Operational Resilience for EAMs: Mapping Critical Services, Vendors and Recovery Tolerances

An International Control Framework for External Asset Managers and Independent Wealth Firms

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

External asset managers and independent wealth firms operate through a dense chain of dependencies. Client instructions may arrive through relationship teams and digital channels. Orders pass through portfolio and order-management systems, brokers, custodian banks and market infrastructure. Valuation, performance, reporting, compliance surveillance, sanctions screening, communications and regulatory records can depend on specialist vendors, cloud platforms and group companies. A disruption in one component can become a client-service failure even when the firm itself remains open.

This paper develops an operational-resilience framework for externally managed wealth businesses. It begins with critical client services, defines measurable impact and recovery tolerances, maps people, processes, technology, facilities, information, banks, vendors and fourth parties, and converts those dependencies into scenario tests, incident decisions and board reporting. It addresses service ownership, vendor classification, contracting, concentration, cyber incidents, data recovery, manual workarounds, communications, regulatory notification, remediation and exit planning.

The framework draws on official materials from the Dubai Financial Services Authority, the United Kingdom Financial Conduct Authority, the European Union, the Monetary Authority of Singapore, the Hong Kong Securities and Futures Commission, the Australian Prudential Regulation Authority, the United States Securities and Exchange Commission and the International Organization of Securities Commissions. These regimes differ in scope and legal effect. The paper uses their materials as international design evidence and does not imply that every requirement applies to every external asset manager.

Six figures present a service map, tolerance model, vendor-dependency network, scenario-test architecture, incident timeline and board dashboard. Six tables provide a critical-service register, international comparison, dependency register, vendor-control matrix, hypothetical scenario results and implementation roadmap. All thresholds, scores, times, amounts and scenarios in worked examples are hypothetical management assumptions created solely to demonstrate the method. They are not benchmarks, forecasts or legal conclusions. Actual requirements depend on jurisdiction, licence, client classification, business model, service, contract and facts. This paper provides general information for professional audiences and does not provide legal, regulatory, technology, cyber, investment, tax or accounting advice.

JEL Classification: G23, G28, L22, L86, M15

Keywords: operational resilience, external asset managers, wealth management, critical services, impact tolerance, outsourcing, third-party risk, business continuity, cyber resilience

1. Start with the client outcome

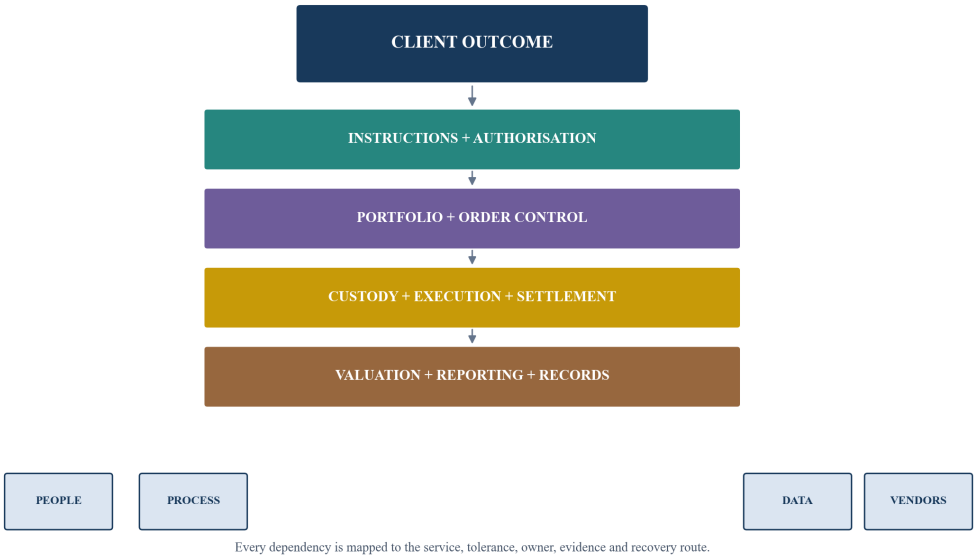
Operational resilience asks whether a firm can continue delivering an important service through disruption within a boundary that protects clients, markets and the firm. This question differs from asking whether a server is available, an office is accessible or a continuity document exists. A technical component can recover while the client remains unable to trade, receive cash, understand exposure or contact the firm.

An external asset manager should describe services in language that connects operating activity to an identifiable outcome. Examples include receiving and authenticating client instructions, executing and settling portfolio transactions, maintaining access to client cash and securities, valuing portfolios, providing accurate statements, monitoring restrictions and meeting regulatory-record obligations. A broad label such as investment management can hide several services with different dependencies and consequences.

