Operational Resilience for New Entrants: Vendors, Data, Cyber and Business Continuity

A Board Framework for Critical Services, Third-Party Dependencies, Data Control, Cyber Readiness and Tested Recovery

Authored by Chennakeshav Adya, Independent Researcher

August 2026

Abstract

Operational resilience is a market-entry design decision. A new entrant can obtain a licence, sign a lease, select cloud and software providers, recruit staff and begin selling while remaining unable to sustain the services that matter when a vendor fails, data becomes unavailable, a cyber incident propagates or a facility is lost. The weakness often sits between functions: the commercial promise assumes continuous service; the operating model depends on concentrated third parties; the contract lacks usable audit or exit rights; data flows cross legal boundaries; recovery plans restore technology without restoring the customer outcome.

This paper develops a board framework for designing resilience before launch. It connects the critical-service view used in leading operational-resilience regimes with UAE requirements on outsourcing, operational risk, personal data, information assurance and regulated financial services. The framework defines important services, maps end-to-end dependencies, classifies providers by materiality and substitutability, translates risk into contractual controls, sets impact tolerances and recovery objectives, integrates cyber and continuity disciplines, tests severe but plausible scenarios, and preserves exit and insourcing options. It also treats resilience as a value and transaction issue because hidden dependencies can change implementation cost, required capital, customer confidence and the price a buyer is willing to pay.

Six original figures and six tables provide a critical-service architecture, regulatory-perimeter map, vendor criticality decision tree, data-control bridge, scenario-testing system, 180-day implementation plan, evidence registers and board metrics. Numerical examples and timings are management assumptions for planning; they are not forecasts, regulatory determinations or statements about a specific company. The analysis reflects official sources available in August 2026 and is educational. It does not replace legal, regulatory, data-protection, cybersecurity, technical, insurance, employment, tax, transaction or financing advice.

JEL Classification: G34, L22, M15, M21, O33

Keywords: operational resilience, UAE market entry, third-party risk, vendor governance, data protection, cybersecurity, business continuity, impact tolerance, exit planning, scenario testing

1. Make resilience a condition of market entry

Market entry is often managed as a sequence of approvals, premises, people, providers and launch milestones. Operational resilience requires another sequence: define what must continue, identify what can stop it, decide how much disruption the organisation can absorb, and build credible options for response and recovery. The sequence belongs in the entry thesis because key dependencies are selected early. Entity structure determines the legal and regulatory perimeter. Customer promises define service obligations. Technology choices establish data locations and concentration. Vendor contracts determine access, testing and exit rights. Staffing choices determine whether critical knowledge exists locally or remains with a distant parent or supplier.

The board should frame resilience around services and outcomes. A customer does not experience an application, a business-continuity document or a vendor register. The customer experiences whether an order is accepted, a payment is processed, an instruction is executed, a claim is handled, a facility is available, a report is delivered or support responds. A critical service is therefore an end-to-end outcome supported by people, process, technology, information, premises and third parties. Its resilience cannot be delegated to one control function.

The entry investment case should contain a resilience memorandum before binding commitments. The memorandum identifies critical services, legal entities, customer harms, regulatory obligations, single points of failure, critical providers, data jurisdictions, recovery objectives, testing requirements, residual exposures, contingency funding and accountable executives. It also records uncertainties. Where the applicable regulatory treatment has not been confirmed, management obtains qualified advice before committing to an architecture that may be difficult to unwind.

This discipline creates a more credible launch plan. Procurement teams can negotiate the required rights before leverage disappears. Finance can include redundancy, testing and exit costs in the budget. Sales can align service levels with demonstrable capability. Technology teams can design observability, segregation and portability into the platform. The board receives an executable route from licence to dependable service rather than a launch date supported by disconnected workstreams.

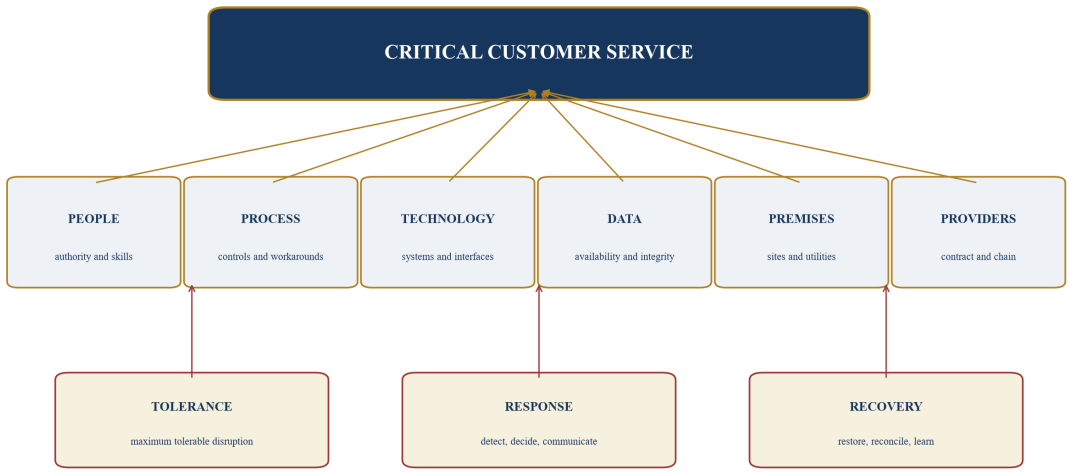
The commercial model should separate baseline operating cost from resilience-enabling cost. Baseline cost delivers the service under expected conditions. Resilience-enabling cost covers independent backups, redundant capacity, alternate communications, specialist response, assurance, exercising and exit readiness. Management can then explain which expenditure protects a customer commitment, satisfies an obligation or preserves strategic flexibility. The distinction also helps the board challenge resilience theatre: spending that creates documents or duplicate components without reducing an identified failure mode.

Table 1. Market-entry resilience diagnostic

Gate	Board question	Minimum evidence	Failure signal	Required decision
critical service	which customer or market outcomes cannot remain unavailable?	service inventory, customer-harm statement and accountable owner	systems are listed without outcomes	define service and tolerance
regulatory perimeter	which entity, activity, data and provider rules apply?	dated legal and regulatory map	group policy is assumed to satisfy local rules	validate and remediate
dependency architecture	what people, process, technology, data, premises and providers support the service?	end-to-end dependency map	a material subcontractor or manual step is missing	map and test
vendor control	can the firm oversee, audit, secure, continue and exit the arrangement?	diligence file, contract schedule, register and exit plan	commercial terms precede control requirements	renegotiate or redesign
data control	where does information originate, travel, persist, back up and leave?	approved data-flow and jurisdiction register	data location or processor chain is unknown	stop transfer and validate
recovery capability	can the service remain within an approved disruption limit?	impact tolerance, recovery objectives and test evidence	recovery time is a supplier assertion	test the end-to-end service
financial capacity	what redundancy, response and recovery funding is required?	approved budget, insurance and liquidity plan	launch economics exclude resilience costs	reprice, fund or defer

The evidence standard should reflect the service, sector, customer promise and applicable law. Open items remain visible until independently validated.

Figure 1. Critical-service resilience architecture



Governance connects service ownership, dependency evidence, disruption limits and tested recovery.

Customer outcomes sit above enabling resources. Each critical dependency must have ownership, evidence, tolerance and a tested response.

2. Define the services and harms that matter

The service definition anchors every later decision. It should be narrow enough to own and test, while broad enough to describe the customer outcome. "Technology" is too broad. "Core banking platform" is a system, not a service. "Allow a customer to view an accurate balance and initiate an authorised payment" describes an outcome whose disruption can be measured. The same principle applies outside finance: dispatching a time-critical shipment, maintaining a cooling service, confirming an investor subscription, completing payroll, issuing a verified valuation or operating a safety-critical industrial process.

