INFORMATION AND COMMUNICATION TECHNOLOGY

Strengthening Cyber-Resilient Digital Communications in Saudi Banking under Vision 2030: Secure Voice, Video Conferencing, and Cloud Collaboration Infrastructure

Sajid Pasha Muhammed

Published November 2026

Abstract

Purpose: This paper investigates how Saudi banks can secure voice, video conferencing and cloud collaboration while maintaining communications during cyber incidents, electrical disruption and supplier failure.

Design/methodology/approach: A structured critical review integrates research published from 2020 to 2025 with recognised cybersecurity engineering guidance. Evidence is appraised across signalling, media, identity, hybrid cloud, governance and power-system dependencies.

Findings: Encryption alone cannot deliver operational resilience. The defensible model couples identity-centred access, segmented media paths, privacy governance, diverse connectivity, autonomous emergency communications and tested electrical continuity.

Research limitations: The synthesis does not represent a measured trial within a Saudi bank; projected outcomes require field validation.

Practical implications: Banks should prioritise recoverable communications, measurable failure containment and supplier exit capability alongside regulatory alignment.

Originality/value: The paper connects unified communications security with banking-sector contagion, physical electrical resilience and Vision 2030 digital-service continuity through an integrated architecture and assessment framework.

Keywords: Cyber resilience; Saudi banking; unified communications; secure voice; video conferencing; hybrid cloud; electrical continuity; Vision 2030

1 Introduction

Saudi Arabia's Vision 2030 positions digital financial services, institutional modernisation and technological capability as essential contributors to economic diversification. The communications estate supporting those ambitions is rarely assessed as a single critical system. Treasury conversations, remote customer service, fraud investigations, incident war rooms, executive approvals and contact-centre interactions all depend on interoperable telephony, conferencing, identity and collaboration services. An outage can therefore obstruct both routine productivity and the coordination needed to restore banking operations. Digital transformation changes business models and organisational relationships, not simply the channels through which information is transmitted (Verhoef et al., 2021).

Cloud meetings and mobile softphones may improve accessibility, yet they also combine public networks, identity providers, equipment vendors, recording services and dispersed administrators. Reisinger et al. (2023) demonstrate why confidentiality, anonymity and metadata protection must be distinguished when assessing unified communications. The challenge is amplified for banks because an attacker can use apparently ordinary meetings to solicit credentials, divert calls or collect commercially sensitive content. Equally damaging is an apparently secure system that becomes unusable when its cloud control plane, local call manager, internet transit or electrical supply fails.

This paper treats cyber resilience as the demonstrated capacity to anticipate, withstand, recover from and adapt to disruptive events while preserving essential communications. Security aims to prevent or constrain compromise; resilience adds survivability when preventive controls fail. The distinction matters because financial networks are interconnected: Eisenbach et al. (2022) show how cyber events can create amplified financial-system disruption through dependent institutions. Their payment-network analysis does not quantify conferencing losses, but it establishes a defensible reason to analyse communications as an operational dependency rather than an optional office service.

The principal contribution is a multi-layer framework that joins media and signalling safeguards with identity governance, supplier concentration controls, grid-aware infrastructure and measured recovery objectives. It explicitly avoids presenting a proposed design as proven deployment. Saudi-specific regulatory alignment is addressed as an evidence-based control-mapping responsibility, rather than a claim that a particular product or cloud topology is automatically compliant.

1.1 Aim and objectives

The aim is to establish a critically justified architecture for cyber-resilient banking communications in Saudi Arabia. The objectives are to identify threats across the voice, video and collaboration lifecycle; compare security and continuity trade-offs in on-premises, cloud and hybrid models; examine electrical and telecommunications interdependence; translate general control principles into auditable banking requirements; and formulate testable research propositions for Vision 2030 implementation. The guiding question is whether communications can remain trustworthy and operational when security, connectivity and physical-power assumptions break simultaneously.

2 Literature review and conceptual foundations

2.1 Collaboration security and communication-specific threats

Unified communications converges signalling, real-time media, presence, messaging, directories, screen sharing and recording. That convergence reduces operational fragmentation but increases the number of trust boundaries crossed by a single session. Reisinger et al. (2023) identify vulnerabilities affecting user privacy, meeting access and exposure of contextual information. Mohd Ramly et al. (2024) catalogue voice-over-IP threats including call hijacking, impersonation, denial of service and toll fraud. These findings cannot be collapsed into a generic network-risk score: an intercepted executive conversation and an unavailable emergency hotline produce different harms, control requirements and recovery priorities.

