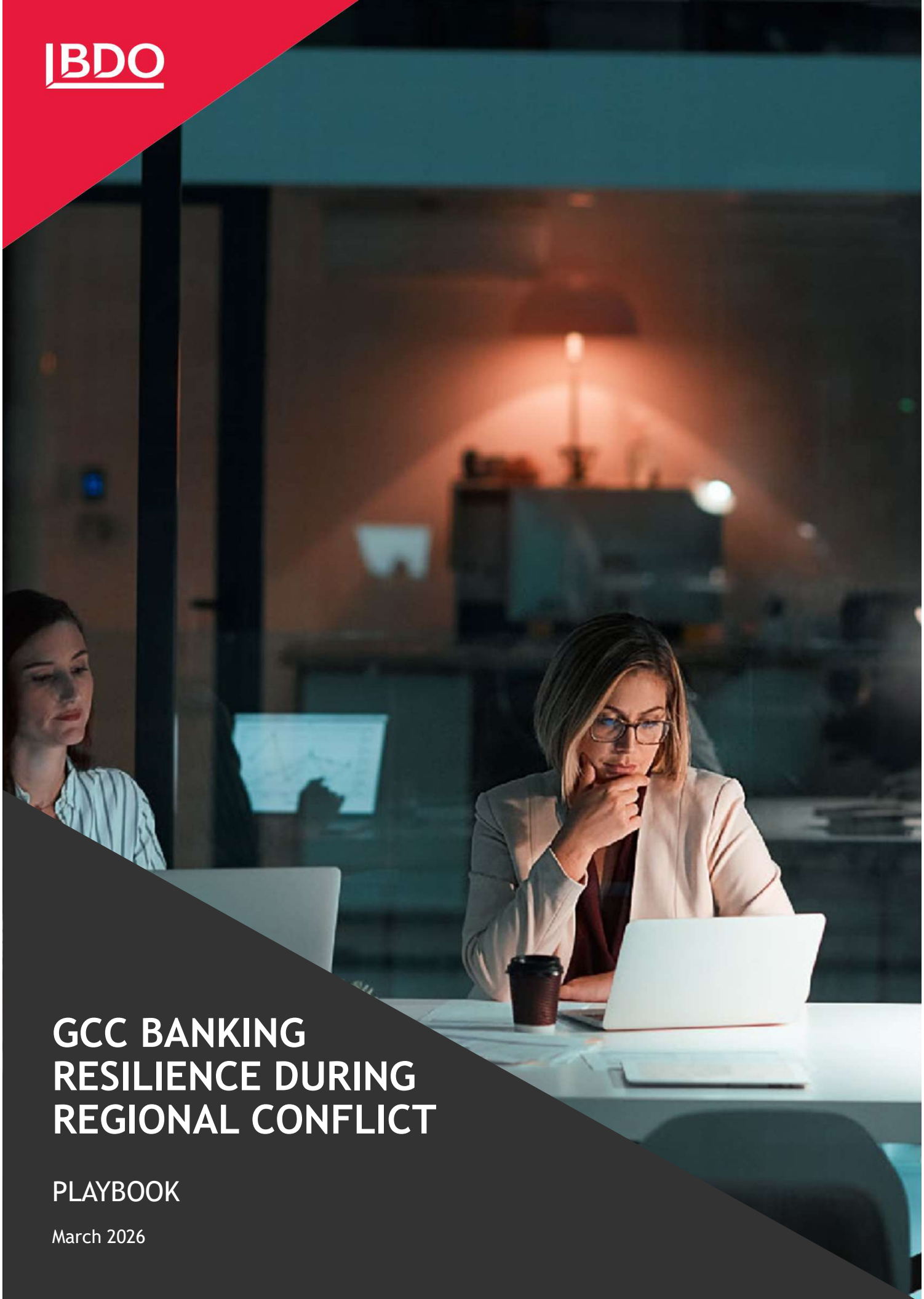


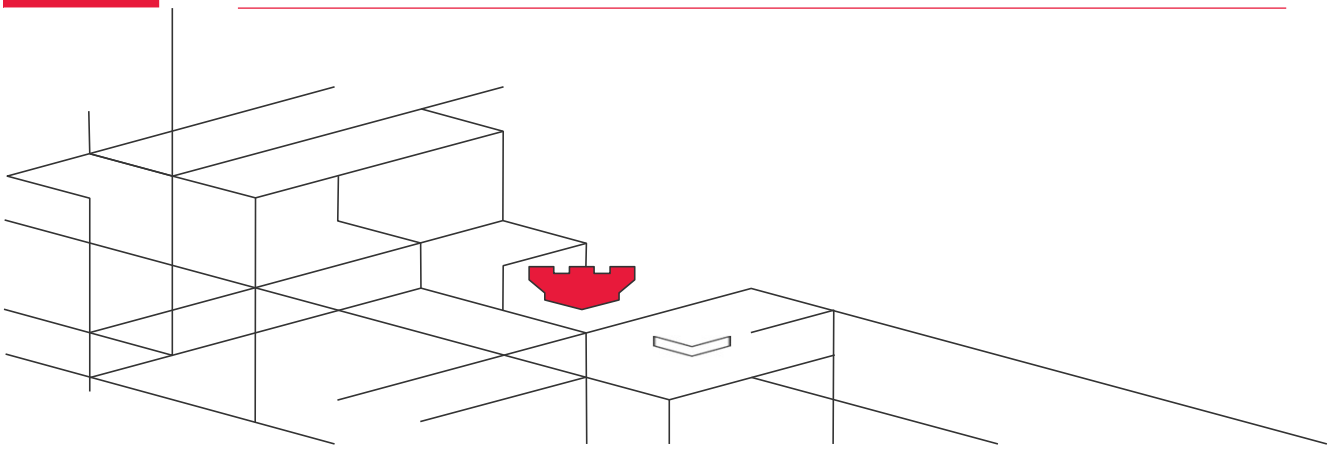
GCC BANKING RESILIENCE DURING REGIONAL CONFLICT

PLAYBOOK

March 2026

Table of contents

01	Executive Summary	03
02	Glossary of Key Terms	04
03	Coverage, Applicability & Impacted Functions	05
04	Governance & War-Room Operating Model	06
05	Critical & Important Business Services (C/IBS)	07
06	Architecture for Survivability	08
07	Zero-Trust Cyber Controls	09
08	Crisis Communications	09
09	Third-Party & Supply Chain Controls	09
10	Testing & Assurance	09



1. Executive Summary

The GCC is now functioning **inside an active war-zone operating environment**, where hybrid threats — **state-sponsored cyberattacks, destructive malware, telecom instability, power constraints, cloud region dependencies, and physical infrastructure threats** — are continuous and intertwined. Banking resilience is no longer defined by documentation or scheduled tests; it is defined by a bank's ability to **withstand, continue, and operate** under multi-layered disruption.

GCC regulators have already mandated **regional resilience baselines**, requiring institutions to demonstrate continuity of **critical and important business services (C/IBS)** even during crisis conditions.

Strategic Shift Required

FROM:
- Compliance exercises
- Documentation-heavy BCP/DRP
- Annual DR drills
- "Recover after disruption"

TO:
- Real-time **operational survivability**
- End-to-end live failover across in-country facilities, cross-GCC redundancy (if applicable), and offshore recovery regions
- 24/7 cyber-war-room readiness
- Zero-trust architecture during crisis
- "Continue operating through disruption"

Objectives of This Playbook:

To deliver actionable guidelines that enable GCC banks to operate effectively during regional conflict by:
- Ensuring the continuity of critical banking services (payments, deposits, cash availability, digital channels)
- Safeguarding customer trust and preserving national financial stability
- Enabling real-time failover through multi-region infrastructure
- Implementing regulator-aligned emergency and wartime protocols
- Maintaining a functional banking ecosystem even when multiple systems experience partial degradation

> *"This playbook strengthens the region's move toward real-time operational resilience by translating regulatory expectations into a practical, modern approach that enables banks to sustain critical services through persistent geopolitical and cyber pressures.*