Each service receives an owner with authority across functions. The owner documents the customers and counterparties affected, contractual and regulatory obligations, volumes, operating windows, geographic reach, peak periods, downstream dependencies and acceptable degraded modes. The owner also describes harms in practical terms: customers unable to access money; transactions duplicated or lost; confidential data exposed; safety compromised; statutory deadlines missed; markets disrupted; counterparties unable to reconcile; or a product rendered unusable.

Impact tolerances should express the maximum disruption the organisation is prepared to accept for a service, not the target time for an individual system. A tolerance can combine duration, volume, value, backlog, customer count, data integrity and safety. A two-hour outage at low volume can differ materially from a two-hour outage during settlement, month end or a regional event. A service can be technically available while producing incorrect results, so integrity and reconciliation conditions belong in the tolerance.

The board approves tolerances after considering legal obligations, customer commitments, financial capacity and plausible recovery capability. An ambitious number unsupported by architecture and testing is a slogan. A generous number that exposes customers or the licence is equally weak. Management should document the rationale, dependencies and planned investment needed to operate within the approved limit. When the firm cannot yet demonstrate compliance, the launch decision records the gap, interim control, deadline and accountable executive.

3. Map the legal and regulatory perimeter

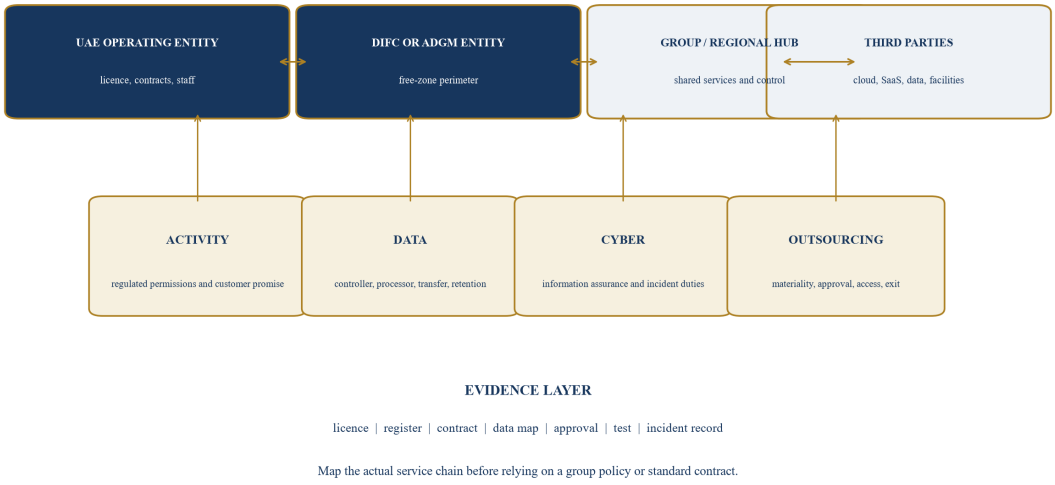
UAE entrants need an entity-and-activity map before they interpret resilience obligations. The federal personal-data framework, national cybersecurity and information-assurance materials, emirate-level requirements, free-zone data-protection regimes and sector rules can overlap through legal entity, establishment, customer, system, information and regulated activity. A group policy offers a useful baseline. It does not establish that every local requirement has been met.

The UAE Personal Data Protection Law establishes obligations that include security, breach handling, data-protection impact assessment in specified circumstances and conditions for cross-border transfers. DIFC and ADGM maintain separate data-protection regimes for organisations within their jurisdictions. Financial services can add supervisory expectations. The Central Bank of the UAE has in-force rules covering operational risk and bank outsourcing. DFSA supervision includes operational and technology risk. ADGM's Financial Services Regulatory Authority has published business-plan and cyber materials that emphasise operational resilience and technology risk.

The perimeter map should identify the responsible legal entity for each critical service, the customer-facing contracting entity, all establishments involved, regulated permissions, controllers and processors, material outsourced functions, relevant data categories, processing purposes, hosting and backup locations, transfer mechanisms, customer jurisdictions and notification routes. The map also identifies where a parent or regional hub performs material activities for the UAE entity. Intra-group delivery remains a dependency and should receive defined service, control, access, continuity and exit arrangements.

Qualified advisers should validate the map. Management then converts the advice into operating evidence: licences, registrations, policies, data-processing records, impact assessments, regulator notifications or approvals, contractual schedules, incident criteria and accountable owners. A legal conclusion without implementation evidence cannot sustain a response during an outage, audit or transaction review.

Figure 2. Entity, service and regulatory-perimeter map



The diagram is a planning model. Actual applicability depends on the entity, activity, customers, data and supervisory position.

4. Map dependencies end to end

Dependency mapping connects the service to the resources required to deliver it. A useful map begins with the customer outcome and follows every material step through channels, authentication, workflow, decision engines, data stores, interfaces, staff, facilities, utilities, telecommunications, security services, settlement agents and external providers. It identifies upstream inputs and downstream obligations. It also records manual workarounds and the capacity limits of those workarounds.

The map should reach beyond the contracted provider. A software company may host on a hyperscale cloud platform, use a separate identity service, depend on a managed-security provider, route messages through a telecommunications carrier and retain backups through another supplier. A building can have two power feeds that share a substation. Two applications can use different vendors whose critical code component or data source is common. A regional support model can appear geographically diverse while the same small team holds privileged

access for all locations.

Management should annotate each dependency with owner, location, legal entity, provider, subcontractors, data handled, authentication method, capacity, recovery objective, tested alternative, monitoring source, contractual right and evidence date. Unknown fields are visible. A dependency without a credible alternative is marked as a single point of failure. A nominal alternative that shares the same failure mode is treated as common-cause exposure.

The map becomes a living control when it connects to change management. New products, acquisitions, migrations, vendor substitutions and architecture changes can alter critical-service dependencies. A formal impact review should update the map, control requirements and scenarios before the change reaches production. This prevents the resilience record from becoming a launch artefact that no longer reflects the service.

Dependency workshops should include the staff who execute the process, not only architecture and control teams. Operators often know which spreadsheet bridges an interface, which individual resolves a failed batch, which vendor ticket queue controls recovery or which physical access card is required during an emergency. These details can determine whether a workaround is executable. The workshop output should be reconciled with system inventories, contracts, invoices, access logs and service records so that experience and evidence reinforce each other.

5. Classify vendors by criticality and substitutability

Vendor tiering determines how much diligence, contracting, oversight, testing and exit planning an arrangement requires. Spend is a poor proxy. A low-cost identity service, market-data feed, domain registrar, specialised maintenance provider or messaging gateway can stop a high-value service. Criticality should reflect the service outcome and the difficulty of replacement.

The classification begins with function. Would failure prevent or materially impair a critical service, breach a legal or customer obligation, expose sensitive data, compromise safety, disrupt financial reporting or remove a key control? It then considers substitutability: the number of credible alternatives, time to migrate, data and configuration portability, technical integration, customer or regulatory consent, skills, capacity and exit assistance. Concentration, location, subcontracting and financial condition refine the result.