The distinction between signalling confidentiality and media confidentiality is fundamental. Transport protection for a session initiation exchange does not itself ensure that every subsequent audio stream is encrypted, correctly authenticated or inaccessible to a bridging service. Conversely,

encrypted media does not necessarily conceal participant identity, meeting timing, contact graphs or the destination of stored transcripts. Chen et al. (2025) provide empirical evidence that real-time communications applications can diverge from protocol specifications. Their observations caution against equating a vendor security claim with independently established interoperable behaviour. A bank therefore needs configuration-level verification, not only architectural diagrams or procurement questionnaires.

Voice security also entails operational compromises. Arpaci and Şentürk (2024) assess performance implications of combining firewalls and virtual private networks in conferencing. Protective gateways can add latency or complexity even as they reduce exposure. Suthar and Rughani (2020) survey practical voice-security controls, reinforcing the need for layered assessment rather than a single protective appliance. For real-time media, the security baseline must preserve acceptable delay, jitter, packet loss and call-setup completion during normal and degraded service. The relevant question is not whether all media travels through the most restrictive inspection path, but whether the chosen path provides an accountable level of protection without undermining safety-critical communication.

2.2 Cloud collaboration, organisational trust and banking governance

Cloud-hosted collaboration shifts much of the control plane outside direct bank ownership. This may offer geographical distribution, rapid patching and elastic capacity, yet the institution retains accountability for identity, data classification, retention, incident response and vendor oversight. Wang et al. (2024) show that banking digital transformation combines privacy and cybersecurity concerns with implementation challenges; their Pakistan-focused findings are informative but not automatically transferable to Saudi regulatory conditions. Cele and Kwenda (2024) synthesise digital-banking adoption threats, while Johri and Kumar (2023) document the significance of customer cybersecurity awareness in Saudi banking. Together these studies indicate that human trust and governance affect whether technically capable systems are used safely.

Financial performance offers an incomplete measure of resilience. Sayari (2024) reports associations between internet banking and profitability in Saudi conventional and Islamic banks, whereas Aldaarmi (2024) finds that digital transformation does not uniformly translate into a significant direct performance effect. Neither study tests the availability of an encrypted call during a sustained outage. This creates a methodological warning: adoption, satisfaction and accounting performance cannot substitute for communications-specific reliability measures. Elsayed et al. (2024) further locate cyber disclosure within broader banking governance, supporting board-level accountability without demonstrating that disclosure itself guarantees engineering readiness.

Zero-trust approaches offer a useful organising principle but are not turnkey designs. Rose et al. (2020) require explicit verification of subjects and devices before resource access; Fernández and Brazhuk (2024) argue that architectural ambiguities persist in practical implementations. Itodo and Ozer (2024) similarly highlight the gap between proposed principles and documented deployment evidence. A bank should therefore specify which communications resources, identities and control decisions are protected, rather than labeling an entire estate zero trust. Azad et al. (2024) extend that concern to heterogeneous connected devices, an important consideration for desk phones, conference-room systems and branch appliances with different patchability and hardware lifecycles.

2.3 Electrical and digital dependencies

Cyber-resilient collaboration depends on electricity, environmental controls, physical facilities and external networks. Ahmed et al. (2021a) analyse reliability implications of data-centre internal power architectures; Ahmed et al. (2021b) review energy and reliability modelling across data-centre components. Gazzola et al. (2023) show why territorial threats and interdependent protection resources belong in continuity assessment. These contributions counter the convenient but misleading assumption that an internet-connected backup site is independent when both sites share a power corridor, cooling vulnerability or telecommunications exchange.

Power-grid research adds a second perspective. Salvi et al. (2022) propose learning-oriented cyber resilience through digital twins in electrical infrastructure, and Ayele et al. (2024) evaluate secure communication protocols for distributed microgrids. Nair et al. (2025) demonstrate a framework for coordinating trusted grid-edge resources. Banking systems do not operate microgrid controls, but they rely on the energy system those controls support. The legitimate transfer is methodological: bank continuity plans should model electrical dependencies, communication delay, restoration sequencing and correlated infrastructure failures. It would be unsound to infer any specific Saudi blackout probability or resilience improvement from these cross-domain studies.

2.4 Synthesis and gap

The evidence falls into four partially disconnected streams: media security, enterprise identity, banking governance and infrastructure continuity. Real-time communications work is technically detailed but seldom models monetary-service criticality; banking research tends to examine customers, disclosure or general cyber loss; power resilience studies emphasise physical and cyber-physical control. The unresolved problem is how to select controls under competing constraints of privacy, call quality, recoverability and supplier concentration. This study addresses that intersection through a control architecture and scenario-based evaluation, without claiming new empirical effects.

