderaan Digital Banking's identity, but also reliant on external APIs and internal compliance checks.

ROLE CARD: Head of Online Transactions

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Online Transactions & Payments Division

Position Description:
As the Head of Online Transactions, you oversee all digital payments and real-time transfers at Alderaan Digital Banking. Your role ensures seamless operation of card transactions, interbank clearing, and fraud checks. You collaborate closely with external payment gateways, card networks, and ADB's internal Real-Time Settlement Engine to guarantee uninterrupted transaction flows.

Primary Objective:
Maintain continuity and security of digital payments and P2P transfers, ensuring compliance with AML guidelines and minimizing transaction failures that could damage ADB's reputation and revenue.

---

2. Single Business Process Details

2.1 Process Name

Digital Payments & Transfers

2.2 Key Process Activities

1. **Transaction Initiation & Authorization**
    - Customer initiates a digital payment or P2P transfer.
    - Payment Gateway Platform validates credentials and payment details.
2. **Fraud/AML Screening**
    - The Fraud Detection Module checks for suspicious patterns or flagged accounts.
    - If any risk is detected, the transaction is held for review.
3. **Real-Time Settlement & Clearing**
    - The Real-Time Settlement Engine verifies account balances internally.

    - The Clearinghouse Connector interfaces with external or national clearing networks for final settlement.

Note: Most transactions flow through in seconds, requiring extremely high uptime to satisfy customer expectations.

2.3 Dependencies

- **Internal Dependencies:**
    - **Fraud Detection Module** for AML checks
    - **Core Banking System** for validating balance/ledger updates
    - **IT & Security Department** for stable network and transaction logs
- **External Dependencies:**
    - **Payment Gateway Platform** (external vendor for card and online payments)
    - **Card Networks** (Visa/Mastercard or local schemes)
    - **Clearinghouse Connector** (APIs to interbank clearing network)
    - **AML Vendor Feeds** (if any external data is used for advanced fraud scoring)

2.4 Peak Operational Periods

- **Weekdays** (Mon-Fri) 9:00–18:00 local time typically see the highest volume.
- **Month-End** (1–2 days) often surges in bill payments and salary disbursements.
- **Holiday Seasons** (varies) can see elevated P2P gifting and e-commerce transactions.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Digital Payments & Transfers	2 Hours	If payments go offline beyond 2 hours, ADB faces significant revenue loss, customer dissatisfaction, and potential fines.

---

4. IT Applications

Application	RTO	RPO
Payment Gateway Platform	2 Hours	0 (near real-time)*
Real-Time Settlement Engine	2 Hours	0–30 Minutes
Fraud Detection Module	4 Hours	30 Minutes
Clearinghouse Connector	2 Hours	0 (real-time data)

*Note: Some card networks may require zero data loss (0 RPO) for transaction logs to ensure dispute resolution.

---

5. Financial Impact

- **Annual Revenue Attributable:**
  - A substantial portion of ADB's transactional revenue stems from fees on payments and transfers. Estimates can exceed **millions of credits** annually.
- **Penalties & Costs:**
  - Extended downtime (beyond 2 hours) risks SLA breaches with partner card networks, incurring potential penalty fees.
  - Regulatory fines possible if AML checks fail to execute during downtime.
- **Total Financial Impact (Tier):**
  - **Tier 4** (High impact) – Each hour of downtime can lead to high lost transaction fees and potential non-compliance fines.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
4	Significant Regulatory Penalties	Failure to process AML checks or meet clearing obligations can lead to official sanctions/fines.

---

7. Brand Impact

Tier	Impact Value	Rationale
4	High Brand Damage	Publicized payment failures shake customer confidence and tarnish ADB's online-only reputation.

---

8. Operational Impact

Tier	Impact Value	Rationale
4	Major Operational Disruption	Payment Operations staff must manually reconcile partial data, or handle complaints and backlog.

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	Severe Customer Dissatisfaction	Payment delays or rejections cause users to lose trust quickly, risking churn or negative social media.

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Digital Payments & Transfers	Core Banking Operations	Account balance validation, ledger updates	High	Yes
2	Input	Digital Payments & Transfers	Fraud Detection & AML Checks	Alerts, flagged transactions	High	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input/Output	Digital Payments & Transfers	Compliance & Legal Department	Reports on suspicious or large transactions	Medium	Yes
2	Output	Digital Payments & Transfers	Finance & Accounting Department	Transaction volume data, fees collected	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Output	Digital Payments & Transfers	Payment Gateway Vendor	Authorization requests/ responses	High	Yes
2	Output	Digital Payments & Transfers	Card Networks (e.g., Visa/ Mastercard)	Clearing, transaction confirmations	High	Yes
3	Input/Output	Digital Payments & Transfers	National Clearinghouse	Settlement instructions, daily net positions	High	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Digital Payments & Transfers	X	X	X	X	X	*	*																

- **Legend:**
  - **X** = High daily transactions
  - ***** = Moderate but can spike due to weekend e-commerce

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
  - If the Real-Time Settlement Engine fails, partial manual input may be needed for reprocessing or dispute resolution.
- **Budget or Resource Constraints:**
  - New AML enhancements are pending budget approval, which might enhance automated fraud detection.
- **Known Historical Incidents:**
  - A 30-minute outage last quarter led to ~5,000 pending transactions that had to be manually reconciled, highlighting the risk of extended downtime.