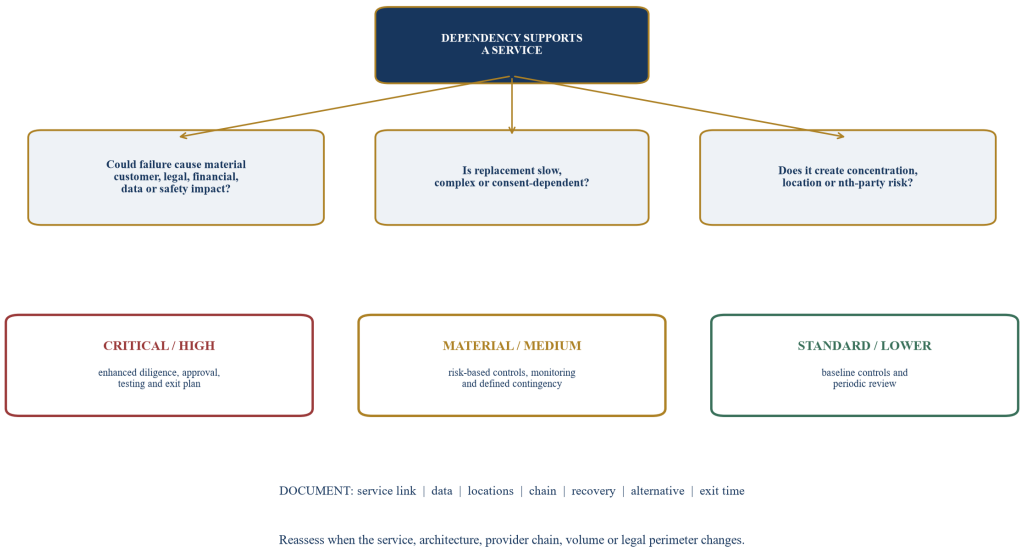
The firm should apply the same logic to outsourcing, purchased technology, professional services, data, facilities, utilities and intragroup arrangements. Legal definitions still matter, especially in regulated sectors, yet operational oversight benefits from one comprehensive dependency register. The register can distinguish regulatory categories while preserving a complete view of service exposure.

Tiering has consequences. A critical or high-impact provider receives enhanced diligence, board or committee approval where required, contract-control schedules, continuous performance and risk monitoring, incident integration, resilience testing, subcontractor visibility, concentration review and a maintained exit plan. Lower-tier providers receive proportionate controls. Exceptions are dated, approved and linked to a remediation or acceptance decision.

Classification should be completed before the request for proposal or contract renewal. Early classification allows requirements to enter the selection criteria and price comparison. A low headline price can be misleading when another bidder includes audit support, export capability,

independent recovery, local capacity and transition assistance. A total-control-cost view compares implementation, assurance, contingency and exit as well as subscription or service fees.

Figure 3. Vendor criticality and substitutability decision tree



The tree supports risk-based triage. Applicable legal definitions and supervisory requirements still govern formal classification.

6. Perform diligence on the provider and its chain

Due diligence should answer whether the provider can support the service under normal conditions, stress and exit. Corporate evidence covers legal identity, ownership, financial capacity, insurance, litigation and geographic presence. Operational evidence covers service architecture, staffing, capacity, change management, support, incident history and continuity. Security evidence covers governance, control design, vulnerability management, identity, logging, secure development, independent assurance and breach response. Data evidence covers roles, purposes, locations, subprocessors, retention, deletion, transfers and access.

Evidence quality matters. A current independent assurance report can support a conclusion within its scope and period; it does not prove every customer-specific control. A certification can establish that a management system was assessed; it does not demonstrate that a particular service will meet a particular recovery objective. A vendor questionnaire is a representation. Management should reconcile representations with contracts, reports, test results, architecture, demonstrations and references where the exposure warrants it.

Nth-party diligence is essential for concentrated technology chains. The entrant needs a current list of material subcontractors and hosting locations, notice of material changes, visibility into which controls are delegated, and a route to assess whether subcontracting changes the risk. The contract should prevent an opaque chain from expanding without review. Where direct audit is impractical, the firm can combine independent reports, pooled audits, regulator access, targeted evidence and contractual escalation.

The diligence conclusion should be specific. It identifies accepted controls, gaps, compensating measures, residual risks, conditions precedent, contractual requirements, testing commitments and

an exit-time estimate. A provider is approved for a defined service, data set, architecture and term. Material changes trigger reassessment. This approach prevents a broad corporate approval from being reused for an arrangement with a different risk profile.

Financial diligence deserves equal weight for providers that hold customer data, operate specialised infrastructure or require a long migration. The entrant should understand revenue concentration, liquidity, insurance, parent support, ownership change and the practical consequences of distress. A stressed-provider playbook can establish early-warning indicators, escalation contacts, data-extraction cadence, contingency capacity and decision thresholds. These controls reduce the chance that commercial deterioration becomes an urgent and disorderly technology exit.

Table 2. Critical-provider diligence and control register

Domain	Evidence sought	Decision test	Contract or control response	Ongoing evidence
corporate viability	ownership, accounts, insurance, litigation and jurisdiction	can the provider sustain the obligation and a stressed exit?	financial-information rights, insurance and termination triggers	annual review and event monitoring
service delivery	architecture, capacity, staffing, support and incident record	can the service meet volume, availability and recovery needs?	service levels, capacity duties, incident process and remedies	performance dashboard and service reviews
security	control framework, assurance, testing, vulnerabilities and privileged access	do controls address the actual data and threat model?	security schedule, access, notification and remediation	reports, findings and closure evidence
data	roles, purposes, categories, locations, subprocessors, retention and deletion	is processing lawful, controlled and portable?	processing schedule, transfer terms, deletion and return	data map and subprocessor notices
continuity	business-impact analysis, recovery design, exercises and dependencies	can the provider support the entrant's service tolerance?	recovery objective, test participation and evidence rights	test results and action closure
concentration	common platforms, locations, customers and subcontractors	can one event impair several critical services?	diversification, capacity reservation and contingency	portfolio concentration review
exit	data export, configuration, knowledge, transition support and timing	can service be transferred before harm becomes unacceptable?	exit plan, assistance, fees, escrow and survival terms	annual exit exercise or validation

Evidence should be current, scoped to the contracted service and retained with the approval record.

7. Translate resilience into contractual rights

A resilient design needs enforceable rights. The contract defines scope, service levels, performance data, incident notification, access, assurance, security, data processing, continuity, subcontracting, change, audit, regulatory cooperation, termination, exit assistance, liability and survival. These provisions work as a system. A termination right without data portability or transition support can be commercially unusable. An audit right without timely access to relevant evidence can arrive after the risk decision. A recovery commitment without participation in end-to-end testing can remain unproven.

Requirements should be written from the service tolerance backwards. If a critical customer process must recover within an approved period, the provider's technical and operational commitments need sufficient headroom for detection, escalation, decision, restoration, validation, reconciliation and backlog clearance. A supplier recovery target equal to the customer tolerance leaves no time for the entrant's own work. Dependencies with tighter recovery needs should have aligned objectives and evidence.

Incident clauses should define materiality, notification timing, content, communication channels, cooperation, evidence preservation, root-cause analysis and remediation. The firm should avoid relying on a final confirmed breach classification before receiving enough information to meet its own obligations. Data clauses should address controller and processor roles, instructions, purpose, locations, transfers, access, segregation, retention, return and deletion. Subcontracting clauses should provide information and control proportionate to criticality.

Commercial terms must support the control design. Pricing should identify transition, portability, testing, additional capacity and exit costs. Liability and insurance should be evaluated against plausible exposure. Service credits can create accountability but rarely fund the full loss. Step-in, suspension or termination rights require a practical operating plan. Legal review should connect the wording to actual architecture and response procedures rather than assess clauses in isolation.

Contract governance continues after signature. The obligations register should translate negotiated clauses into tasks, owners, dates and evidence. Provider reviews then cover both service performance and control delivery: assurance reports, test participation, incident actions, subprocessor changes, capacity, recovery evidence and exit materials. A waiver or missed deliverable receives the same risk treatment as a technical finding because an unexercised right can decay into a non-usable dependency.

8. Govern subcontractors and common dependencies

Third-party risk extends through the service chain. A prime provider can rely on cloud infrastructure, identity, open-source components, data suppliers, call centres, security operations, telecommunications and specialist contractors. The entrant needs enough transparency to identify which dependencies can affect critical services and whether several providers share them.

Subcontractor governance begins with an accurate schedule covering service, entity, location, data, criticality and change process. Material additions or relocations should trigger advance notice and assessment. Where consent is required, the process should define the criteria and consequences of refusal. The prime provider remains accountable for the contracted service. The entrant retains the ability to obtain relevant assurance and support its regulator or auditor.

Common-dependency analysis should work across the portfolio. Different vendors can share one cloud region, identity platform, software library, telecommunications route or managed-service team. Procurement data alone may hide this. Architecture and service maps reveal the convergence. The board dashboard should show critical services dependent on each major platform, location and supplier group, together with capacity, alternatives and tested workarounds.