3 Review methodology

3.1 Design and source selection

A structured, critical narrative review was selected because the research question crosses technology standards, organisational governance and critical infrastructure engineering. Sources were sought by combining phrases for unified communications, voice security, WebRTC, video conferencing, zero trust, cloud collaboration, bank cyber risk, data-centre power and microgrid communications. The publication window was restricted to 2020–2025; seminal older background was excluded from the final reference set. Preference was given to peer-reviewed journal articles, conference proceedings and formally issued technical standards with identifiable digital object identifiers. The included literature was examined for mechanisms and applicability rather than pooled into a numerical effect estimate.

Source eligibility required a direct contribution to one of the analytical layers, methodological transparency or a recognised normative control baseline. Conceptual studies were separated from case studies and empirical measurement papers. A geographically external result could inform a failure mechanism but was not treated as measured Saudi evidence. Research on electricity was included only where it clarified communications availability or correlated failure. The review intentionally does not report database hit counts, duplicate-removal statistics or inter-reviewer

agreement because those metrics were not generated. Accordingly, this is a reproducibly described critical synthesis, not an exhaustive systematic review or a meta-analysis.

3.2 Critical appraisal and synthesis

Each source was appraised against four questions: what claim was actually tested; what system or population was studied; which threats or dependencies remained outside scope; and how cautiously the evidence could be transferred to Saudi banking. Normative guidance was distinguished from observed outcomes. The United States National Institute of Standards and Technology cybersecurity framework provides governance and risk-management structure (NIST, 2024), while its security-control catalogue provides implementation categories (NIST, 2020). Neither is itself a Saudi legal determination or evidence of successful deployment. Incident-response guidance informs exercises and organisational learning (NIST, 2025).

The synthesis uses a failure-path matrix, architectural reasoning and a proposed measurement framework. No interviews, packet captures, penetration tests, power measurements or bank-specific records were collected for this paper. Thus, tables express analytical judgements and requirements, not invented effectiveness percentages. The exact limits of that evidence matter: high-confidence mechanisms can support design recommendations, whereas causal claims about Saudi outcomes require prospective validation.

4 Proposed cyber-resilient communications architecture

4.1 Functional layers and trust boundaries

The proposed architecture contains five connected planes: endpoints; identity and policy; signalling and call control; media and collaboration; and continuity infrastructure. Endpoint inventory covers desk telephones, mobile clients, branch contact-centre workstations, conferencing equipment and privileged administration consoles. The identity plane provides role-aware authentication, device posture checks, certificate lifecycle management and timely access revocation. The signalling plane contains registration services, session border controllers, dial plans and call-routing controls. The media plane includes encrypted audio, video, screen sharing, messaging and approved storage. The continuity plane encompasses independent connectivity, standby call routing, electrical distribution, uninterruptible power supplies, generators, cooling and tested recovery procedures.

An identity-first design must not assume that a successful login establishes lasting trust. Access to executive meetings, payment-approval bridges, call recordings and emergency administration requires different privileges. High-risk joining actions should be challenged without repeatedly interrupting legitimate low-risk conversation. Organisational directories should provision approved identities and synchronise status, but the collaboration directory should not become an unbounded replica of banking personnel data. Directory integration must use scoped attributes, separate service accounts, managed secrets, reconciliation alerts and defensible deprovisioning deadlines. A stale account is simultaneously a confidentiality risk and an incident-containment failure.

Figure 1 locates the principal trust boundaries and resilience dependencies. The architecture deliberately avoids claiming that deployment of one vendor, named cloud provider or session border controller guarantees compliance. Interoperability is a design objective that requires proof using actual bank configurations, emergency call paths and recording policies. Centralised policy is valuable when consistent, but a single unreachable policy engine can become the reason no call can

be established. Local emergency operation should therefore be separately authorised, narrowly scoped and logged for subsequent reconciliation.