Hashem Qtaishat
Senior Director
Technology Advisory Services

2. Glossary of Key Terms

C/IBS – Critical & Important Business Services	Banking functions that must remain operational during crisis (e.g., core banking, RTGS, digital channels).
IOT – Impact Tolerance	The maximum acceptable level of disruption (duration or magnitude) before a service becomes unsafe or destabilizing
MTD	Mean Time to Detect- How long it takes on average to discover an issue such as outage and system failure.
RTO – Recovery Time Objective	The maximum acceptable time to restore a service after a disruption.
RPO – Recovery Point Objective	The maximum acceptable data loss measured in time (e.g., ≤10 minutes).
EDR/XDR – Endpoint / Extended Detection & Response	Advanced threat detection tools monitoring all endpoints and identity behavior.
SOAR – Security Orchestration, Automation & Response	Automation engine for incident response, alert triage, and playbook execution.
CLZ – Cloud Landing Zone	A pre-built, pre-secured cloud environment ready to host workloads during failover.
War-Room (Gold/ Silver/Bronze)	Three-tiered crisis governance model for command, execution, and technical action.
Degraded Mode	Reduced functionality mode maintaining essential banking operations under attack.
Data Evacuation	Emergency replication of critical data to a safe region during imminent threat.
Immutable / WORM Backups	Backups that cannot be altered or deleted, protecting against ransomware or wipers.
MPLS	Multiprotocol Label Switching- A high-performance, private networking technique for predictable, secure, low-latency connectivity across sites.
SASE	Secure Access Service Edge: A modern cloud-based architecture that combines networking + security into one unified, cloud-delivered service.
Zero-Trust	Security model that continuously verifies identity, device, and context before granting access

3. Coverage, Applicability & Impacted Functions

Critical functions in-scope:

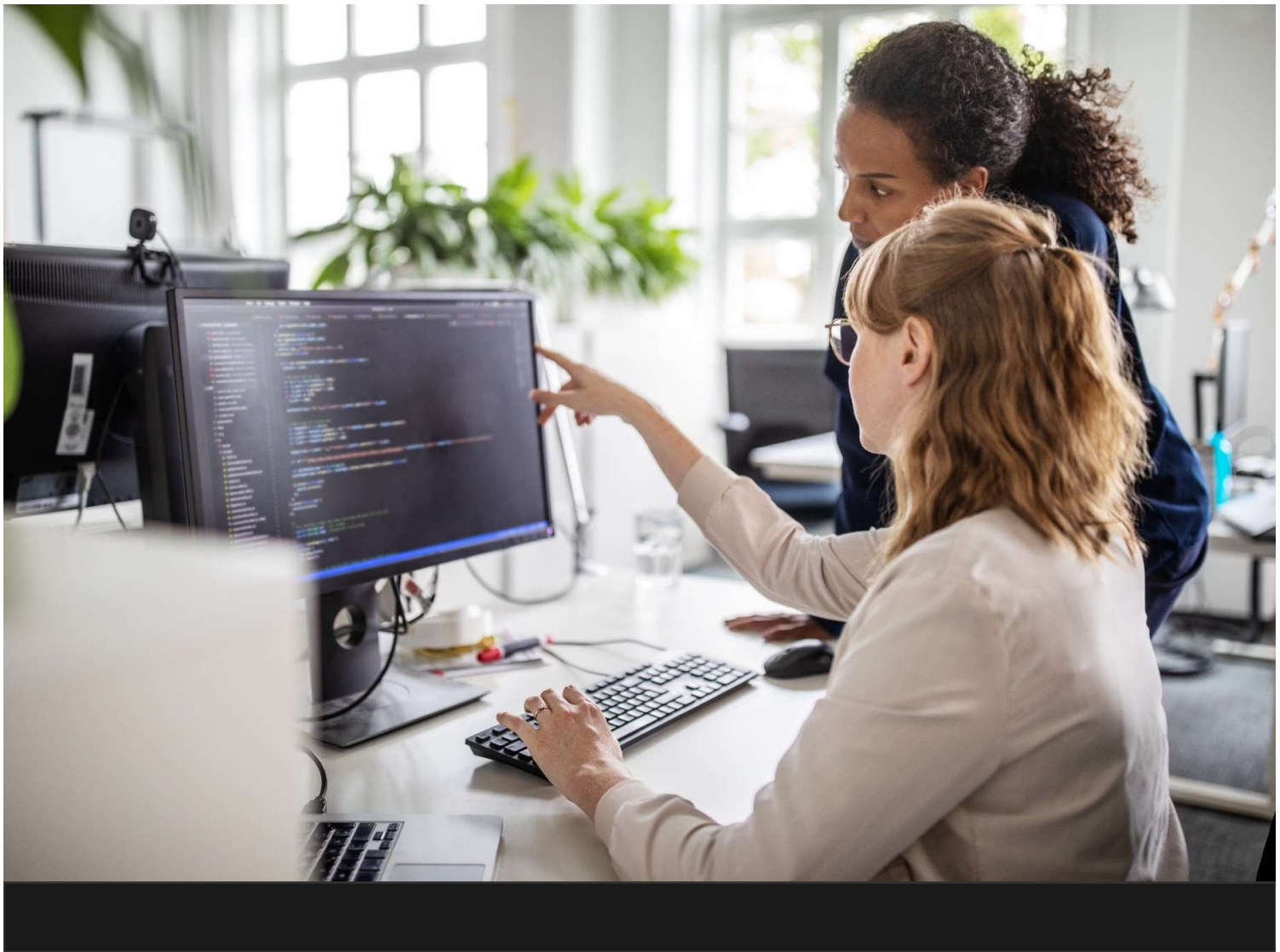
Core banking, payments, RTGS/SWIFT, digital channels, treasury, Anti Money Laundry (AML) risk, fraud, operations, Security Operations Center (SOC), IT, facilities, communications, legal, vendor management.