The response can include diversification, architectural isolation, multi-region design, data portability, independent backups, capacity reservations, alternative communications, manual processes, escrow, internal skill retention and staged migration. Diversification should reduce a verified failure mode. Two suppliers that share the same infrastructure or geography do not create effective resilience against that common cause.

9. Design data control around purpose and jurisdiction

Data architecture is a resilience architecture. The organisation must know what information supports each critical service, why it is processed, who controls it, who can access it, where it is stored and backed up, how it moves, how long it is retained, and how it can be restored, reconciled, returned or deleted. Availability without integrity can be dangerous. A recovered database that omits committed transactions or contains duplicate instructions can increase customer harm.

The data-flow register should follow the lifecycle from collection and creation through use, transformation, sharing, storage, backup, archive and disposal. It records personal, confidential, financial, operational and regulated data separately; identifies controller, processor and subprocessor roles; and maps legal entities and jurisdictions. Interfaces, exports, logs, model inputs, support access and test environments belong in scope. Hidden operational copies often sit outside the primary application inventory.

Resilience controls include classification, least privilege, strong authentication, encryption, segregation, immutable or protected backups, restoration tests, reconciliation, lineage, retention, deletion and monitoring. Recovery procedures should specify the authoritative system of record, recovery point, transaction replay, duplicate detection, manual adjustments and approval. The service owner decides when restored data is sufficiently complete and accurate to resume customer activity.

Cross-border design requires legal validation and operating evidence. UAE federal law, DIFC rules, ADGM rules and sector requirements can differ in scope and mechanism. The firm should retain the transfer assessment or applicable mechanism, vendor commitments, data locations, access controls and change notices. A provider's generic global data statement cannot substitute for a service-specific map.

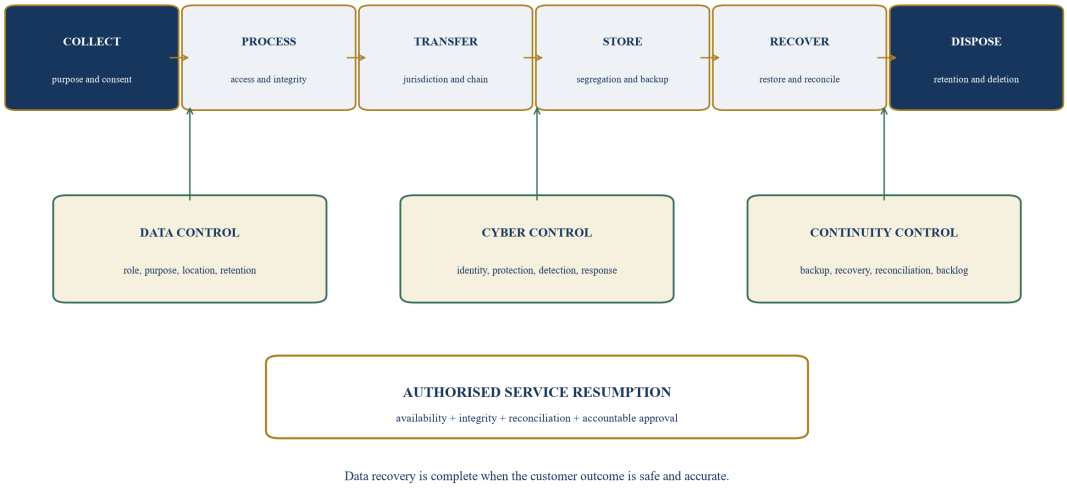
Data minimisation can improve resilience as well as privacy. Fewer unnecessary copies reduce the attack surface, reconciliation burden and deletion complexity. Clear systems of record reduce ambiguity during recovery. Separating critical operational data from analytical or convenience copies helps teams prioritise restoration. The architecture decision should still account for evidential, regulatory and business-retention duties, so deletion and consolidation follow an approved schedule rather than an outage-driven improvisation.

Table 3. Data-flow and jurisdiction register

Data set	Service and purpose	Controller / processor chain	Primary and backup locations	Recovery and integrity control	Transfer / retention evidence
customer identity	onboarding, authentication and service access	operating entity, identity provider and support processor	approved production region and protected backup	restore test, identity reconciliation and access review	processing record, transfer basis and deletion schedule
transaction record	instruction, execution, settlement and reporting	operating entity, platform and settlement parties	system of record, replica and archive	point-in-time recovery, replay controls and balance reconciliation	contract, retention rule and legal hold
security telemetry	detection, investigation and response	operating entity and security providers	monitoring platform and evidence store	log continuity, clock integrity and protected retention	access register and incident protocol
employee data	workforce administration and privileged access	employing entity and HR / identity providers	HR platform and regional backup	account recovery, joiner-mover-leaver reconciliation	employee notice and retention schedule
business records	contracts, approvals, invoices and control evidence	contracting entity and document providers	controlled repository and archive	versioning, backup test and authorised restoration	records schedule and legal hold

The register links privacy, security and recovery evidence. Entries should reflect actual architecture and validated legal treatment.

Figure 4. Data, cyber and continuity control bridge



Controls are designed around a service and its information lifecycle. Recovery includes integrity, reconciliation and authorised resumption.

10. Build cyber controls around service outcomes

Cybersecurity and operational resilience share a service lens. Security controls reduce the probability and impact of compromise. Resilience assumes that prevention can fail and prepares the organisation to sustain or recover the outcome. A mature design connects governance, asset knowledge, protective controls, detection, response and recovery to the critical-service map.

The UAE Information Assurance Regulation provides a national control reference, while the National Cybersecurity Strategy approved by the Cabinet in February 2025 describes governance, protection, innovation, capability building and partnership as pillars. Sector and free-zone expectations can add requirements. International references such as NIST Cybersecurity Framework 2.0 and NIST supply-chain guidance help structure governance and evidence. The applicable control set should be validated for the entrant's legal and regulatory perimeter.

Architecture should minimise blast radius. Segmentation, least privilege, privileged-access controls, secure configuration, strong authentication, protected administration, vulnerability management, endpoint detection, resilient logging and tested backups limit propagation and improve response. Identity and recovery systems deserve particular attention because an attacker who controls administrators or backup credentials can impair both production and recovery.

Response procedures should link security events to service impact. The incident team needs the authority to isolate systems, suspend channels, switch providers, activate workarounds, communicate with customers and notify authorities. It also needs current contact routes that do not depend on the affected platform. Exercises should test decisions under uncertainty, including incomplete attribution, disputed vendor responsibility, concurrent misinformation and pressure to restore before integrity is established.

Cyber metrics should support action. Patch counts and alerts have value, yet the board also needs to know whether critical-service assets are known, high-risk findings are closed, privileged access is controlled, backups are isolated and restored, vendors participate in tests, detection covers the service chain, and incident decisions can be made within the available time. These measures connect security investment to customer and enterprise outcomes.

Secure recovery should be designed as a separate operating capability. Clean credentials, protected administrative workstations, trusted software and configuration sources, isolated backups and forensic evidence can all be needed when the production environment is suspect. The recovery team should know how to re-establish a trusted control plane before reconnecting services. Tests should verify that recovery materials remain accessible when normal identity, messaging and documentation platforms are unavailable.

11. Set impact tolerances and recovery objectives

Impact tolerance, recovery time objective and recovery point objective answer different questions. The impact tolerance defines how much disruption to the service is acceptable before intolerable harm occurs. The recovery time objective sets the target time to restore a resource or capability. The recovery point objective defines the acceptable data loss measured in time or another meaningful unit. A complete design also defines minimum service level, data-integrity conditions, backlog capacity and the authority to resume.

Objectives should form a dependency budget. If a service tolerance is four hours, management cannot allocate four hours to every supporting system. Detection, escalation, decision, provider recovery, internal restoration, validation, reconciliation, communication and backlog processing all consume time. Critical dependencies need objectives that leave sufficient margin for the end-to-end sequence and for uncertainty.