---

13. Summary for Role-Play

1. **Key Talking Points**:
   - **Real-Time Settlement** must not exceed 2-hour downtime.
   - **Fraud/AML** checks rely heavily on external vendor uptime.
   - **Clearinghouse** dependencies can cause compounding delays if disrupted.

2. **Process Criticality**:

    - High revenue generation via per-transaction fees.
    - Failing real-time payments tarnishes ADB’s standing as a swift digital bank.

3. **Data Provided**:

    - **RTO**: 2 Hours
    - **Financial Scale**: Millions in annual fees; thousands of transactions/hour
    - **Dependencies**: Payment Gateway, Card Networks, Clearinghouse, Fraud Module
    - **Peak Periods**: Weekdays, plus end-of-month spikes

ROLE CARD: Payment Clearing and Settlement Lead

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Online Transactions & Payments Division (focusing on **Cross-Border Transaction & Clearing**)

Position Description:
This role manages the intricate end-to-end process for cross-border transactions, ensuring smooth interaction with national and international clearinghouses. The Payment Clearing and Settlement Lead coordinates with internal IT (especially for SWIFT and clearing connectors) and external entities like foreign banks and currency exchanges. They also oversee currency settlement runs, verifying that AML checks and compliance guidelines are met.

Primary Objective:
Guarantee **timely, accurate, and compliant** settlement of cross-border transactions in multiple currencies, minimizing delays and brand risks tied to clearance bottlenecks.

---

2. Single Business Process Details

2.1 Process Name

Cross-Border Transaction & Clearing

2.2 Key Process Activities

1. **SWIFT Messaging & Validation**
    - Prepare outgoing payment instructions or receive inbound ones.
    - Use the **SWIFT Interface** to format and transmit messages securely.
2. **Multi-Currency Clearing**
    - Use the **Clearinghouse Connector** (internal) to coordinate with domestic or international clearing networks.
    - Conduct AML checks in collaboration with compliance.

3. **FX Conversion & Settlement Runs**
    - Employ the **FX Conversion Engine** to manage real-time or scheduled currency conversions.
    - Invoke the **Settlement Scheduler** for daily or real-time netting of transactions, confirming final balances.

2.3 Dependencies

- **Internal Dependencies:**
    - **IT Manager** (for system maintenance of clearinghouse interfaces).
    - **Compliance & Legal** (AML oversight, regulatory alignment).
    - **Finance & Accounting** (reconciliation of settlement amounts in official books).
- **External Dependencies:**
    - **SWIFT** (international messaging network).
    - **National/Regional Clearinghouses** (interbank or cross-border settlement).
    - **FX Data Providers** (live currency feeds, possibly re-checking rates).

2.4 Peak Operational Periods

- **End-of-Business Days** (time-sensitive settlement runs).
- **Month-End** (increased volume for corporate transactions).
- **Quarter Ends** (foreign currency exposures often heavier, leading to more conversions).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Cross-Border Transaction & Clearing	4 hours	If clearing is offline over half a business day, it disrupts corporate remittances, incurring brand damage and potential regulatory issues for unprocessed payments.

---

4. IT Applications

Application	RTO	RPO
SWIFT Interface	4 hrs	2 hrs
Clearinghouse Connector	4 hrs	2 hrs
FX Conversion Engine	4 hrs	2 hrs
Settlement Scheduler	4 hrs	1 hr

