GCC BANKING RESILIENCE DURING REGIONAL CONFLICT

EXECUTIVE QUICK GUIDE

A rapid-action guide for Boards, Executive Committees, and Crisis Command Teams

01

Executive Summary

The GCC is now operating inside an active war-zone environment. Banks face simultaneous cyber warfare, physical disruption, telecom instability, and geopolitical escalation. Regulators have mandated minimum operational & cybersecurity resilience baselines that require banks to maintain operations even while under attack.

THE FUNDAMENTAL SHIFT:

FROM: Compliance	TO: Wartime
Documentation & periodic testing	Real-time survivability under attack

- Continuity of critical banking services
- Data survivability during disruption
- Cloud & multi-region failover readiness
- Cyber defense under hybrid warfare
- Communication & coordination resilience
- Alignment with regulatory wartime expectations

By Hashem Qtaishat- BDO Kuwait

02

Recommended Actions during **wartime**

Banks must immediately anchor operations around these **five wartime pillars:**

01	**Data Center Survivability**	Multi-region DC: Primary GCC, Secondary GCC, Offshore/Cloud	Hot-standby capability with **near-zero RPO**	Power independence: **N+2 generators** + 7–14 days fuel autonomy	
02	**Cloud Hot-Standby Activation**	Pre-built, pre-hardened cloud landing zone	Tier-1 workloads (Core Banking, Payments) failover **within hours**	Automated routing: DNS/SWIFT/RTGS endpoint redirection	
03	**Cyber Hardening (War-Room Posture)**	24/7 Cyber War-Room activation	Network segmentation (payments, core, endpoints, cloud)	Rapid patching (critical CVEs fixed in hours)	100% endpoint coverage with XDR/EDR
04	**Communications Redundancy**	Multi-telco failover	Cross-GCC routing	Satellite overlay, if available	Cloud-hosted customer messaging
05	**War-Room Governance**	Single operational command structure (CEO–COO–CISO–CTO)	Real-time dashboards (cyber + operations + communications)	Crisis SLAs aligned with regulators	National security coordination

03

Board & Executive **Checklist** (1/2)

A comprehensive governance framework to validate wartime readiness.

A. Strategy & Regulation

- Has the Board formally adopted a war-zone resilience posture?
- Are regional regulatory expectations fully embedded?
- Has 'operational survivability' replaced 'compliance' as priority?
- Are quarterly resilience briefings provided to the Board?

B. Data Centers & Power

- Do we operate in **three zones** (Primary GCC, Secondary GCC, Offshore/Cloud)?
- Can we execute **hot failover** at any moment?
- Do DCs provide **dual UPS (A+B)** and **N+2** redundancy?
- Is fuel autonomy secured for **7-14 days** with priority supply agreements?

C. Data Survivability

- Is all in-country customer data encrypted as per regulations?
- Do we maintain **immutable WORM backups** + **air-gapped** copies?
- Are encryption keys stored **outside** conflict envelopes?
- Are replication policies aligned with **<10 min RPO** targets?

D. Cloud Readiness

- Is the cloud landing zone **built, tested, and hardened?**
- Can Tier-1 systems failover within hours?
- Are DNS/SWIFT/RTGS rerouting procedures tested?
- Are multi-cloud or cross-region pathways validated?

E. Cyber Operations

- Is a **24/7 Cyber War-Room** activated with SOC + Intel + Network + Cloud teams?
- Is XDR/EDR deployed across 100% of endpoints and servers?
- Are critical vulnerabilities patched within **hours**, not weeks?
- Is lateral movement segmentation enforced (Core/Payments /Cloud)?

04

Board & Executive **Checklist** (2/2)

A comprehensive governance framework to validate wartime readiness.

F. Communications

- Do we have multi-telco redundancy fallback?
- Are encrypted channels enforced for crisis teams?
- Is customer messaging cloud-hosted and multi-region redundant?
- Are outage templates and regulator communication scripts pre-approved?

G. Third-Party Dependencies

- Are critical vendors operating under enforced wartime mode?
- Are non-essential APIs shut down during crisis?
- Are vendor cloud regions resilient or under stress?
- Are multi-cloud failover routes available for critical services?

H. Public Trust & Disinformation

- Is there **one official verified channel** for communication?
- Are we monitoring for social spoofing, phishing, misinformation?
- Do we have ready-to-deploy customer messaging for outages, payments, delays?
- Do we coordinate public messaging with regulators?

I. National Coordination

- Are we aligned with national wartime resilience frameworks?
- Do we deliver **hourly/daily updates** during active crises?
- Are we integrated with national cyber and security early-warning systems?
- Do we participate in cross-GCC crisis coordination calls?

CONTACT DETAILS

Hashem Qtaishat
Technology Advisory Leader

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

www.bdo.com.kw