The board should review objective feasibility. Evidence can include architecture analysis, supplier commitments, restoration tests, processing capacity, staff availability, alternate-site readiness and scenario exercises. A contractual target without test evidence remains an assumption. A successful infrastructure recovery without application validation or customer reconciliation does not demonstrate service recovery.

Tolerances should be reviewed when the service changes. Volume growth can exhaust a manual workaround. A new customer segment can increase harm. A new jurisdiction can add a reporting deadline. An acquisition can create a shared dependency. Management should report both the approved limit and the most recent evidence of operating within it.

Table 4. Service tolerance and recovery objective register

Service	Maximum tolerable disruption	Minimum service / integrity condition	Key dependency objectives	Backlog clearance	Evidence and owner
customer access	approved duration plus customer-count threshold	authenticated access to accurate priority information	identity, channel and data objectives within service budget	capacity tested for deferred requests	end-to-end exercise; service owner
transaction processing	approved duration, value and volume limits	authorised instructions preserved with no duplicate execution	workflow, ledger, interface and settlement objectives	reconciliation and replay tested	recovery test; operations owner
regulatory reporting	statutory or supervisory deadline	complete, traceable and approved submission	source data, calculation and document objectives	exception workflow validated	reporting exercise; finance owner
customer support	approved degraded-service window	priority cases triaged through alternate channel	telephony, case data and staff access objectives	surge roster and queue model	communications exercise; support owner
critical facility operation	safety and service-specific threshold	safe state and essential output maintained	power, cooling, controls and specialist support objectives	restart and inspection sequence	integrated site test; facility owner

Values shown are illustrative management fields. Each firm should approve values supported by legal analysis, customer obligations, architecture and testing.

12. Integrate continuity, disaster recovery and crisis management

Business continuity, disaster recovery, cyber response, emergency management and crisis communication often sit in separate documents. A severe event crosses these boundaries. The integrated operating model should specify who declares an incident, who owns the service, who controls technical recovery, who protects people, who assesses legal and regulatory duties, who communicates, who authorises spending and who decides that the service can resume.

The plan should use common severity levels and decision records. A disruption enters through monitoring, staff, customer, vendor or authority notification. Triage identifies affected services, data, customers and jurisdictions. The incident leader sets priorities and activates specialist workstreams. Every material decision records the evidence available, risk accepted, owner and time. This log supports handover, notification, recovery, investigation and lessons learned.

Alternative communication is a core dependency. Contact lists, conferencing, collaboration tools, status pages and customer messages can all depend on the affected identity or network

environment. The firm should maintain an authorised out-of-band route and periodically test access. Vendor escalation contacts should include operational and executive levels, with an alternate path when the usual portal is unavailable.

Recovery requires more than restoration. Technical teams restore systems and data. Operations reconcile transactions and exceptions. Security validates containment and access. The service owner confirms that minimum service and integrity conditions have been met. Legal and communications teams manage notifications and stakeholder information. Finance tracks cost, liquidity, claims and customer remediation. The crisis closes only after backlog, residual risk and corrective actions are governed.

People resilience should be explicit. Named deputies, decision limits, access rights, fatigue management, transport, remote-work capability and specialist succession determine whether the plan can operate for more than a few hours. The entrant should avoid concentrating critical knowledge in one founder, expatriate executive, vendor engineer or parent-company team. Runbooks, cross-training and observed exercises provide evidence that authority and knowledge can transfer under stress.

13. Test severe but plausible scenarios

Testing converts design claims into evidence. The programme should combine walkthroughs, technical restoration, component failover, vendor exercises, crisis simulations and end-to-end service tests. Each method answers a different question. A tabletop can reveal authority and communication gaps. A restoration test can prove backup usability. A live failover can demonstrate architecture. An end-to-end exercise can show whether the customer outcome stays within tolerance.

Scenarios should target the firm's actual dependencies and threat model. Useful examples include cloud-region unavailability, identity-provider compromise, ransomware affecting production and backups, data corruption discovered after processing, telecommunications failure, facility loss, utility disruption, vendor insolvency, critical-subcontractor failure, insider misuse, simultaneous cyber and misinformation events, or a failed migration during peak demand. The test design states what is simulated, what remains live, safety constraints and success criteria.

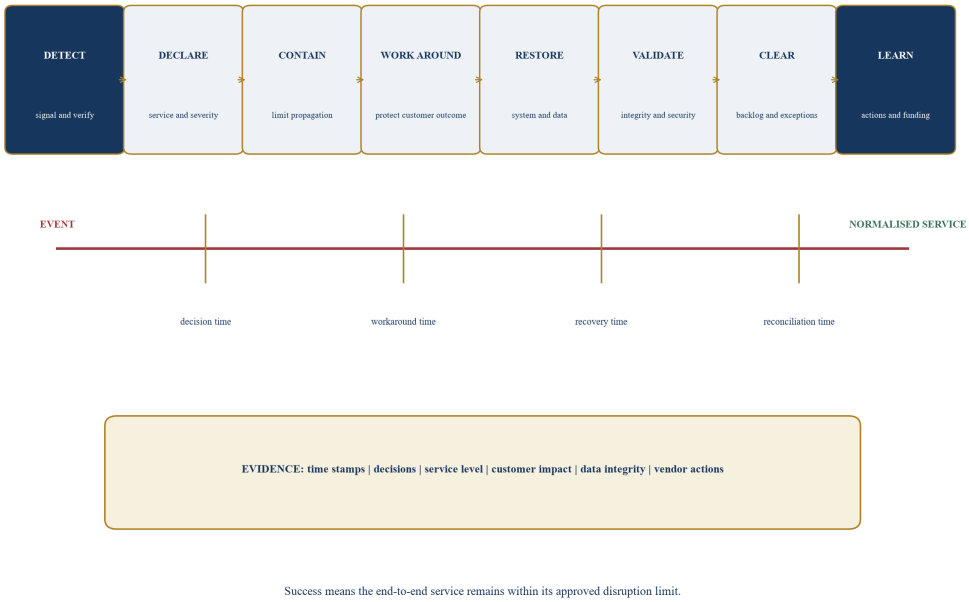
The exercise clock should follow the service. It measures detection, classification, escalation, decision, containment, workaround, restoration, validation, communication, backlog clearance and return to normal. Observers record evidence. The team should distinguish a plan action from an action actually performed. If a vendor promises to respond during the exercise, its response and timing form part of the result.

Findings should be prioritised by service harm and control dependency. Each action receives an owner, funding, deadline, interim control and validation method. Repeated findings escalate. The board sees whether the organisation remained within tolerance, where time was consumed, which assumptions failed and whether remediation changed the residual risk.

Testing should also cover the return to normal. Temporary workarounds can create control debt, duplicate records, manual approvals, privileged access and deferred customer actions. The exercise should specify how temporary changes are retired, data is reconciled, access is removed, customers are remediated and monitoring returns to normal. This stage often determines the true

duration and cost of disruption even after the headline service appears available.

Figure 5. Severe-but-plausible scenario test and evidence clock



The exercise measures the complete service response, including reconciliation and backlog, rather than technology restoration alone.

Table 5. Scenario-test matrix

Scenario	Services and dependencies tested	Key decisions	Success evidence	Escalation trigger
identity compromise	customer access, staff access, privileged administration and recovery accounts	isolate, revoke, establish trusted access and communicate	authenticated priority service restored; privileged paths validated	trusted administration cannot be established within budget
data corruption	transactions, records, backups, interfaces and reports	stop processing, select recovery point, replay and reconcile	complete and accurate records; duplicate and omission checks pass	authoritative data set cannot be identified
critical vendor outage	service, provider chain, alternate provider and manual process	invoke escalation, workaround, failover or exit	minimum service sustained and backlog cleared	provider response or alternative breaches tolerance
facility and utility loss	people, power, cooling, network, access and site safety	move, reduce service, use alternate site and prioritise load	safe state maintained; priority service resumes	shared utility or access blocks both sites
ransomware and misinformation	technology, security, communications, legal and customer support	contain, preserve evidence, validate messages and restore	clean recovery and consistent authorised communication	pressure to resume exceeds integrity evidence

Management selects scenarios from the actual dependency map and records measured outcomes. Results shown should never be replaced by planned actions.