---

5. Financial Impact

- **Annual Revenue Attributable**: Substantial inbound/outbound cross-border transactions. Fees may be moderate, but the volume is high, especially for corporate clients.
- **Penalties & Costs**: Non-cleared or delayed transactions can lead to contract penalties, especially if SLA breaches occur for corporate clients.
- **Total Financial Impact (Tier)**: **High**. Delays in clearing can cause major reputational and monetary setbacks, especially in international deals.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Criticism / Notice of Non-Compliance	Regulators (domestic or foreign) may intervene if cross-border settlement fails or is delayed, though massive fines are possible if it’s recurrent.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Moderate Brand Damage	Customers (especially corporates) rely on timely cross-border flows. Repeated delays tarnish ADB’s reliability.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Significant Strain on Internal Settlement Teams	They’d have to do emergency manual settlements, extended hours, and risk human error under time pressure.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
3	Noticeable Dissatisfaction	Delayed or lost cross-border funds can anger corporate and retail customers seeking quick global transfers.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Cross-Border Trans. & Clearing	Core Banking Operations	Transaction data, ledger updates	High	Yes
2	Output	Cross-Border Trans. & Clearing	Accounting & Finance	Final settlement amounts, clearing logs	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Cross-Border Trans. & Clearing	Compliance & Regulatory	AML checks, suspicious transaction alerts	High	Yes
2	Input	Cross-Border Trans. & Clearing	IT & Security Department	Secure connections, patching SWIFT systems	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input/Output	Cross-Border Trans. & Clearing	SWIFT Network	Payment messages, settlement status	High	Yes
2	Input	Cross-Border Trans. & Clearing	Clearinghouse Connector	Local or regional clearing instructions	Medium	Yes
3	Input	Cross-Border Trans. & Clearing	FX Data Providers	Real-time exchange rates	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Cross-Border Transaction & Clearing	*	*	*	*	**	-	-	*	*	*	***	*	*	*	*	***	*	*	*	***	*	***	***

Legend: *** indicates month/quarter-end settlement peaks; ** typical busy day (Friday closings); * normal but steady.

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Multi-currency steps sometimes require manual checks, especially if automated feeds lag or if exotic currencies are involved.
- **Budget or Resource Constraints**: SWIFT upgrades can be costly; often reprioritized against other IT projects.
- **Known Historical Incidents**: Past slowdowns in cross-border clearing caused corporate clients to threaten to move to competitor banks, highlighting brand risk.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - SWIFT downtime is highly damaging; strong AML/compliance oversight needed.
    - Quarter-end FX surges can overload the system if not scaled properly.
    - Manual currency check steps pose risk if staff are absent.

2. **Process Criticality**:
    - Cross-border transactions are essential for corporate clients and treasury functions—delays compromise ADB’s reliability and revenue.
3. **Data Provided**:
    - **RTO**: 4 hours for clearing infrastructure.
    - High-tier financial and brand impact if unprocessed cross-border flows accumulate.
    - Peak loads around month/quarter ends, requiring close cooperation with compliance and IT.

ROLE CARD: Mobile Banking Product Manager

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Mobile and Web Application Management (within the broader IT & Security Department)

Position Description:
As the Mobile Banking Product Manager, you oversee the end-to-end lifecycle of ADB's mobile and web channels. This includes designing user-friendly interfaces, planning feature roadmaps, coordinating releases with DevOps, and ensuring a secure, high-performing online experience for customers.

Primary Objective: - Maintain a seamless, reliable mobile and web banking platform. - Continuously enhance features and performance through coordinated deployments, QA, and security scans.

---

2. Single Business Process Details

2.1 Process Name

Mobile and Web Application Management

2.2 Key Process Activities

1. **Design & User Journeys:**
    - Research and finalize UI/UX improvements for both mobile apps and web front-end.
    - Incorporate feedback from customer usage patterns and marketing insights.
2. **Feature Development & Releases:**
    - Work with DevOps and QA teams to ensure new features and bug fixes pass code analysis and vulnerability scanning.
    - Schedule and execute production deployments with minimal downtime.
3. **Post-Release Monitoring & Optimization:**
    - Track app performance, crash analytics, user feedback, and usage metrics.
    - Initiate quick patches or hotfixes for any discovered issues or vulnerabilities.

2.3 Dependencies

- **Internal Dependencies:**
  - DevOps & QA Teams: For code builds, automated testing, and release pipelines.
  - Cybersecurity Team: For vulnerability scanning, security code reviews.
  - Backend/Core Banking Teams: To ensure APIs and backend services are stable and updated in sync.
- **External Dependencies:**
  - **Static Code Analysis Tool** (vendor or on-prem software)
  - **Vulnerability Scanner** (integrated, possibly from a third-party vendor)
  - Mobile App Stores (Apple/Google) for app distribution approvals

2.4 Peak Operational Periods

- New feature release cycles (often monthly or quarterly).
- Holiday seasons or major marketing campaigns (increases user traffic).
- End/beginning of the month (customers frequently check balances, make transfers).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Mobile & Web Application Management	4 hours	Downtime beyond 4 hours severely impacts user access to their accounts, leading to lost transactions, poor customer satisfaction, and brand erosion.

