Organization: _____ **Resilience Lead:** _____ **Assessment Date:** 202___-___-___ **Review Cycle:** Annual / Post-Trigger

STEP 1: STAKEHOLDER CONSULTATION & SERVICE SCOPING REGISTER

Conduct stakeholder interviews across business lines, customer-facing operations, and technology teams. Distinguish potential Important Business Services (IBS) from internal supporting functions.

Svc ID	Candidate Service Name	Business Line / Unit	Customer Populations Served	Revenue & Materiality Weight	External / Systemic Footprint	Initial Classification
CS-01	Wholesale Payment Clearing & Wire Settlement	Corporate Treasury / Transaction Banking	Institutional clients, multinational corporates, interbank participants	High: $4.2B daily volume; critical liquidity driver	High: Systemic interbank counterparty exposure (Fedwire/CHIPS)	**Candidate IBS**
CS-02	Retail Digital Banking & Mobile Payments	Consumer Banking & Digital Channels	1.8M retail checking and cardholder customers	Material: Primary retail transactional volume and fee base	Moderate: Direct customer harm if payments/ATM access halts	**Candidate IBS**
CS-03	Commercial Lending Loan Origination	Commercial Credit Services	Middle-market business borrowing applicants	Moderate: Loan pipeline revenue; multi-day processing cycle	Low: Delay inconveniences borrowers but causes no liquidity crisis	**Supporting Function**
CS-04	Customer Authentication & Multi-Factor Service	Enterprise Cyber / Identity Infrastructure	Shared across 100% of retail and corporate digital platforms	Indirect: Critical gating mechanism for all digital revenues	High: Cascades into multiple downstream IBS if compromised	**Critical Supporting Function**
CS-05						
CS-06						
CS-07						
CS-08						

STAKEHOLDER INTERVIEW & SCOPING AUDIT PROTOCOL

Scoping Dimension	Key Investigation Questions (Step 1 Protocol)	Evidence Requirements
Customer Harm Assessment	Would disruption of this service cause immediate, significant financial loss, health/safety risk, or critical data loss to end customers?	Customer contract SLAs, consumer complaint records, regulatory breach notices.
Systemic Market Impact	Could disruption cascade into other market participants, payment clearing facilities, or financial sector stability (Bank of England / DORA criteria)?	Market share data, interbank counterparty links, clearing house transaction logs.
Organizational Viability	Would prolonged disruption threaten the capital, solvency, regulatory licensing, or existential franchise of the firm?	Financial materiality assessments, regulatory capital models, licensing conditions.
Supporting Function Cascading	Does this internal capability act as a single point of failure for two or more candidate IBS (e.g. IAM, authentication, data warehouse)?	Enterprise architecture maps, API dependency graphs, single-sign-on topologies.

STEP 2: FIVE-DIMENSION IMPACT ANALYSIS FRAMEWORK

Evaluate each candidate service against the article's five impact dimensions. Score severity on an objective scale (Low, Medium, High, Severe) based on disruption escalation over time.

Impact Dimension	Evaluation Criteria (Post 29 Framework)	Tolerable Limit Indicator	Disruption Escalation Point	Candidate Svc Score
1. Financial Impact	Direct revenue loss, regulatory non-compliance fines, contractual penalties, interest costs, or settlement failures.	Loss exceeds defined capital/revenue threshold or triggers liquidity crunch.	Escalates rapidly from minor fee loss to material solvency exposure at Hour 4+.	
2. Customer Impact	Inability of customers to access critical funds, execute time-sensitive transactions, access essential records, or conduct business.	Widespread customer hardship, locked accounts, financial distress to retail/SME users.	Customer harm accelerates sharply after 2 hours without transactional alternative.	
3. Systemic Impact	Potential cascading effects across market participants, interbank payment systems, clearing networks, or financial stability.	Failure to settle positions cascades into secondary financial institution liquidity halts.	Intraday cut-off window breach (e.g., end-of-day central bank clearing deadline).	
4. Reputational Impact	Severe damage to brand value, loss of customer confidence, sustained adverse media coverage, customer attrition.	National headline coverage, social media contagion, measurable client deposit flight.	Sustained outage past public commitment threshold creates permanent brand trust erosion.	
5. Operational Impact	Loss of business function continuity, service availability degradation, staff overload, manual workaround failure.	Backlog exceeds manual processing capacity; data reconciliation impossible.	Workarounds collapse when transaction queues exceed 8 hours of standard volume.	

STEP 3: THRESHOLD DEFINITION & QUALIFICATION DECISION

Quantitative Threshold Criteria:
• **Customer Volume Threshold:** ≥ _____ customers affected simultaneously.
• **Financial Exposure Threshold:** ≥ $_____ loss or exposure per 24 hours.
• **Duration Threshold:** Disruption > _____ hours causes irreversible customer harm.
• **Systemic Threshold:** Triggers statutory regulatory reporting or interbank notice.