14. Build usable exit and portability options

Exit planning begins at procurement. The firm should know what data, configuration, code, documentation, credentials, interfaces, records and specialist knowledge are needed to transfer or insource the service. It should estimate the time, cost, capacity, consent and risk involved. The contract then secures the rights and assistance necessary to execute that plan.

An exit plan should cover triggers, decision authority, target options, transition governance, data export, format and validation, parallel operation, customer and regulator communication, staff and knowledge transfer, security, deletion, final reconciliation and residual obligations. It also addresses a stressed exit when the provider is uncooperative, insolvent or disrupted. A normal commercial migration plan alone is insufficient for that case.

Portability should be tested proportionately. The firm can request and validate sample exports, restore independent backups, recreate configurations, exercise alternate connectivity, document runbooks, rotate staff through critical tasks, or conduct a limited transition. Escrow can help in defined software arrangements, but its value depends on current materials, rights, build capability and regular verification.

Exit economics belong in the entry case and the valuation. Concentrated proprietary architecture may reduce initial cost while increasing switching cost and strategic exposure. Management should model transition expenditure, dual running, contract termination, remediation, customer support and working capital. A board can then decide whether the economics justify the dependency or whether architectural choices should preserve more optionality.

The plan should identify the latest safe decision date. A firm that waits until contract expiry, provider distress or regulatory intervention may lack enough time to migrate within tolerance. The safe date is derived from procurement, build, data transfer, testing, consent, parallel operation and termination lead times. Monitoring can then escalate when declining service, pricing change, control weakness or financial distress consumes the remaining option window.

15. Manage concentration and geographic risk

Concentration exists when one event can impair several critical services, entities or customers. It can arise from a provider, platform, region, data centre, utility, network route, software component, security tool, specialist team or physical corridor. Geographic diversity helps only when the locations do not share the relevant failure mode.

Portfolio analysis should aggregate dependencies by legal provider group, cloud service and region, data location, subcontractor, technology component, telecommunications route, facility, utility and privileged-support team. It should also consider customer concentration: a disruption during a major customer's critical period can create disproportionate commercial and reputational harm. The analysis links each concentration to affected services, tolerances, alternatives and tested response.

Management can reduce exposure through segmentation, multiple zones or regions, independent backup, portable data, alternate carriers, internal capability, provider diversity, capacity reservations and contractual priority. The response should be proportionate to harm and cost. Full duplication can be uneconomic, while a tested degraded mode can provide sufficient protection for some services. Safety, regulatory and customer obligations set the boundary.

The board should see changes over time. Rapid growth, acquisitions and vendor consolidation can increase concentration after approval. A provider can acquire a subcontractor or move workloads. A new product can reuse a platform across several services. Change notices and periodic mapping should therefore feed a concentration dashboard rather than remain in individual contract files.

Scenario economics can help prioritise mitigation. Management estimates the services affected, plausible duration, customer remediation, contractual exposure, lost contribution, recovery expense and strategic delay under defined assumptions. The estimate is a planning tool rather than a prediction. Comparing it with the cost and effectiveness of mitigation allows the board to allocate capital to the dependencies that dominate enterprise harm.

16. Connect resilience to M&A, financing and valuation

Operational resilience affects transaction quality because it shapes earnings durability, implementation cost, liabilities and strategic optionality. A buyer may discover that revenue depends on one unassignable vendor contract, sensitive data sits in an unknown jurisdiction, the platform lacks tested recovery, key administrators are employed by a seller affiliate, or a carve-out requires services that cannot be separated within the deal timetable. These findings can change price, structure, conditions, indemnities, transition services and the integration plan.

Due diligence should map critical services and dependencies alongside financial and commercial work. The team reviews provider concentration, assignment and change-of-control clauses, material incidents, regulator correspondence, data-processing records, assurance reports, recovery tests, continuity findings, cyber exposures, exit plans, technical debt, insurance and remediation budgets. Claims are reconciled with evidence. A policy document is not treated as proof that a service has been tested.

The value bridge can include recurring resilience expenditure, one-off remediation, duplicated infrastructure, transition services, vendor termination costs, consent risk, integration delay, customer remediation, expected downtime exposure and contingency funding. The model should identify management assumptions and sensitivities. Legal and technical findings influence the scenario; they do not become precise valuation deductions without an approved financial method.

Financing documents can also depend on resilience. Lenders and investors may examine information security, continuity, material contracts, data, litigation, regulatory compliance and insurance. A credible evidence pack can shorten diligence and support covenant negotiation. A weak pack can increase conditions precedent, reserves, representations or execution uncertainty. Management should treat resilience records as part of transaction readiness.

Integration planning should protect the target's working recovery capability while the future architecture is being built. Premature consolidation of identity, networks, providers or support teams can create new common points of failure. The integration plan should state the resilience condition for each cutover, the rollback route, the evidence required to decommission the former environment and the service owner authorised to proceed. Transitional-service agreements should contain continuity, access and exit provisions aligned with the deal timetable.

17. Use international comparators carefully

International frameworks provide useful design principles. The Basel Committee's operational-resilience principles focus on the ability to deliver critical operations through disruption. Its third-party risk principles broaden attention across the lifecycle of third-party arrangements. The Financial Stability Board toolkit addresses third-party risk management and oversight. NIST Cybersecurity Framework 2.0 and its supply-chain publications support governance and control design. ISO 22301 provides a business-continuity management-system reference.

Financial-sector regimes provide detailed comparators. The United Kingdom's operational-resilience framework uses important business services, impact tolerances, mapping and testing. European Union DORA applies requirements for ICT risk management, incident reporting, testing and third-party risk to covered financial entities. APRA's CPS 230 addresses operational risk, critical operations, service providers and continuity in Australia. The Reserve Bank of India has directions covering IT outsourcing and related risk, continuity and exit.

Comparators should inform questions, not determine UAE legal conclusions. Scope, definitions, proportionality, notification, approval and enforcement differ. A non-financial entrant can still use service mapping, tolerance, testing and exit disciplines as management practices. A regulated entrant should validate the precise local obligation with the relevant authority and advisers.

The practical method is a control crosswalk. Management lists local requirements first, maps group and international controls against them, identifies gaps and documents the evidence that implements each response. This preserves the benefit of mature group standards while preventing an imported label from masking a local obligation.

18. Execute a 180-day resilience programme

The first 180 days should build a usable minimum system and then test it. Days 0 to 30 establish governance, legal perimeter, critical services and accountable owners. Days 31 to 60 map dependencies, data and critical providers. Days 61 to 90 close priority contract and architecture gaps, define tolerances and integrate incident governance. Days 91 to 120 build workarounds, recovery procedures and exit plans. Days 121 to 150 run technical and service exercises. Days 151 to 180 close critical findings and present the board with evidence, residual risk and the next investment wave.

The programme needs a decision backlog, not a document backlog. Each work item states the service, exposure, required evidence, executive owner, deadline, cost and decision. High-risk issues can include missing data locations, absent audit or exit rights, untested backups, shared privileged accounts, unsupported systems, no alternate communications, unknown subcontractors or recovery objectives that consume the entire service tolerance.