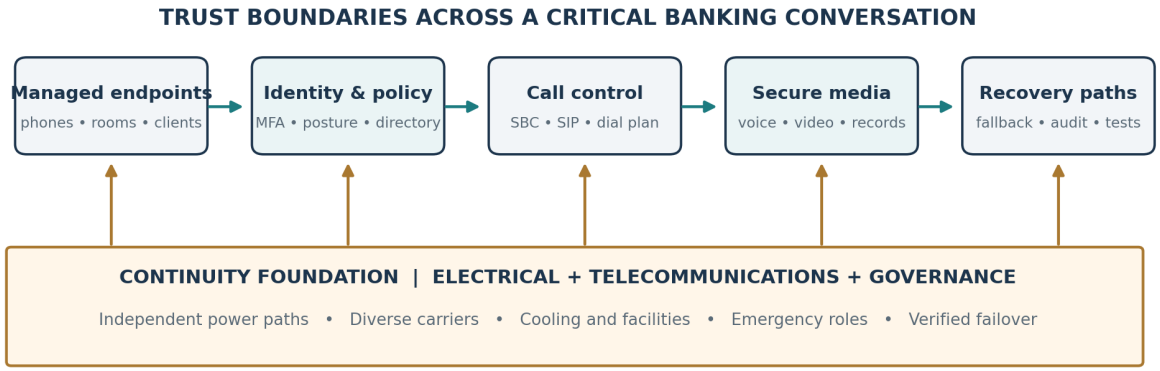

Figure 1. Original conceptual architecture showing trust boundaries, secure call handling and underlying electrical, telecommunications and governance dependencies. Source: author-developed analytical framework.

4.2 Secure voice and signalling

A protected call begins before audio starts. Registration requests, endpoint certificates, dial plans, signalling gateways, administrator credentials and telephony trunks provide different attack surfaces. Banks should bind endpoints to managed identities, encrypt signalling where supported, authenticate trunk relationships and restrict management interfaces to controlled zones. Session border controllers can normalise signalling and constrain external exposure, but they also create operational choke points. Redundant controllers must be tested for split-brain conditions, certificate mismatch, trunk failover and loss of upstream name resolution, not merely for hardware switchover.

Voice-media encryption should be verified end to end for defined call classes, including internal calls, interbank communications and contact-centre transfers. When gateways decrypt and re-encrypt streams, the bank must document where plaintext exists, who controls the keys and which lawful recording functions can access content. A meeting protected on a client may lose equivalent protection at a dial-in gateway; Reisinger et al. (2023) identify precisely this class of interoperability caveat. Recording is a governed exception, not proof that all communication should be stored indefinitely. Access logs, retention limits, integrity checks and purpose restrictions should follow the sensitivity of the conversation.

Call survivability requires a separate routing plan. A branch facing wide-area disconnection may need local internal calling, approved emergency numbers and a manual escalation route even if the ordinary cloud directory is unreachable. During a ransomware containment event, banking administrators should be able to activate predefined crisis communications from a clean administrative environment. However, unrestricted fallback accounts would defeat the purpose of containment. The compromise is a small, rehearsed set of emergency roles with time-limited permissions, dual control where feasible and post-event review. Mohd Ramly et al. (2024) support a broad threat model; the proposed safeguards are architectural responses requiring local validation.

4.3 Video conferencing, media privacy and collaboration data

Video conferences have a larger disclosure surface than voice calls: participant lists, calendars, meeting URLs, captions, shared screens, chat attachments, transcripts and cloud recordings all reveal

context. Invitations should use expiring access mechanisms and validated guest policies. Meeting organisers should distinguish public webinars from executive decision rooms and confidential investigations. Waiting rooms, host approvals and participant re-authentication address meeting intrusion, while data loss prevention and restrictive default sharing reduce accidental leakage. Yet strict controls can also obstruct urgent coordination; emergency templates should be pre-approved rather than invented during an incident.

Media protection must be evaluated across clients and gateways, not judged from a marketing label. Mahmoud and Abozariba (2025) identify interoperability, connectivity, security and user-experience challenges in WebRTC deployments. Chen et al. (2025) further question assumptions about uniform standards compliance. Banks should therefore capture representative signalling traces in an authorised test environment, verify negotiated cipher suites and key exchange, examine relay behaviour and confirm that external dial-in participants do not silently alter confidentiality guarantees. Where application-level end-to-end protection cannot coexist with regulated recording, banks should explicitly select and document the lawful compromise instead of promising both without qualification.

Cloud content governance extends beyond the duration of a call. Transcripts, searchable chat, meeting metadata and automated summaries can create additional regulated information assets. Data minimisation should address whether content is created at all, rather than relying exclusively on encryption after collection. Search permissions, legal holds, e-discovery, cross-border processing, backup copies and deletion propagation require joint approval from legal, risk, technology and business owners. Wang et al. (2024) illustrate the governance implications of banking data transformation. The wider lesson is that a usable collaboration service must be engineered with traceable information lifecycles, particularly when staff operate across subsidiaries and third-party providers.

4.4 Cloud, on-premises and hybrid deployment trade-offs

A fully local deployment may provide stronger direct control over routing and storage but requires sustained patching, redundant sites and specialist operations. A cloud deployment can improve feature delivery and geographical reach, but it introduces dependence on provider identity systems, external connectivity, contractual remedies and service-side changes. Hybrid deployment can preserve local call control and selected recording functions while extending meetings and remote collaboration through a managed service. Its weakness is integration complexity: directory synchronisation, dial-plan consistency, certificate renewal and cross-platform emergency procedures become shared failure domains.