The service definition should state the client population, delivery window, currencies, markets, channels and peak periods. It should identify what constitutes disruption and which consequences determine materiality. The owner should be accountable for the whole service even when delivery crosses relationship management, investment, trading, operations, finance, compliance, technology, custodian banks and vendors.

Service-led design creates a practical test. If a portfolio-management platform fails, the firm can ask whether instructions can still be validated, restrictions checked, orders created, approved, routed, confirmed, settled and recorded. The answer comes from the complete chain, not the platform's status page.

Figure 1. Critical-service map for an external asset manager



Author framework. A client outcome depends on linked internal capabilities, banks, vendors and market infrastructure.

Table 1. Critical-service register

Service	Client outcome	Disruption signal	Accountable owner	Core evidence
instruction handling	valid instructions are received, authenticated and actioned	channel unavailable or authentication cannot complete	client service head	channel logs, authority records, exception queue
portfolio decision and order	mandate-compliant decisions become approved orders	portfolio data or restriction control unavailable	chief investment officer	positions, mandates, approvals, restriction results
execution and settlement	orders reach markets and settle accurately	broker, custodian or matching failure	operations head	order trail, confirmations, cash and position reconciliations
cash and asset access	authorised client payments and asset movements complete	payment or custody access unavailable	chief operating officer	bank authority, callbacks, payment and custody records
valuation and reporting	clients receive supportable portfolio information	prices, positions or calculation engine unavailable	valuation owner	source prices, position files, calculation and approval logs
regulatory records	complete records remain accessible and reproducible	required data cannot be retrieved or reconstructed	compliance head	retention map, backups, access tests, regulatory extracts

The examples describe a management-control structure and do not prescribe regulatory classifications.

2. Define impact tolerance before recovery plans

An impact tolerance states the maximum tolerable disruption to an important service. It can combine time, volume, value, client harm, market effect, data loss and regulatory consequence. A service may therefore have several boundaries. An external asset manager might tolerate a short delay in producing an indicative portfolio view while accepting no unauthorised payment and very limited loss of transaction records.

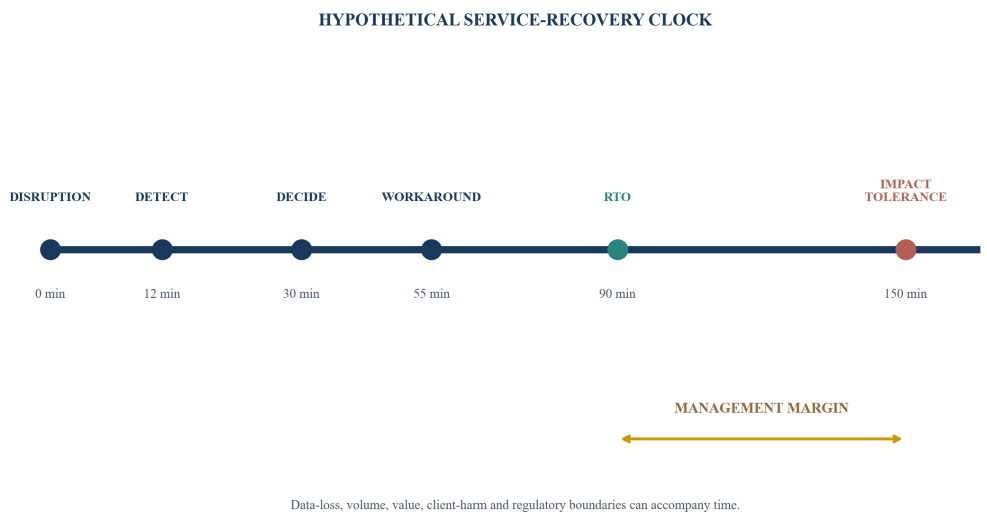
The United Kingdom FCA distinguishes an impact tolerance from a recovery-time objective. The impact tolerance marks the maximum tolerable disruption to the service. A recovery-time objective is generally an internal target set within that boundary. The gap provides time to detect failure, decide, communicate, invoke alternatives and handle uncertainty. Setting the two measures equal removes management margin.

Recovery-point objectives address the amount of data that can be lost or reconstructed. Maximum tolerable transaction backlogs, client populations, monetary exposures and control exceptions can be equally important. Each metric should have an observable data source and an escalation owner.

Tolerance should reflect harm, legal obligations, market windows, time zones and dependencies. The trading service may have a tighter boundary during volatile markets. Client reporting may have contractual or regulatory dates. Payment services can require near-zero tolerance for unauthorised release while permitting a bounded delay for non-urgent instructions.

The board should approve the method and material tolerances within the applicable governance framework. Service owners should provide the evidence supporting them. Scenario tests should demonstrate whether operating capability can remain inside them.