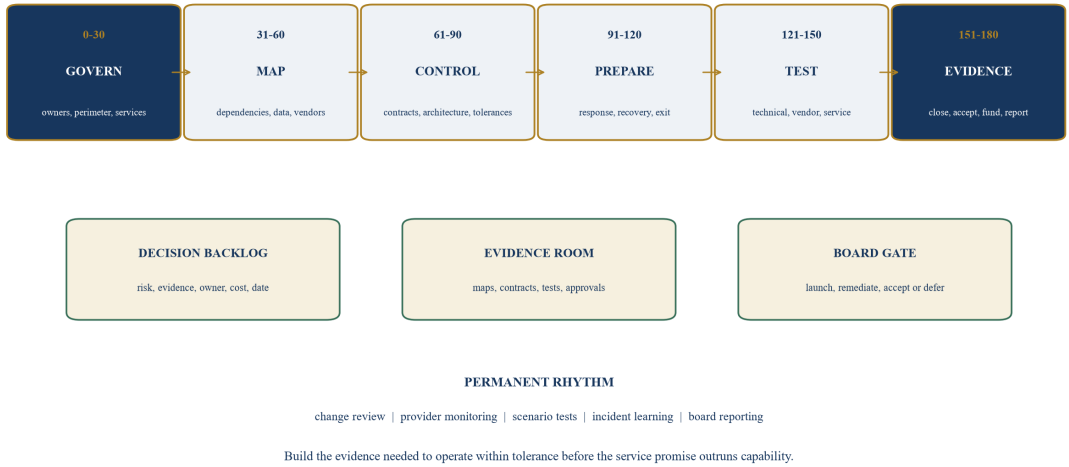
Sequencing should follow irreversibility. Entity, licence, customer promise, core architecture and strategic-provider choices are expensive to reverse, so they receive early attention. Policies and registers can follow once the operating facts are known. Testing begins as soon as a meaningful slice exists, because early exercises reveal false assumptions before launch pressure peaks.

Management should retain an evidence room containing the perimeter memo, service inventory, maps, vendor approvals, contracts, data records, risk acceptances, plans, tests, incidents,

remediation and board decisions. The room supports regulation, customers, insurance, transactions and continuous improvement. Access remains controlled according to sensitivity.

The programme office should publish a weekly critical-path view. It distinguishes items that block launch, items that constrain scale and items that form the next maturity wave. Evidence is accepted only when it is complete, current and owned. This prevents an action from closing because a document exists while the underlying contract, architecture, test or operating procedure remains incomplete.

Figure 6. The 180-day operational-resilience build



The sequence is a management planning model. Actual timing depends on licence, service criticality, architecture, contracts and unresolved risks.

19. Govern through evidence and board decisions

The operating model needs three lines of accountability. Service and business owners manage delivery, dependencies and response. Risk, compliance, privacy and security functions establish standards, challenge decisions and monitor exposure. Internal audit provides independent assurance according to its mandate. The board retains responsibility for risk appetite, critical-service tolerances, material outsourcing and residual risks where applicable.

The dashboard should show service status rather than aggregate activity alone. Useful measures include the percentage of critical services with current maps; critical providers with complete approval, contract controls and tested exits; services demonstrated within tolerance; overdue severe findings; concentration without tested alternatives; backup restoration success; privileged-access exceptions; incident decision time; customer-impact and backlog; and resilience expenditure against the approved plan.

Metrics require definitions and evidence dates. A green result based on a two-year-old test can mislead. The dashboard should show the last tested scenario, scope, result, open finding and next test. Risk acceptance should identify the exposure, affected service, interim control, expiry, accountable executive and board or committee authority. Expired acceptances escalate automatically.

Board papers should ask for decisions. Typical decisions include approving the critical-service inventory and tolerances, funding architecture or staffing, authorising a material provider, requiring contract remediation, accepting a time-bound residual risk, deferring launch, changing a customer promise, or directing an exit. Evidence allows directors to distinguish an implementation gap from a structural risk that changes the market-entry thesis.

Management committees should review emerging events between board cycles. Provider acquisitions, regional incidents, material vulnerabilities, regulatory notices, control failures, litigation and sharp volume changes can alter the exposure quickly. A defined trigger matrix routes these events to the service owner, control functions and board committee. The same matrix establishes when a new risk assessment, contract action, scenario test or customer communication is required.

Table 6. Board operational-resilience dashboard

Dimension	Board measure	Evidence date	Escalation	Decision use
service coverage	critical services with approved owner, tolerance and current map	latest approved inventory and change review	missing or stale service record	scope and accountability
tested resilience	services demonstrated within tolerance under relevant scenarios	last end-to-end test and action closure	breach of tolerance or repeated finding	funding, remediation or launch gate
provider control	critical providers with complete diligence, contract, monitoring and exit evidence	provider register and assurance period	expired evidence, material exception or unknown chain	approve, condition, renegotiate or exit
data and cyber	critical data flows mapped; recovery and privileged controls tested	architecture, access and restoration evidence	unknown location, failed restore or uncontrolled privilege	stop change, remediate or accept
concentration	services exposed to a provider, platform, location or team without tested alternative	portfolio dependency map	common-cause exposure exceeds appetite	diversify, isolate or fund contingency
incident readiness	detection, decision, communication, restoration and backlog times	exercise and incident records	response consumes service tolerance	authority, staffing and process change
remediation	severe findings, risk acceptances and overdue actions	action system and approvals	expired acceptance or missed critical deadline	escalate owner and capital allocation

Thresholds and reporting frequency are management decisions subject to applicable governance requirements. Each metric needs a defined evidence source.

20. Board conclusions and limitations

Operational resilience gives the board a disciplined answer to a simple question: can the new entrant continue delivering its most important outcomes when a material dependency fails? The answer is built from service definitions, perimeter analysis, dependency evidence, provider controls, data architecture, cyber readiness, continuity, testing and exit options. Every element needs an owner and a verifiable operating record.

The framework supports several board conclusions. Resilience belongs in market-entry economics and architecture before launch. Criticality follows customer and enterprise harm rather than supplier spend. Data availability, integrity and jurisdiction are inseparable. Contract rights must be executable through tested plans. Technology recovery is one step within service recovery. Concentration should be measured across the full portfolio. Scenario testing is the evidence that connects a plan to an outcome. Residual risks require explicit, time-bound decisions.

The framework also has limits. Applicable obligations depend on the entity, regulated activity, location, customers, data, contracts and supervisory position. Regulations, guidance and technology change. The paper does not evaluate a specific architecture, provider, licence, legal mechanism or incident. Management assumptions in any implementation plan require validation through qualified advice, current documents, technical evidence and tests.

A credible entrant can use the framework to create a board-ready 180-day agenda. The first deliverable is the critical-service and perimeter map. The second is a verified dependency and provider register. The third is a control, contract and exit plan. The fourth is an integrated response and recovery system. The fifth is an end-to-end test that demonstrates performance within tolerance. These outputs convert resilience from a statement of intent into a governed market-entry capability.

Implementation should finish each phase with an evidence gate. The gate confirms what has been validated, what remains an assumption, which risks have approved interim controls, and whether the service promise can proceed. This gives commercial teams a defensible basis for customer commitments and gives directors a clear record of the judgement exercised. The result is a resilience capability that supports responsible growth, transaction readiness and durable enterprise value.