Table 1 compares these trade-offs without treating one topology as universally preferable. Selection should depend on business impact analysis, authorised data flows, local support maturity, adversarial exposure and demonstrable recovery. A nominally diverse cloud design is not resilient if both regions depend on a single identity provider, domain-name service, backbone route or privileged administrative account. Similarly, a dual-site local design can share utility substations or cooling-water dependency. The bank must document common-cause failure explicitly before interpreting redundancy as independence. Rose et al. (2020) supply the verification principle, whereas Gazzola et al. (2023) clarify the physical dependency dimension.

Table 1. Comparative deployment trade-offs for Saudi banking communications.

Assessment dimension	Bank-operated local	Cloud-hosted service	Hybrid integration
Direct operational control	High; local specialist burden	Provider-mediated; contractual	Split; detailed RACI required
Identity dependency	Local availability possible	Cloud login often critical	Federated identity can be shared risk
Network fault response	Branch and carrier constrained	Internet and provider constrained	Alternative call paths feasible
Media and recording	Local key and storage design	Provider features and data controls	Gateways complicate encryption
Power and facilities	Own UPS, cooling and generation	Provider site, local access still needed	Both local and provider dependencies
Exit and recovery	Hardware and platform portability	Export terms and service continuity	Interoperability testing essential

4.5 Electrical continuity and telecommunications dependencies

The electrical dimension is not incidental to a communications paper. Session border controllers, core switches, branch access devices, authentication platforms, telephony servers, wireless access points and cooling systems require protected power. Uninterruptible power supplies can bridge short disturbances, while longer continuity depends on generation, fuel availability, distribution design and maintenance. Electrical protection must be coordinated with orderly service shutdown and restart. Restoring power to a building does not automatically restore a damaged call database, expired certificate, unavailable external carrier or saturated conference bridge.

Ahmed et al. (2021a) demonstrate how internal distribution architecture affects data-centre reliability; their results should not be converted into assumed availability for a specific Saudi bank. The practical implication is to test electrical failure at the level of complete services. Exercises should confirm that network devices, identity services and emergency call routes remain operational for the same required period, under realistic cooling loads. A generator-backed server is not useful when the attached network switch has no surviving power path. Likewise, a redundant cloud meeting service cannot overcome the loss of every carrier entering an affected district.

Figure 2 therefore represents resilience as a sequence of correlated failures and controlled degradation. The relevant design unit is the critical conversation, not the individual server. Power planning should consider heat-related equipment stress, maintenance windows and simultaneous demand on alternative sites, but numerical probabilities must be derived from verified local data. Lessons from secure microgrid communication (Ayele et al., 2024) and digital-twin-based power resilience (Salvi et al., 2022) support dependency mapping and learning-oriented simulations, not unsupported equivalence between banking voice traffic and grid control protocols.

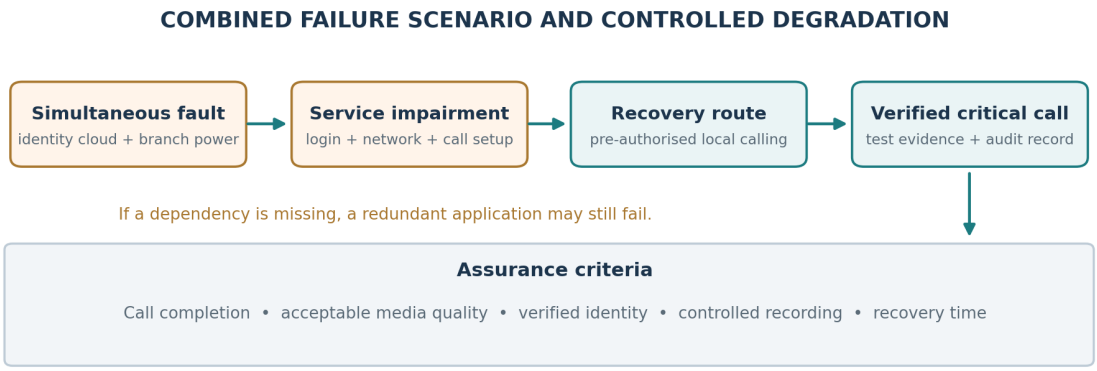

Figure 2. Original scenario model connecting simultaneous identity and electrical failures with pre-authorised recovery and measurable service assurance. Source: author-developed analytical framework.