Figure 2. Impact tolerance and internal recovery targets



Author framework. Values are hypothetical management assumptions and demonstrate the difference between a boundary and internal targets.

3. Map the full delivery chain

Dependency mapping should identify the resources needed to deliver each critical service. The FCA's operational-resilience materials identify people, processes, technology, facilities and information. APRA's CPS 230 includes people, technology, information, facilities and service providers. MAS materials emphasise critical business services, service-recovery time objectives and dependency mapping. These categories provide a useful starting taxonomy.

The map should reach the operating edge. A relationship manager may depend on identity and authority data, telephony, email, a client portal, a customer-record system, a payment callback process and local decision authority. A trader may depend on current positions, investment restrictions, pricing, market data, an order-management system, brokers, custodian connectivity and post-trade matching. A valuation process may depend on administrator files, custodian positions, data vendors, models, corporate actions, currency rates and approval.

Each dependency needs an owner, location, provider, contract, data source, access route, recovery capability and alternative. Mapping should show upstream and downstream links because a healthy application can contain stale data and a functioning provider can depend on an unavailable subcontractor.

The firm should reconcile diagrams to reality. Configuration records, invoices, access lists, contracts, data flows, interfaces and staff walkthroughs can reveal shadow applications, manual files and undocumented vendors. A service map is complete when a scenario can be traced from the client outcome to the control and recovery route.

Table 2. International operational-resilience design evidence

Market	Official material	Design discipline	Scope boundary
DIFC	DFSA GEN and PIB operational-risk materials	retain responsibility for outsourcing; maintain and test continuity; identify infrastructure dependencies	apply the current Rulebook and actual licence
United Kingdom	FCA operational-resilience framework and 2026 observations	important services, impact tolerances, full mapping, severe testing, communications and remediation	detailed rules apply to defined in-scope firms
European Union	DORA, Regulation (EU) 2022/2554	govern ICT risk, incidents, resilience testing and critical ICT third-party contracts	applies to listed categories of EU financial entities from 17 January 2025
Singapore	MAS 2022 BCM materials and outsourcing guidance	critical services, service-recovery objectives, mapping, concentration, testing and accountable outsourcing	legal and supervisory effect depends on the instrument and firm
Hong Kong	SFC 2021 operational-resilience report and circular	prevent, adapt, respond, recover and learn; address remote-working and provider risk	standards address licensed corporations within SFC scope
Australia	APRA CPS 230 in force from 1 July 2026	critical operations, tolerance levels, tested BCPs and material service-provider management	applies to APRA-regulated entities rather than every wealth firm
United States	SEC Regulation S-P amendments	incident response for customer information, service-provider oversight and affected-individual notification	applies to covered institutions under the amended rule
International	IOSCO Principles on Outsourcing	due diligence, contracts, monitoring, concentration, access, continuity and termination	principles require application through relevant local frameworks

The regimes are legally distinct; applicability depends on entity, activity, licence, product and facts.

4. Classify vendors by service consequence

A procurement label does not establish operational materiality. A low-spend data feed can stop valuation. A widely used cloud service can support several critical applications. A custodian bank can combine asset safekeeping, settlement, cash, reporting and records. The classification should therefore begin with service consequence.

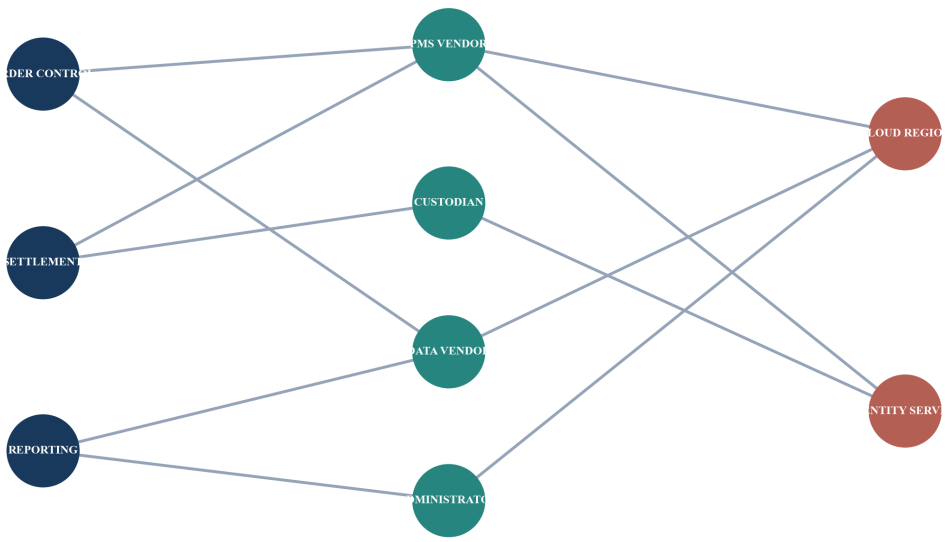
The firm can classify a provider as critical or material when its failure could push a critical service beyond tolerance, create material operational risk, compromise protected information or prevent compliance. The assessment should consider substitutability, concentration, data sensitivity, transaction authority, cross-border location, financial condition, sub-outsourcing and recovery capability.