---

4. IT Applications

Application	RTO	RPO
Mobile Banking App	4 hours	1 hour
Web Front-End	4 hours	1 hour
Static Code Analysis Tool	12 hours	24 hours
Vulnerability Scanner	12 hours	24 hours

Note: The Mobile/Web channels must be restored rapidly (4 hours or less). Code scanning or vulnerability checks can tolerate a slightly longer downtime, though still critical in the SDLC.

5. Financial Impact

- **Annual Revenue Attributable:**
  A significant share of ADB's transaction revenue and customer service fees flow through mobile and web channels—potentially millions of credits annually.

- **Penalties & Costs:**

  - SLA breach with IBC or potential refunds to customers if service is unavailable.
  - Potential overtime costs to expedite fixes and restore service.

- **Total Financial Impact (Tier):**
  High – Each extended outage can lead to direct loss of transaction fees and potential non-compliance penalties if downtime disrupts regulated e-banking services.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Criticism / Possible Fines	Extended outages in online banking can attract scrutiny from financial regulators, leading to official criticism or moderate fines.

---

7. Brand Impact

Tier	Impact Value	Rationale
4	Significant Brand Damage	A prolonged outage on the public-facing app erodes customer trust and can harm ADB's reputation in highly competitive digital banking.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Moderate Operational Disruption	While the organization can still process some transactions through alternative channels, missing the main app/web front-end means staff and development teams must scramble for manual workarounds and hotfixes.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	High Customer Dissatisfaction	Frequent or lengthy outages on the mobile/web platform can quickly lead to churn, negative reviews, and a drop in user adoption.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Mobile & Web App Dev	Core Banking Operations	Transaction data / Account APIs	High	Yes
2	Output	Mobile & Web App Dev	QA & DevOps Pipeline	Build artifacts, test results	High	Yes
3	Both	Mobile & Web App Dev	Cybersecurity (Threat Intelligence)	Security advisories, vulnerabilities	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	User Journey / Feature Requirements	Marketing & Customer Engagement	Customer feedback, campaign details	Medium	Yes
2	Output	Incident Handling (if needed)	Compliance & Legal	Breach notifications, regulatory updates	Medium	Yes
3	Both	Production Releases	Finance & Accounting	Possible fee calculations for premium features	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Code Scanning & QA	Static Code Analysis Vendor	Scan reports, vulnerabilities	High	Yes
2	Input	Vulnerability Scanner	Third-Party Security Providers	Threat signatures, scanning plugin updates	Medium	Yes
3	Output	App Distribution	Apple/Google App Stores	App submission, updates, usage stats	High	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	De
Mobile & Web App Management					X	X	X							X									X

Legend: - **Weekends (Fri-Sun):** Higher usage as customers frequently check balances or transfer funds. - **Month End / Quarter End (Mar, Dec):** Larger transaction volumes due to salary credits, holiday shopping, year-end expenses.

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
    - Some manual steps remain for final sign-off before publishing app updates to production.
    - Occasional manual hotfix deployment if automated pipelines detect critical issues.
- **Budget or Resource Constraints:**
    - Funding for advanced application performance monitoring and mobile analytics may be limited.
    - Additional licenses for specialized security scanning tools still under review.
- **Known Historical Incidents:**
    - A short but critical outage during a holiday sale event last year led to customer complaints and refunds.
    - A missed vulnerability patch once delayed a feature release by 2 days.

---

13. Summary for Role-Play

1. **Key Talking Points:**
    - Coordination complexities between product releases and DevOps/ vulnerability scanning.
    - High user traffic peaks during weekends and end-of-month.
    - Potential brand/revenue impacts if the apps experience prolonged downtime.
2. **Process Criticality:**
    - The mobile/web platforms are the primary customer-facing interface for banking services.
    - Disruption directly affects customer satisfaction, transaction volume, and revenue generation.
3. **Data Provided:**
    - **RTO:** 4 hours for the core app/web front-end.
    - **Financial Scale:** High (significant share of daily transactions).
    - **Major Dependencies:** DevOps pipeline, code scanning tools, Apple/Google app stores.
    - **Peak Load Times:** Weekends, month-end, holiday seasons.

ROLE CARD: Marketing Campaigns Director

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Marketing & Customer Engagement

Position Description:
As the Marketing Campaigns Director, you lead initiatives to enhance ADB's user experience (UI/UX) and guide customer journeys across digital channels. Your team conducts A/B testing, analyzes engagement data, and implements cross-selling or upselling campaigns to increase product adoption. You also coordinate with compliance to ensure that user tracking and marketing actions respect regulatory constraints.

Primary Objective:
Strengthen customer satisfaction and drive revenue by continuously optimizing digital user experiences, leveraging data analytics to refine onboarding flows, personalized offers, and campaign effectiveness.