5 Critical evaluation of risk and control effectiveness

5.1 Threat-to-control analysis

Table 2 links six disruption mechanisms to primary safeguards, residual weaknesses and evidence required before a control can be considered effective. The analysis resists treating technologies as binary protections. Multi-factor authentication is valuable against stolen credentials, for example, but may not prevent abuse of an already trusted session or the fraudulent approval of a privileged joining request. Segmentation reduces lateral reach, yet may complicate media relaying and discovery. Encryption protects content in transit but does not protect data once displayed to an authorised yet compromised endpoint. Each control therefore requires an assumption register describing what it protects, what it cannot protect and how failure will be detected.

Table 2. Scenario-based threat, residual risk and assurance requirements.

Threat / fault	Primary control	Residual exposure	Verification test
Caller spoofing or hijacking	Mutual authentication; constrained trunks	Compromised approved endpoint	Spoofed registration and trunk-failure exercise
Meeting intrusion or leakage	Guest policy; protected media; DLP	Screenshots and disclosed metadata	External guest and dial-in test
Identity provider compromise	Least privilege; separate emergency identity	Shared privileged access	Revoke and restore critical role
Supplier or carrier outage	Diverse routing; standby communications	Common upstream dependencies	Simultaneous control-plane and ISP loss
Electrical interruption	UPS; generator; supported switches	Cooling and fuel continuity	Full-service outage and restart exercise
Recording or transcript misuse	Retention; encryption; audited access	Authorised insider misuse	Lifecycle deletion and restore test

Cyber risk should be assessed against scenarios that combine security with availability. A compromised conferencing administrator might disable authentication, redirect recordings and delete audit logs. A successful denial-of-service attack might coincide with an external carrier fault. A supplier update could cause widespread client failures without malicious activity. A regional

electrical disruption could force traffic towards one remaining conference service precisely as a phishing campaign targets staff under pressure. NIST (2025) frames incident response as an integrated risk-management activity; the present model converts that principle into communication-specific recovery rehearsals.

5.2 Prioritisation and governance mechanisms

Prioritisation must begin with the service that the bank cannot safely postpone. Crisis-management bridges, fraud-response hotlines, treasury coordination and statutory or contractual escalation may warrant stronger survivability than everyday team meetings. Nevertheless, sensitivity does not map directly onto urgency: an executive video meeting may be confidential but deferrable, whereas an ordinary-looking branch call may support a time-critical incident. Service owners should assign both information classifications and maximum tolerable disruption, then approve the necessary technical routing and recording arrangements.

Peihani (2022) argues for a resilience-oriented perspective on bank cyber regulation, while Uddin et al. (2023) link digital banking to changes in operational-risk exposure. These studies support more realistic governance than purchasing controls solely to satisfy a checklist. A board-facing dashboard should distinguish preventive coverage from resilience evidence: completed failover tests, successful emergency calls, verified restoration of meeting authentication, and the proportion of critical services that survive loss of a major supplier. Governance reporting must also capture failed tests and unresolved dependencies, because a polished availability percentage conceals correlated outages.

5.3 Decision criteria and operational measures

A practical assessment includes confidentiality of high-sensitivity media, probability of unauthorised meeting entry, integrity of caller identity, successful call establishment under degraded networks, time to recover a critical bridge, dependency concentration and audit completeness. These are proposed measurement categories, not estimated values. For each service, owners should document an explicit recovery-time objective, a recovery-point objective where stateful call data matters, and an evidence-based maximum outage tolerance. Quality thresholds for jitter, delay and packet loss should be set for the actual codec, network and task rather than copied from unrelated environments.

Security and resilience can pull in opposite directions. Deep inspection may delay calls; strict identity revocation can strand emergency users; a single master directory simplifies governance but concentrates operational risk. The correct response is to test trade-offs using pre-authorised exceptions with compensating controls. A bank should consider a control effective only if it reduces the targeted risk without creating a more consequential failure mode elsewhere. This standard is demanding but consistent with the objective of sustaining trusted financial services, not merely achieving favourable configuration scores.

6 Discussion, limitations and research agenda

The central finding of this synthesis is architectural rather than statistical: a communication service is cyber resilient only when trust decisions and critical conversations survive plausible combinations of compromise, supplier unavailability and infrastructure degradation. This interpretation challenges two common assumptions. First, secure media does not guarantee a secure meeting ecosystem when directories, recordings and invitation workflows remain exposed. Secondly, redundant applications do not guarantee continuity when they share electrical, identity or carrier dependencies. Control

effectiveness must therefore be evaluated across a complete service chain, including people and physical facilities.