Supporting assets & infrastructure

Primary/secondary Data Centers (DCs), cloud landing zones, Networking (WAN/satellite links (if available)), Identify & Access Management (IAM), security controls, data protection layers, crisis communications platforms.

Applicability:

Bank-wide, recommended for all C/IBS.



4. Governance & War-Room Operating Model

(Optimized and structured using the Gold/Silver/Bronze command system)

4.1 War-Room Command Structure

Gold (Strategic): CEO, COO, CRO, CIO/CTO, CISO, Communications Head, Regulator Liaison.

Silver (Operational): IT Operations Team, Network & Applications Administrators , SOC Lead, DR Lead, Facilities Engineers, Vendor Management Lead.

Bronze (Tactical): Engineers, DC & DR Site Engineers , platform owners, incident responders.

4.2 Activation Triggers

- Confirmed Advanced Performance Trigger (APT)/wiper attack
- DC instability or national grid disruption
- Within the country or Cross-border telecom degradation
- Regulator escalation
- Physical risk to critical sites

4.3 Decision Rights

- Failover approval: **Gold**
- Routing changes, isolation, kill switches: **Silver**
- Public communications: **Gold**
- SWIFT/RTGS channel decisions: **Gold + Regulator Liaison**
- Execute technical steps and report to Silver**: Bronze**

4.4 War-Room Rhythm

- Situation Report (SITREP) **every 60 minutes** (15 minutes during active failover)
- Regulator updates **every 2-4 hours**
- Customer updates: **T0** (*Time Incident Declared*), **T+60** (*First Communication Time To Customer after declaring the incident*) , then **every 2-4 hours**

5. Critical & Important Business Services (C/IBS)

5.1 Service Catalogue

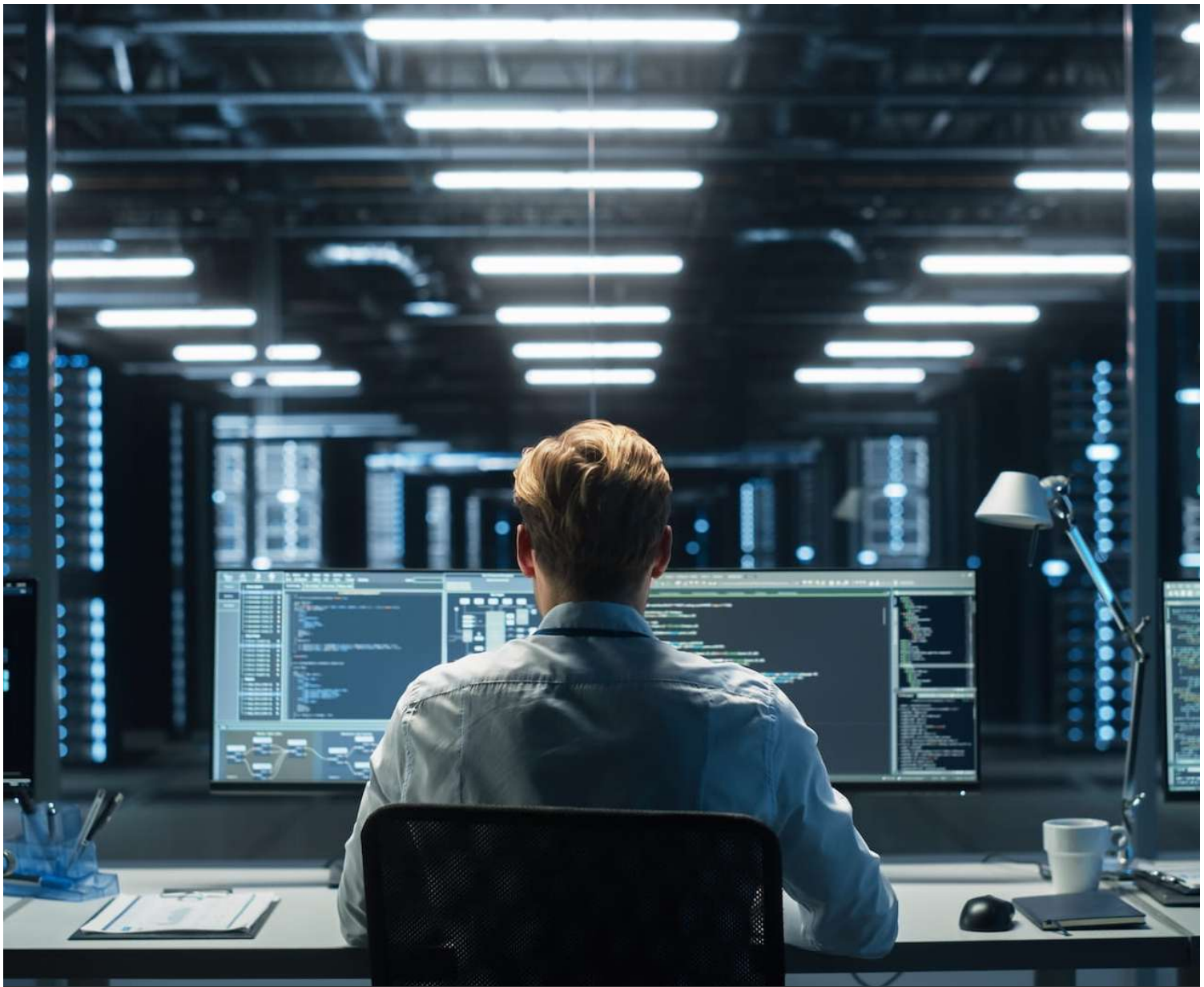
Tier 1: Core banking, payments, RTGS, SWIFT, digital channels, ATM, IAM