---

2. Single Business Process Details

2.1 Process Name

UI/UX Enhancement & Customer Journeys

2.2 Key Process Activities

1. **Customer Engagement Analysis**
    - Gather and interpret metrics from analytics platforms (e.g., bounce rates, conversion funnels).
    - Identify behavioral trends to adjust marketing strategies or UX design.
2. **A/B Testing & Experimentation**
    - Use the A/B Testing Suite (e.g., Optimizely) to compare interface variations.
    - Gather results to inform design changes or personalized marketing flows.

3. **Cross-Selling & Campaign Launch**
    - Craft targeted offers (e.g., new loans, credit card promotions) based on user segments in the CRM.
    - Automate campaign triggers via the Marketing Automation Tool, ensuring proper compliance checks.

Note: Timely analysis and fast iteration are crucial to maintaining a competitive edge and positive user experience.

2.3 Dependencies

- **Internal Dependencies:**
    - **Compliance & Legal Department** for user data privacy constraints and marketing disclaimers.
    - **IT & Security Department** for stable tracking integrations, secure data handling, and approvals for new tracking scripts.
- **External Dependencies:**
    - **A/B Testing Suite Vendor** (if external, for platform updates and support).
    - **Analytics Platform** (e.g., Google Analytics) that might rely on third-party scripts or hosted services.
    - **Cloud-based Marketing Automation** (if using an external SaaS for email/push notifications).

2.4 Peak Operational Periods

- **Product Launch Windows**: When new features or promotional campaigns go live, typically monthly or quarterly.
- **Major Holidays & Shopping Seasons**: Increased traffic due to holiday campaigns and special deals.
- **Ad Hoc**: Spikes during unexpected marketing pushes or competitor moves.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
UI/UX Enhancement & Customer Journeys	12 Hours	Extended downtime hinders marketing campaigns and user experience testing, risking lost engagement and missed revenue opportunities.

---

4. IT Applications

Application	RTO	RPO
A/B Testing Suite	12 Hours	4 Hours
Marketing Automation Tool	12 Hours	4 Hours
Analytics Platform	12 Hours	12 Hours
CRM	12 Hours	4 Hours

---

5. Financial Impact

- **Annual Revenue Attributable**:
  - Marketing campaigns and optimized user experiences can significantly impact ADB's product uptake, potentially influencing **millions of credits** in cross-sell opportunities.
- **Penalties & Costs**:
  - Non-compliance with user privacy/data usage regulations can lead to fines.
  - Missed cross-sell or campaign windows can reduce customer lifetime value.
- **Total Financial Impact (Tier)**:
  - **Tier 2-3** (Moderate). Disruption impacts marketing ROI but may be recoverable if short term.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2-3	Some Official Scrutiny / Fines	Mishandling user data or violating privacy laws can attract moderate regulatory attention.

---

7. Brand Impact

Tier	Impact Value	Rationale
2-3	Mild to Moderate Brand Concerns	Negative UX or missed campaign messages can irritate users, but direct brand damage is less critical unless prolonged.

---

8. Operational Impact

Tier	Impact Value	Rationale
2	Limited Operational Disruption	Staff can manually pause or shift campaign schedules, though missing analytics reduces agility.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2-3	Mild to Noticeable Impact	If site optimizations or new features are delayed, user frustration can emerge, though tolerance is moderate.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	UI/UX Enhancement & Customer Journeys	Data Privacy & Retention	Consent tracking, anonymization rules	Medium	Yes
2	Output	UI/UX Enhancement & Customer Journeys	DevOps & Deployment Pipelines	Front-end changes, experiment code deployments	High	Yes
3	Input	UI/UX Enhancement & Customer Journeys	Compliance & Regulatory Audits	Confirmation that marketing data is used lawfully	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	UI/UX Enhancement & Customer Journeys	Finance & Accounting Department	Potential revenue projections from campaigns	Medium	Yes
2	Output	UI/UX Enhancement & Customer Journeys	HR & Administration	Training or staffing for new marketing tools	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	UI/UX Enhancement & Customer Journeys	A/B Testing Suite Provider	Access to testing platform, user metric data	Medium	Yes
2	Input/Output	UI/UX Enhancement & Customer Journeys	Marketing Automation Tool Vendor	Email campaign APIs, user segmentation	Medium	Yes
3	Input/Output	UI/UX Enhancement & Customer Journeys	Analytics Platform (Google, etc.)	Traffic data, conversion funnels	High	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	D
UI/UX Enhancement & Customer Journeys	X	X	X	X	X	*	*					*			*					*		*	*

- **Legend:**
  - **X** = Regular daily workload (Mon-Fri).
  - ***** = Higher priority around product releases or holiday campaigns (varies by month).