IBS Qualification Decision:
[ ] **QUALIFIED AS IMPORTANT BUSINESS SERVICE (IBS)**
[ ] **CRITICAL SUPPORTING FUNCTION (Cascading Dependency)**
[ ] **STANDARD SUPPORTING FUNCTION (Non-IBS)**
Sign-Off Rationale: _____

Service Name: _____ **Service Ref ID:** IBS-___ **Service Owner:** _____ **Technical Lead:** _____

CRITICAL RESOURCE INVENTORY: PEOPLE, FACILITIES & DATA

Resource Tier	Primary Operational Node	Designated Alternate / Backup	Minimum Operating Threshold	Identified Resilience Gap
People (Ops Staff)	Core Transaction Settlement Desk (6 FTEs)	Secondary Regional Operations Hub (4 FTEs)	3 FTEs required for manual wire verification	Shift handover protocol undocumented for split teams
People (Tech Admins)	Senior Systems Architect & Lead DBA	On-call DevOps rotation engineer	1 certified DBA for active failover execution	Sole-architect dependency for database encryption keys
Facilities (Primary)	Headquarters Operations Floor (Tower A)	Backup Business Continuity Site (Facility B)	20 dual-monitor workstations with secure tokens	Alternate facility generator unvalidated under load
Facilities (Remote)	Secure Home Telework Profiles	Emergency Co-Working Disaster Pods	100% staff token access with VPN redundancy	SLA latency spikes on secondary VPN gateway
Data (Transactional)	Active Transaction Ledger Database (PostgreSQL)	Synchronous Replicated Standby (Secondary Region)	Zero loss for cleared trades; ≤ 1 min queue	Asynchronous replication lag during peak batch hours
Data (Customer Records)	Enterprise Customer Reference Master	Air-gapped immutable backup snapshots	RPO ≤ 15 minutes; full audit trail preserved	Full restore takes 6 hours; exceeds preliminary RTO

SINGLE POINTS OF FAILURE (SPOF) RISK AUDIT

Flag all single points of failure across operational nodes that could halt the service without immediate automated or manual redundancy.

SPOF ID	Vulnerable Resource / Node	Failure Scenario & Root Cause	Cascading Impact Severity	Mandatory Mitigation / Redundancy Action
SPOF-01	Lead Settlement Operations DBA	Sudden medical leave or simultaneous unavailability	**Severe** (Halts failover)	Cross-train 2 secondary DBAs; mandate split-key emergency vault.
SPOF-02	Primary Fiber Interconnect Hub	Metropolitan fiber conduit physical severance	**High** (Disables clearing link)	Provision dual-routed path diversity via secondary carrier.
SPOF-03				
SPOF-04				

TECHNOLOGY INFRASTRUCTURE MAPPING (5 CRITICAL LAYERS)

Map the technology stack underpinning the Important Business Service across all five layers outlined in Post 29.

Technology Infrastructure Layer	Underlying Systems, Assets & Architecture	Redundancy & Failover Mechanism	Demonstrated Recovery Speed
1. Core Applications & Databases	Core ledger application, relational database cluster, caching nodes	Multi-zone active-passive auto-failover; synchronous replication	Automated failover: 8 minutes; data integrity confirmed
2. Networking & Telecoms	Edge firewalls, SD-WAN interconnects, MPLS lines, DNS routing	BGP route failover with dual disparate telecom providers	DNS cutover takes up to 45 mins due to external TTL propagation
3. Cloud & Hosting Environments	Primary hyperscaler VPC (Region East); secondary DR VPC (Region West)	Infrastructure as Code (Terraform) cold-to-warm spin-up	Full environment spin-up: 2 hours 15 minutes
4. Integration & Data Pipelines	Kafka message queues, event streaming pipelines, nightly ETL batch jobs	Clustered broker nodes with multi-broker partition replication	Message replay buffer supports 4 hours of queue holding
5. Cybersecurity & Authentication	SSO directory, SAML authentication, Hardware Security Modules (HSM)	Clustered HSMs across regions; cached directory credentials	Local directory fallback operational; HSM failover: 12 minutes

THIRD-PARTY & CRITICAL ICT VENDOR DEPENDENCIES (EU DORA & BASEL COMMITTEE)

Third-Party Vendor	Service Provided / Function	Contractual RTO/RPO	Single-Vendor Flag	Contingency & Redundancy Arrangement
AWS (Cloud Hyperscaler)	Primary compute and storage infrastructure	SLA: 99.99% availability; RTO 4h	**YES (SPOF)**	Multi-region deployment; contingency playbook for cross-cloud container portability.
Swift / Fedwire Gateway	Interbank messaging and final settlement	SLA: RTO ≤ 2 hours	**YES (Industry Mandate)**	Contractual bypass terminal; manual clearing contingency facility.
Stripe / Payment Processor	Merchant payment tokenization & card rails	SLA: 99.95% uptime	**NO (Dual-Sourced)**	Secondary processor (Adyen) pre-integrated with automated traffic rerouting.