For Saudi banks, Vision 2030 provides a strategic rationale for reliable digital collaboration, but national ambition should not be confused with measured engineering performance. The proposed architecture can support customer access, distributed financial operations and incident coordination, provided deployment decisions remain proportionate to operational criticality. Banking regulators, national cybersecurity requirements and personal-data obligations should be mapped to actual contracts, processing locations and control owners using current official instruments. This review does not purport to certify a particular provider against those obligations. Technical governance should be demonstrable through test records and independent challenge rather than product accreditation language alone.

Four research priorities follow. First, controlled simulations should compare cloud-only, local and hybrid arrangements under identical combined network, identity and power faults, measuring both recovery and media confidentiality. Secondly, field studies should assess whether repeated emergency-communications exercises improve restoration decisions, not simply participants' confidence. Thirdly, privacy research should quantify metadata exposure across conferencing gateways and regulated recording architectures. Fourthly, longitudinal evidence should investigate whether supply-chain diversification genuinely reduces common-mode failures after accounting for shared telecommunications, electrical and identity infrastructure. Munusamy and Khodadi (2023) identify organisational capabilities relevant to building cyber resilience, although their analysis does not establish outcomes for Saudi banks.

A staged implementation sequence follows from this analysis. Banks should first inventory mission-critical conversations and their dependency chains, recording which capabilities must function when external administration is unavailable. They should then classify the confidentiality and recovery needs of each workflow, before selecting network segmentation, recording locations and fallback dial plans. Independent assurance should challenge supplier resilience claims using evidence from realistic exercises. Subsequent phases should test simultaneous loss of a conferencing control plane and a branch electricity supply; verify emergency authentication when normal directory synchronisation stops; and restore recordings without granting excessive privileges. Procurement contracts should specify incident notification, data portability, independent audit evidence and an achievable exit procedure. The value of these requirements lies in their falsifiability: a failed exercise produces an observable control weakness that can be corrected. Shared ownership among security, telecommunications, facilities and business continuity teams prevents the dangerous separation of electronic availability from operational banking obligations.

These arrangements must also evolve as threats and banking service dependencies change.

Important limitations remain. The selected evidence spans different countries, industries and research designs, preventing pooled causal estimation. Technical standards describe desirable practices but do not establish achieved effectiveness. The proposed layer boundaries simplify real deployments, where cloud platforms and carrier networks may conceal operational dependencies. No Saudi banking architecture was independently examined, and no quantitative claim is made regarding outage reduction, financial savings or national grid reliability. These limitations are reasons for transparent scenario testing, not for abandoning implementation guidance.

7 Conclusion

Cyber-resilient digital communications require more than secure telephones, encrypted video or modern collaboration subscriptions. Saudi banking institutions need a governed system of identities, trusted signalling, protected media, controlled data lifecycles, independent emergency routes and tested electrical continuity. The proposed framework identifies where those layers interact and where apparently strong controls can create new concentrations of risk. Its practical value rests on making assumptions explicit and translating them into measurable scenarios. Under Vision 2030, progress should be judged by sustained trustworthy collaboration during disruption, with documented recovery evidence and accountable governance under genuine operating conditions, rather than by feature adoption alone.

References

[1] Ahmed, K.M.U., Alvarez, M. and Bollen, M.H.J. (2021a), Reliability Analysis of Internal Power Supply Architecture of Data Centers in Terms of Power Losses. *Electric Power Systems Research*. https://doi.org/10.1016/j.epsr.2021.107025

[2] Ahmed, K.M.U., Bollen, M.H.J. and Alvarez, M. (2021b), A Review of Data Centers Energy Consumption and Reliability Modeling. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3125092

[3] Aldaarmi, A.A. (2024), Fintech Service Quality of Saudi Banks: Digital Transformation and Awareness in Satisfaction, Re-Use Intentions, and the Sustainable Performance of Firms. Sustainability, 16(6), 2261. https://doi.org/10.3390/su16062261

[4] Arpaci, S. and Şentürk, A. (2024), Performance Analysis of Firewall and Virtual Private Network (VPN) Usage in Video Conferencing Applications. Düzce University Journal of Science and Technology, 12(4), pp. 1879–1894. https://doi.org/10.29130/dubited.1462133

[5] Ayele, E.D., Gonzalez, J.F. and Teeuw, W.B. (2024), Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. Sensors, 24(3), 854. https://doi.org/10.3390/s24030854

[6] Azad, M.A., Abdullah, S., Arshad, J., Lallie, H. and Ahmed, Y.H. (2024), Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*. https://doi.org/10.1016/j.iot.2024.101227

[7] Cele, N.N. and Kwenda, S. (2024), Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), pp. 31–48. https://doi.org/10.1108/JFC-10-2023-0263