---

12. Additional Observations

- **Automation Gaps / Manual Steps**:
  - Some campaigns or AB tests require manual toggling if automation is incomplete.
- **Budget or Resource Constraints**:
  - Certain advanced analytics features not yet funded; reliance on partial free-tier tools.
- **Known Historical Incidents**:
  - Past compliance concern over user data usage for retargeting led to temporary campaign suspension.

---

13. Summary for Role-Play

1. **Key Talking Points**:

   - Data analytics reliance (risk if analytics platform fails).
   - Potential compliance pitfalls if user data is mishandled.
   - Necessity for quick iteration and minimal downtime to maintain user engagement.

2. **Process Criticality**:

    ◦ Enhances cross-sell and upsell revenue streams, fosters customer loyalty.
    ◦ Minimizes churn by providing consistent, user-friendly digital experiences.

3. **Data Provided**:

    ◦ **RTO**: 12 hours for resuming UI/UX improvements and marketing campaigns.
    ◦ **Financial Scale**: Moderate—affects revenue indirectly through improved user conversions.
    ◦ **Dependencies**: A/B Testing Suite, Marketing Automation, Analytics, CRM.
    ◦ **Peak Load**: Seasonal promotions, new product launches, or competitor-driven campaigns.

ROLE CARD: Accounting & Finance Manager

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Finance & Accounting Department

Position Description:
As the Accounting & Finance Manager at Alderaan Digital Banking (ADB), you oversee the monthly and quarterly financial closures, manage transaction reconciliations with various internal systems, and ensure that final financial statements meet compliance and reporting standards. You work closely with Treasury, the Core Banking Operations team, and external auditors to ensure accurate records and regulatory compliance.

Primary Objective:
Maintain accurate financial reporting, ensuring that all incoming and outgoing transactions are reconciled, liquidity and cash flow positions are correctly recorded, and that statutory financial statements are produced on schedule.

---

2. Single Business Process Details

2.1 Process Name

Accounting & Finance Reporting

2.2 Key Process Activities

1. **Monthly Closures:**
    - Aggregate transaction data from core banking exports and relevant ledger entries.
    - Perform trial balances, identify discrepancies, and finalize monthly statements.
2. **Transaction Reconciliations:**
    - Compare daily settlement reports, payment logs, and vendor fees with internal records for any mismatches.
    - Investigate and correct discrepancies found during reconciliation to avoid financial misstatements.

3. **Financial Statement Preparation:**
    - Generate required management reports (profit & loss, balance sheet, cash flow).
    - Collaborate with compliance/legal advisors to incorporate regulatory disclosures into official statements.

Note: The goal is to produce timely and precise financial outputs that reflect ADB's performance while meeting regulatory expectations.

2.3 Dependencies

- **Internal Dependencies:**
- **Core Banking Data Exports** (provides daily transactions, account balances).
- **Treasury Data** (short-term investments, liquidity positions).
- **Advanced Reporting Modules** (analyzes large datasets for monthly/quarterly statements).
- **External Dependencies:**
- **External Auditors** (periodic checks on financial statements).
- **Regulatory Entities** (submission of official financial disclosures).
- **Vendor Tools** (if using external software for reconciliations or advanced analytics).

2.4 Peak Operational Periods

- **End of Each Month**: High-intensity closure activities.
- **Quarter-End & Year-End**: Larger scope of auditing and financial statement production.
- **Tax Filing Season**: Additional reporting demands from local or intergalactic taxation authorities.

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Accounting & Finance Reporting	2 Days	Extended downtime delays monthly statements, disrupts regulatory deadlines, and halts daily reconciliation processes.

---

4. IT Applications

Application	RTO	RPO
Finance & GL System	2 Days	1 Hour
Reporting & BI Platform	2 Days	24 Hours
Reconciliation Tool	2 Days	4 Hours
Treasury Module	1 Day	30 Minutes

---

5. Financial Impact

- **Annual Revenue Attributable**: While not directly generating revenue, delays in producing financial statements can result in misinformed budgeting or missed investment opportunities.
- **Penalties & Costs**: Non-compliance with regulatory reporting timelines can incur fines or official criticism; inaccurate statements risk reputational damage.
- **Total Financial Impact (Tier)**: Likely mid-to-high tier, given that blocked or delayed closings can lead to multi-million credit shortfalls or regulatory issues.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
2	Official Criticism/Some Fines	Missing reporting deadlines or inaccurate statements invite fines.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	Inconsistent or delayed financial data undermines stakeholder trust.