References

[1] UAE Legislation, Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data https://uaelegislation.gov.ae/en/legislations/1972

[2] UAE Cabinet, National Cybersecurity Strategy and API-First Policy https://uaecabinet.ae/en/news/uae-cabinet-approves-national-cybersecurity-strategy-api-first-policy

[3] UAE Cabinet, National Cybersecurity Policies and Programmes https://uaecabinet.ae/en/news/uae-cabinet-chaired-by-mohammed-bin-rashid-approves-national-policy-for-economic-clusters-agenda-of-uae-government-s-annual-meetings

[4] UAE Official Portal, Cyber Safety and Digital Security https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

[5] UAE Official Portal, Critical Information Infrastructure Protection Policy https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/-/media/Documents-2023/Critical-Information-Infrastructure-Protection-CIIP-Policy.ashx

[6] Telecommunications and Digital Government Regulatory Authority, UAE Information Assurance Regulation https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/UAE-Information-Assurance-Regulation-v1-1-pdf.ashx

[7] Central Bank of the UAE Rulebook, Operational Risk Regulation https://rulebook.centralbank.ae/en/rulebook/operational-risk-regulation

[8] Central Bank of the UAE, Operational Risk Standards https://www.centralbank.ae/en/rulebook/banking/risk-management/operational-risk/operational-risk-standards/

[9] Central Bank of the UAE Rulebook, Operational Risk Standards PDF https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_2355_VER1.pdf

[10] Central Bank of the UAE Rulebook, Disaster Recovery and Business Continuity Management https://rulebook.centralbank.ae/en/rulebook/article-7-disaster-recovery-and-business-continuity-management

[11] Central Bank of the UAE Rulebook, Operational Risk Reporting Requirements and Disclosure https://rulebook.centralbank.ae/en/rulebook/article-10-reporting-requirements-and-disclosure-0

[12] Central Bank of the UAE Rulebook, Outsourcing Regulation for Banks https://rulebook.centralbank.ae/en/rulebook/outsourcing-regulation-banks

[13] Central Bank of the UAE Rulebook, Outsourcing Regulation for Banks PDF https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_2327_VER1.pdf

[14] Central Bank of the UAE Rulebook, Policies and Procedures for Material Outsourcing https://rulebook.centralbank.ae/en/rulebook/22-policies-and-procedures-assessment-and-approval-outsourcing-material-business

[15] Central Bank of the UAE Rulebook, Outsourcing and Bank Data https://rulebook.centralbank.ae/en/rulebook/article-20-outsourcing

[16] Central Bank of the UAE Rulebook, Outsourcing and Service Continuity https://rulebook.centralbank.ae/en/rulebook/article-16-outsourcing

[17] Dubai International Financial Centre, Data Protection Law No. 5 of 2020 https://www.difc.com/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020

[18] Dubai International Financial Centre, Commissioner of Data Protection https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection

[19] Abu Dhabi Global Market, Office of Data Protection Guidance https://www.adgm.com/operating-in-adgm/office-of-data-protection/guidance

[20] Abu Dhabi Global Market, Data Protection Regulations 2021 Rules https://www.adgm.com/media/announcements/adgm-makes-rules-under-new-data-protection-regulations-2021

[21] Dubai Financial Services Authority, Operational and Technology Risk Supervision https://www.dfsa.ae/what-we-do/supervision/operational-technology-risk-supervision/summary

[22] Dubai Financial Services Authority, Operational and Technology Risk Supervisory Methodology https://www.dfsa.ae/what-we-do/supervision/operational-technology-risk-supervision/supervisory-methodology

[23] Abu Dhabi Global Market Financial Services Regulatory Authority, Business Plan 2025 to 2026 https://assets.adgm.com/download/assets/FSRA%2BBusiness%2BPlan%2B2025%2B-%2B2026.pdf/60b2624c1e7e11f093d71a0ac1bcf369

[24] Abu Dhabi Global Market, Cybercrime Prevention https://www.adgm.com/operating-in-adgm/financial-and-cyber-crime-prevention/cybercrime-prevention

[25] Abu Dhabi Global Market, Cyber Threats Relevant to Virtual Asset Service Providers https://assets.adgm.com/download/assets/FCCP%2BNotice%2BNo.76%2Bof%2B2026%2B-%2BCyber%2BThreats%2BRelevant%2Bto%2BVirtual%2BAsset%2BService%2BProviders.pdf/f645f89e447711f1a008f6b405c9aabb

[26] Basel Committee on Banking Supervision, Principles for Operational Resilience https://www.bis.org/bcbs/publ/d516.pdf

[27] Basel Committee on Banking Supervision, Operational Resilience Principles https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/20.htm

[28] Basel Committee on Banking Supervision, Principles for the Sound Management of Third-Party Risk https://www.bis.org/bcbs/publ/d605.htm

[29] Basel Committee on Banking Supervision, Third-Party Risk Principles https://www.bis.org/basel_consolidated_guidelines/chapter/ORR/30.htm

[30] Financial Stability Board, Enhancing Third-Party Risk Management and Oversight Toolkit https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/

[31] Financial Stability Board, Third-Party Risk Toolkit PDF https://www.fsb.org/wp-content/uploads/P041223-1.pdf

[32] National Institute of Standards and Technology, Cybersecurity Framework 2.0 https://www.nist.gov/document/nist-csf-20-core-withdrawn-csf-11-elements

[33] National Institute of Standards and Technology, Cybersecurity Framework 2.0 PDF https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

[34] National Institute of Standards and Technology, Cybersecurity Supply Chain Risk Management SP 800-161 Rev. 1 https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

[35] National Institute of Standards and Technology, Supply Chain Due Diligence Quick-Start Guide SP 1326 https://csrc.nist.gov/pubs/sp/1326/final

[36] International Organization for Standardization, ISO 22301 Business Continuity Management Systems https://www.iso.org/standard/75106.html

[37] International Organization for Standardization, ISO IEC 27001 Information Security Management Systems https://www.iso.org/standard/27001

[38] European Union, Digital Operational Resilience Regulation 2022/2554 https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[39] European Commission, DORA Implementing and Delegated Acts https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

[40] European Banking Authority, Guidelines on Outsourcing Arrangements https://eba.europa.eu/guidelines-outsourcing

[41] European Banking Authority, Revised Guidelines on Outsourcing Arrangements https://eba.europa.eu/publications-and-media/press-releases/eba-publishes-revised-guidelines-outsourcing-arrangements

[42] Financial Conduct Authority, Operational Resilience https://www.fca.org.uk/firms/operational-resilience

[43] Financial Conduct Authority, Operational Resilience Insights One Year After the Transition Period https://www.fca.org.uk/publications/good-and-poor-practice/operational-resilience-insights-observations-one-year

[44] Financial Conduct Authority, Operational Resilience Insights and Observations https://www.fca.org.uk/firms/operational-resilience/insights-observations

[45] Financial Conduct Authority Handbook, SYSC 15A Operational Resilience https://handbook.fca.org.uk/handbook/SYSC/15A/2.html

[46] Bank of England Prudential Regulation Authority, Supervisory Statement SS1/21 Operational Resilience https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss

[47] Bank of England Prudential Regulation Authority, Supervisory Statement SS2/21 Outsourcing and Third Party Risk Management https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss

[48] Australian Prudential Regulation Authority, CPS 230 Operational Risk Management https://www.apra.gov.au/consultations/operational-risk-management

[49] Australian Prudential Regulation Authority, CPS 230 Comes into Force https://www.apra.gov.au/news-and-publications/apras-new-prudential-standard-operational-risk-management-comes-force

[50] Reserve Bank of India, Master Direction on Outsourcing of Information Technology Services 2023 https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12486&Mode=0&fn=14

[51] Reserve Bank of India, Master Directions Index https://systemhealth.rbi.org.in/Scripts/BS_ViewMasterDirections.aspx.html

[52] Organisation for Economic Co-operation and Development, Investment Policy Perspectives in the United Arab Emirates https://www.oecd.org/en/publications/investment-policy-perspectives-in-the-united-arab-emirates_d83cbff3-en.html

[53] UAE Federal Tax Authority, Corporate Tax Frequently Asked Questions https://tax.gov.ae/en/taxes/corporate.tax/faqs.aspx

[54] Cyber Security Council UAE, Official Website https://csc.gov.ae/en/

[55] Dubai Electronic Security Center, Dubai Cyber Security Strategy https://www.desc.gov.ae/cyber-security-strategy/

[56] UK Government, Critical Third Parties to the Finance Sector Policy Statement https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement

[57] UK Government, Memorandum of Understanding on Critical Third Parties https://www.gov.uk/government/publications/memorandum-of-understanding-between-the-bank-of-england-fca-and-pra

[58] European Union, DORA Summary and Application Date https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32022R2554

About the Author

Authored by Chennakeshav Adya, Independent Researcher

Chennakeshav Adya researches corporate finance, transactions, strategy, operating models and institutional decision systems. His work translates regulation, market evidence and implementation dependencies into practical frameworks for boards, investors and management teams.