Service Name: _____ **Service Ref ID:** IBS-___ **Target RTO:** ____ Hours / Mins **Target RPO:** ____ Mins / Secs

EVIDENCE-BASED RTO FORMULATION (THE 4 GOVERNING FACTORS)

Recovery Time Objective (RTO) must be evidence-based and reflect the point at which continued disruption creates unacceptable impact, not an arbitrary goal.

Governing Factor	Operational Analysis & Empirical Evidence	RTO Constraint / Determination
1. Customer Impact Escalation Over Time	• *Hour 0–1:* Minor inconvenience; queued transactions. • *Hour 1–4:* Escalating customer calls, failed business vendor payments. • *Hour 4+:* Material financial harm, overdrafts, inability to payroll.	Customer harm crosses tolerable threshold at **4 Hours**. Continued outage causes irreversible customer distress.
2. Regulatory Requirements	Supervisory mandates (Bank of England SS1/21, EU DORA) require core settlement to restore before interbank end-of-day cut-off window.	Regulatory non-compliance and mandatory notification triggered if service down > **2 Hours**.
3. Competitive Considerations	Customer tolerance compared to peer institutions with multi-region instantaneous failover capabilities.	Industry peer benchmark for critical wholesale clearing: **2 to 4 Hours** maximum tolerable downtime.
4. Operational Constraints	Technical recovery realistic speed: database snapshot restore, DNS cutover, integrity reconciliation, security check.	Minimum proven technical recovery window: **1 Hour 45 Mins**. Target RTO must allow operational safety buffer.

FINAL AGREED RTO FOR THIS SERVICE: _____ Hours / Minutes | **Evidence Sign-off:** _____

RECOVERY POINT OBJECTIVE (RPO) & MULTI-DIMENSIONAL IMPACT THRESHOLDS

Tolerance Threshold Dimension	Operational Definition & Boundary Limit	Monitoring & Breach Protocol
Recovery Point Objective (RPO)	Maximum acceptable data loss: **≤ 15 Minutes** of transactional ledger data. Synchronous log shipping mandated.	Automated replication lag alert triggers at 5 mins; failover halts if gap exceeds 15 mins.
Data Availability Cap	Minimum **95%** of historical customer account data must remain queryable; real-time balances must be current within RPO.	Degraded read-only mode activated if primary database cluster encounters data corruption.
Service Degradation Cap	Maximum acceptable transaction throughput reduction: **30%**. Response latency must remain under 3.5 seconds.	Non-essential reporting and analytics traffic throttled to preserve core settlement rails.
Affected Users Cap	Maximum **15%** of total customer population may experience degraded service concurrently during failover routing.	Regional DNS routing confines disruption to affected geographic availability zone.
Financial Impact Ceiling	Maximum acceptable unhedged financial loss / penalty exposure per disruption event: **≤ $500,000**.	Executive Risk Committee escalation invoked immediately upon breach of $250,000 threshold.

MASTER IMPORTANT BUSINESS SERVICES (IBS) REGISTER TEMPLATE

IBS ID	Service Definition & Scope	Customer Cohort	Critical Dependencies	RTO	RPO	SPOFs?	Sign-Off
IBS-01	Wholesale Payment Clearing & Wire Settlement	Institutional / Corporate Treasury	People (Settlement), Core App, Fedwire Gateway, AWS East	**2 Hours**	**0 Secs**	Yes (Fedwire)	Approved
IBS-02	Retail Digital Banking & Card Authorization	1.8M Consumer Checking / Cards	Card Engine, Auth Cluster, SD-WAN, Stripe/Adyen	**4 Hours**	**15 Mins**	Mitigated	Approved
IBS-03							
IBS-04							
IBS-05							

12-WEEK IMPLEMENTATION ROADMAP TRACKER

Roadmap Phase	Key Workstreams & Operational Deliverables	Accountable Lead	Completion Status
Weeks 1–2	Form cross-functional governance structure; conduct executive & BU stakeholder interviews.	Resilience Lead	[ ] Complete • Date: _____
Weeks 3–4	Develop 5-dimension impact assessment framework; apply systematically across services.	Risk / Compliance Lead	[ ] Complete • Date: _____
Weeks 5–6	Finalize candidate IBS list; document business, customer, and regulatory rationale.	Business Unit Heads	[ ] Complete • Date: _____
Weeks 7–8	Conduct end-to-end dependency mapping (People, Tech, Facilities, Data, Vendors); flag SPOFs.	Enterprise Architect / IT Ops	[ ] Complete • Date: _____
Weeks 9–10	Establish evidence-based impact tolerances (RTO, RPO, Degradation caps) via 4-factor analysis.	Resilience & Finance Leads	[ ] Complete • Date: _____
Weeks 11–12	Document final register; obtain Executive Steering Committee sign-off; integrate scenario tests.	Executive Sponsor	[ ] Complete • Date: _____

GOVERNANCE & EXECUTIVE SIGN-OFF BLOCK

Operational Resilience Lead:
Signature: _____
Date: 202___-___-___

Chief Information Officer (CIO):
Signature: _____
Date: 202___-___-___

Chair, Risk Committee / Board Sponsor:
Signature: _____
Date: 202___-___-___