---

8. Operational Impact

Tier	Impact Value	Rationale
2	There are only a select few who know the process	The reconciliation methods can be intricate, requiring specialists to oversee.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
4	Little Impact	Most customers do not see behind-the-scenes financial closures unless major errors occur.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Accounting & Finance Reporting	Core Banking Operations	Daily ledger exports, transaction data	High	Yes
2	Input	Accounting & Finance Reporting	Treasury & Liquidity	Surplus funds, short-term investments	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Output	Accounting & Finance Reporting	Compliance & Regulatory Audits	Official financial statements	Medium	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Output	Accounting & Finance Reporting	External Auditors	Financial statements, supporting docs	Medium	Yes
2	Output	Accounting & Finance Reporting	Regulatory Entities	Periodic compliance disclosures	High	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Accounting & Finance Reporting					X	-	-	-	-	-	X	-	-	X	-	-	-	-	X	-	-	X	X

(*Month-end (final week) and quarter-end spikes occur, plus heavier year-end loads.*)

---

12. Additional Observations

- **Automation Gaps / Manual Steps**: Some reconciliation steps are manually performed using spreadsheets, subject to human error.
- **Budget or Resource Constraints**: Proposed upgrades for advanced analytics or real-time reconciliation remain on hold.
- **Known Historical Incidents**: Last year, a month-end closure encountered a multi-day delay due to database patching misalignment, causing official warnings from IBC group oversight.

---

13. Summary for Role-Play

1. **Key Talking Points**:
    - Reliance on accurate data from the core banking system, daily ledger exports.
    - Tightly scheduled monthly closings and external audits create strict deadlines.
2. **Process Criticality**:
    - Delays or inaccuracies in financial statements undermine regulatory compliance and group-level reporting.
    - Potential brand risk if discovered errors are major or repeated.

3. **Data Provided**:

    - RTO of 2 Days; Tier 2 or higher for regulatory impact.
    - Heavy synergy with core ledger data and external auditors.
    - Peak load at month-end, quarter-end, and year-end closures.

ROLE CARD: Collection and Recovery Team Lead

Alderaan Digital Banking (ADB)

---

1. Role Overview

Department/Unit:
Support & Back-Office Operations Division

Position Description:
As the Collection and Recovery Team Lead, you oversee strategies to engage customers who have defaulted or are at risk of defaulting on their loans. You coordinate outreach efforts, track overdue accounts, collaborate with internal legal teams for escalations, and ensure that ADB recovers outstanding debts while maintaining compliance with financial regulations.

Primary Objective:

- Maximize successful collections through automated contact strategies and efficient follow-up.
- Coordinate with legal channels and CRM systems to handle escalations and maintain accurate records.

---

2. Single Business Process Details

2.1 Process Name

Collections & Recovery

2.2 Key Process Activities

1. **Account Segmentation & Prioritization**
    - Identify overdue accounts, categorize by risk level, and plan outreach schedules.
    - Use loan underwriting and CRM data to set recovery priorities.
2. **Automated Customer Outreach**
    - Trigger SMS, emails, or phone calls via the Dialer/SMS tool.
    - Record responses, partial payments, or agreements in the Collections Management System.

3. **Escalation & Legal Coordination**
    - When standard outreach fails, escalate accounts to ADB's legal channels.
    - Track ongoing legal proceedings, collaborate with internal Legal Case Management system.

Note: The workflow typically begins with segmentation, continues through automated outreach, and finalizes with legal action for severe delinquencies.

2.3 Dependencies

- **Internal Dependencies:**
- **Loan Underwriting Data:** Provides background on loan terms, customer risk scores.
- **CRM:** Stores borrower contact details, conversation history, payment arrangements.

- **Legal Advisory / Internal Legal Processes:** For advanced or escalated collections.

- **External Dependencies:**

- **Dialer / SMS Outreach Tool:** Could be a vendor-provided platform.
- **Third-Party Credit Bureaus:** (If needed) to verify updated addresses, skip-tracing, etc.

2.4 Peak Operational Periods

- End/Beginning of month (customers often miss deadlines or attempt partial payments).
- After major economic changes or crises (e.g., unemployment spikes leading to more delinquencies).
- Quarterly reviews (ADB might push for heavier collection efforts at quarter-end).

---

3. Recovery Time Objective (RTO)

Process	RTO	RTO Rationale
Collections & Recovery	24 hours	Longer downtime hampers overdue account monitoring, delaying outreach. This can lead to bigger write-offs, missed recovery windows, and compliance risks.

---

4. IT Applications

Application	RTO	RPO
Collections Management System	24 hours	12 hours
Dialer / SMS Outreach Tool	24 hours	12 hours
CRM	12 hours	4 hours
Legal Case Management	48 hours	24 hours

> **Note:** CRM needs quick recovery to retain contact history and maintain continuous outreach. The Legal Case Management system can tolerate a bit more downtime but still critical for escalations.