[8] Chen, P., Qiu, P., Lambda and Liu, Z. (2025), Protocol Compliance in Popular RTC Applications. Proceedings of the ACM Internet Measurement Conference, pp. 294–307. https://doi.org/10.1145/3730567.3764438

[9] Eisenbach, T.M., Kovner, A. and Lee, M.J. (2022), Cyber risk and the U.S. financial system: A pre-mortem analysis. Journal of Financial Economics, 145(3), pp. 802–826. https://doi.org/10.1016/j.jfineco.2021.10.007

[10] Elsayed, D.H., Ismail, T.H. and Ahmed, E.A. (2024), The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. Future Business Journal, 10, 115. https://doi.org/10.1186/s43093-024-00402-9

[11] Fernández, E.B. and Brazhuk, A. (2024), A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832. https://doi.org/10.1016/j.csi.2024.103832

[12] Gazzola, V., Menoni, S., Ghignatti, P., Marini, A., Mauri, R. and Oldani, G. (2023), Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers. Sustainability, 15(7), 6005. https://doi.org/10.3390/su15076005

[13] Itodo, C. and Ozer, M. (2024), Multivocal literature review on zero-trust security implementation. Computers & Security, 141, 103827. https://doi.org/10.1016/j.cose.2024.103827

[14] Johri, A. and Kumar, S. (2023), Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies, 2023, 2103442*. https://doi.org/10.1155/2023/2103442

[15] Mahmoud, H. and Abozariba, R. (2025), A systematic review on WebRTC for potential applications and challenges beyond audio video streaming. Multimedia Tools and Applications, 84, pp. 2909–2946. https://doi.org/10.1007/s11042-024-20448-9

[16] Mohd Ramly, A., Ng, Z.W., Khamayseh, Y., Kwan, C.S.C., Amphawan, A. and Neo, T.-K. (2024), Review and Enhancement of VoIP Security: Identifying Vulnerabilities and Proposing Integrated Solutions. Journal of Telecommunications and the Digital Economy, 12(4), pp. 109–136. https://doi.org/10.18080/jtde.v12n4.1022

[17] Munusamy, T. and Khodadi, T. (2023), Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security. Journal of Informatics and Web Engineering, 2(2), pp. 59–71. https://doi.org/10.33093/jiwe.2023.2.2.5

[18] Nair, V.J., Srivastava, P., Venkataramanan, V. et al. (2025), Resilience of the electric grid through trustable IoT-coordinated assets. *Proceedings of the National Academy of Sciences, 122*. https://doi.org/10.1073/pnas.2413967121

[19] National Institute of Standards and Technology (NIST) (2020), Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53 Revision 5. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-53r5

[20] National Institute of Standards and Technology (NIST) (2024), The NIST Cybersecurity Framework (CSF) 2.0. *NIST Cybersecurity White Paper 29*. https://doi.org/10.6028/NIST.CSWP.29

[21] National Institute of Standards and Technology (NIST) (2025), Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. *Special Publication 800-61 Revision 3*. https://doi.org/10.6028/NIST.SP.800-61r3

[22] Peihani, M. (2022), Regulation of Cyber Risk in the Banking System: A Canadian Case Study. Journal of Financial Regulation, 8(2), pp. 139–161. https://doi.org/10.1093/jfr/fjac006

[23] Reisinger, T., Wagner, I. and Boiten, E.A. (2023), Security and Privacy in Unified Communication. *ACM Computing Surveys, 55(3)*. https://doi.org/10.1145/3498335

[24] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture. *NIST Special Publication 800-207*. https://doi.org/10.6028/NIST.SP.800-207

[25] Salvi, A., Spagnoletti, P. and Saad Noori, N. (2022), Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102507

[26] Sayari, S. (2024), Driving Digital Transformation: Analyzing the Impact of Internet Banking on Profitability in the Saudi Arabian Banking Sector. Journal of Risk and Financial Management, 17(5), 174. https://doi.org/10.3390/jrfm17050174

[27] Suthar, D. and Rughani, P.H. (2020), A Comprehensive Study of VoIP Security. 2020 International Conference on Advances in Computing, Communication Control and Networking, pp. 812–817. https://doi.org/10.1109/ICACCCN51052.2020.9362943

[28] Uddin, M.H., Mollah, S., Islam, N. and Ali, M.H. (2023), Does digital transformation matter for operational risk exposure?. Technological Forecasting and Social Change, 197, 122919. https://doi.org/10.1016/j.techfore.2023.122919

[29] Verhoef, P.C., Broekhuizen, T., Bart, Y. et al. (2021), Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, pp. 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

[30] Wang, S., Asif, M., Shahzad, M.F. and Ashfaq, M. (2024), Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & Security, 147, 104051. https://doi.org/10.1016/j.cose.2024.104051