Tier 2: AML, screening, fraud, treasury, risk

Tier 3: Analytics, archive, non-critical batch

5.2 Impact Tolerances

- Tier 1 MTD: **≤60 minutes**
- RPO: **≤10 minutes**
- Customer cash access: **≥95%**
- Payment success: **≥97%**



6. Architecture for Survivability

Primary (local), Secondary (GCC), Tertiary (cloud/offshore)

6.1 Facilities & Power

- N+2 generators (*Every generator to have additional generators beyond the minimum*)
- 7–14 days autonomy
- Dual UPS (*uninterruptable Power Supply*)
- Physical hardening

6.2 Network & Telecom

- Multi-telco operators' connectivity
- Regional or offshore MPLS/SASE backbones
- Satellite overlay, if available
- Prebuilt DNS (*Domain Name System*)/geo-routing

6.3 Data Protection

- Encryption
- Immutable storage
- Air-gapped copies (***keeping ongoing backup data copies stored in a location that is completely isolated from any network — no internet, no LAN, no external connectivity***)
- Split key custody

6.4 Cloud Landing Zone

- Segmented VPC (*Virtual Private Cloud*)/VNET (*Virtual Network*)
- Cloud-native WAF/firewall
- KMS (*Key Management Servies*) integrated
- IaC (*Infrastructure as Code*) modules

7. Zero-Trust Cyber Controls

- MFA (*Multi Factor Authentication*) everywhere
- Just-In- Time privileged access
- Segmentation of payments/core/channels
- 100% EDR/XDR
- Patch CVEs (*Common Vulnerabilities & Exposures*) within hours
- Threat intel + deception

8. Crisis Communications

- Encrypted internal channels
- Out of Band Pagers (or communication devises/ methods) as alerting channels that operate **outside the primary network**, ensuring that critical alerts still reach engineers and war-room teams even when there is network and/or internet disruptions)
- Pre-approved customer messaging
- Regulator SITREP templates

9. Third-Party & Supply Chain Controls

- Reinforcement of Wartime SLAs with critical vendors
- API thinning (temporarily reducing or restricting the number of APIs, endpoints, or features exposed to customers or internal systems during high load or crisis scenarios)
- Cloud region diversification
- Vendor failover testing

10. Testing & Assurance

- Quarterly table-tops/ Simulation Exercises
- Semi-annual live failover
- Evidence packs & KPIs

FOR MORE INFORMATION:

Hashem Qtaishat
Technology Advisory Leader

Email:
hashem.qtaishat@bdo.com.kw
Phone: +965 2295 7593

www.bdo.com.kw