---

5. Financial Impact

- **Annual Revenue Attributable:**
  Collections can significantly impact net income by reducing charge-offs. For ADB, recovered funds from overdue loans can amount to millions of credits annually.
- **Penalties & Costs:**
- Potential regulatory issues if consumer protection laws or debt-collection regulations are not followed.
- Extra overhead if manual methods are required during system downtimes.
- **Total Financial Impact (Tier):**
  High – Inability to collect overdue debts results in direct revenue losses and increased operational overhead.

---

6. Regulatory/Legal Impact

Tier	Impact Value	Rationale
3	Official Criticism / Moderate Fines Possible	Aggressive or improper collection processes can attract regulatory scrutiny. Delays in legal escalations can also breach compliance.

---

7. Brand Impact

Tier	Impact Value	Rationale
3	Some Temporary Brand Damage	If publicized that ADB fails to handle collections ethically, negative perceptions can arise—though not as visible as a systemwide outage.

---

8. Operational Impact

Tier	Impact Value	Rationale
3	Moderate Operational Disruption	Staff can revert to manual tracking or spreadsheets, but it’s time-consuming, error-prone, and can delay legal escalations.

---

9. Customer Satisfaction Overview

Tier	Impact Value	Rationale
2	Limited Customer Impact	Most customers affected are already overdue. Reputation issues arise if the process is deemed too harsh or unresponsive.

---

10. Business Interdependencies

10.1 Intra-Dependencies (Within ADB)

#	Input/Output	Process	Intra-Dependency	What is Exchanged	Impact	Electronic
1	Input	Collections & Recovery	Loan Origination & Underwriting	Loan status, risk tiers, account history	High	Yes
2	Output	Collections & Recovery	Legal Advisory (Internal)	Escalated cases, lawsuit documentation	High	Yes
3	Both	Collections & Recovery	CRM (Marketing, if shared)	Customer contact updates, responses, payment records	Medium	Yes

10.2 Inter-Dependencies (Cross-Department)

#	Input/Output	Process	Business Unit	What is Exchanged	Impact	Electronic
1	Input	Collections & Recovery	Finance & Accounting	Detailed info on monthly recoveries, revenue adjustments	Medium	Yes
2	Output	Collections & Recovery	Compliance & Legal	Regulatory compliance checks on debt collection strategies	Medium	Yes
3	Input	Collections & Recovery	Vendor Management	SLAs for dialer or collection tool vendors, performance metrics	Low	Yes

10.3 External Dependencies

#	Input/Output	Process	External Entity	What is Exchanged	Impact	Electronic
1	Input	Collections & Recovery	Dialer / SMS Vendor	Voice/SMS campaigns, success/failure logs	High	Yes
2	Input	Collections & Recovery	Third-Party Credit Bureaus	Updated addresses, skip-tracing data	Medium	Yes
3	Output	Collections & Recovery	External Legal Services	Legal notices, final demands (if escalated)	Medium	Yes

---

11. Peak Periods

Process	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1stWk	2ndWk	3rdWk	4thWk	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Collections & Recovery	X	X			X	X			X														X

Legend:

- **Mondays, Tuesdays, Fridays:** Common days for contacting overdue customers.
- **2nd Week of the Month:** After many monthly due dates pass, heavier call volume.
- **December:** End-of-year push to clear outstanding debts.

---

12. Additional Observations

- **Automation Gaps / Manual Steps:**
- Some manual follow-ups remain for high-value or complex cases.

- Email communications are partially automated, but prioritization might require manual overrides.

- **Budget or Resource Constraints:**

- More advanced dialer AI features are pending approval.

- Additional staff training for difficult negotiations or legal knowledge is in discussion.

- **Known Historical Incidents:**

- Brief outage of the dialer system led to missed contact windows, causing some accounts to slip further into delinquency.
- A high-risk account wasn’t escalated properly, resulting in a prolonged legal dispute.

---

13. Summary for Role-Play

1. **Key Talking Points:**
    - Potential compliance/regulatory concerns if collections aren't handled properly.
    - Heavy reliance on automated outreach tools, with manual backup for complex cases.
    - Financial impact is substantial when tools are down, as overdue payments remain uncollected.
2. **Process Criticality:**
    - Crucial for minimizing ADB's loan losses and maintaining healthy credit portfolios.
    - Supports compliance by documenting outreach steps and legal escalation procedures.
3. **Data Provided:**
    - **RTO:** 24 hours for Collections & Recovery.
    - **Financial Scale:** High (significant impact on net income).
    - **Major Dependencies:** Loan underwriting data, CRM, dialer vendor, legal modules.
    - **Peak Load Times:** Month-end, second week of the month, end-of-year collection drives.