A provider can support several services and create aggregate exposure. Multiple providers can rely on the same cloud, telecommunications carrier, identity platform or market-data source. This fourth-party concentration often remains invisible in a flat vendor list. Contract disclosures, architecture records, assurance reports and incident experience can help identify it.

Classification should produce a differentiated control plan. Critical providers require deeper due diligence, formal accountability, service and security obligations, access and audit rights where feasible, incident notification, continuity evidence, recovery tests, sub-outsourcing controls and an exit route. Lower-risk providers can receive proportionate review.

The provider register should be linked to the service map and reviewed when services, technology, ownership, subcontractors or locations change. Its purpose is to support decisions during normal operations, incident response and exit.

Figure 3. Vendor and fourth-party dependency network



Author framework. A shared upstream dependency can concentrate several apparently separate service arrangements.

Table 3. Dependency register

Dependency	Service role	Failure consequence	Recovery route	Decision evidence
portfolio system	positions, mandates, orders and approvals	decisions and orders cannot be supported	verified read-only extract and controlled manual order process	recovery test, position reconciliation, access list
custodian bank	custody, cash, settlement and reporting	asset access, settlement and records affected	alternate channels, named escalation and bounded manual instruction	contract, authority matrix, channel test, incident SLA
market data	prices, corporate actions and reference data	valuation, controls and reporting may be stale	approved secondary source with exception reconciliation	source hierarchy, licence, comparison test
administrator	books, NAV support and investor records	reporting and valuation evidence delayed	retained records and agreed recovery file	service description, file inventory, recovery test
identity provider	access and authentication	staff and clients may lose system access	break-glass access with independent control	privileged-access register and activation test
cloud region	hosting and storage	several applications can fail together	tested multi-zone or alternate processing design	architecture, configuration, restoration evidence

Fields should be reconciled to current architecture, contracts, access and test evidence.

5. Preserve accountability through outsourcing

Outsourcing changes the delivery chain and does not transfer the firm's accountability for regulated obligations or client outcomes. DFSA GEN materials state that an authorised firm remains responsible for compliance when it outsources a function and should conduct due diligence, supervise the outsourced function and manage provider failures. IOSCO's outsourcing principles similarly address accountability, due diligence, contracting, monitoring, concentration, regulator access, business continuity and termination.

The accountable executive should understand which obligations remain with the firm, which tasks the provider performs, which decisions can be delegated and which controls must remain independent. A responsibility matrix should cover data ownership, access, change, incident classification, notification, investigation, regulatory contact, client communication, remediation, subcontracting and termination.

The contract should describe service scope, performance, security, confidentiality, audit and assurance, records, data location, incident timing, continuity, testing, sub-outsourcing, cooperation, regulatory access and exit. Contract strength must be tested against operating evidence. A clause requiring recovery within two hours has limited value if the provider's architecture and most recent test cannot support it.

Concentration and bargaining power can limit contractual options. The control response can include architecture choices, retained capability, alternative data, portable records, escalation relationships and tested exit steps. The decision record should identify any gap between desired and obtainable terms and who accepted the residual risk.

Table 4. Material-provider control matrix

Control domain	Before appointment	During service	Failure or exit
service and accountability	define service outcome, roles and retained decisions	review service evidence and exceptions	invoke authority, workaround and escalation
financial and operational capacity	assess viability, resources, locations and concentration	monitor material change, incidents and capacity	evaluate continuity support and replacement viability
security and information	assess data, access, encryption, logging and response	review assurance, vulnerabilities and access	contain access, preserve evidence and recover data
continuity	reconcile provider recovery to service tolerance	participate in severe scenario tests	activate alternative, track backlog and communicate
subcontracting	identify critical fourth parties and approval rights	monitor material subcontractor changes	address shared failure and provider coordination
records and access	define ownership, format, retention and regulatory access	test retrieval and completeness	export, validate, retain and revoke access
termination	assess substitutability, transition time and cost	keep plans, inventories and alternatives current	execute transition, reconcile data and close obligations

Control depth should reflect service consequence, data, concentration, substitutability and applicable obligations.

6. Design severe but plausible scenarios

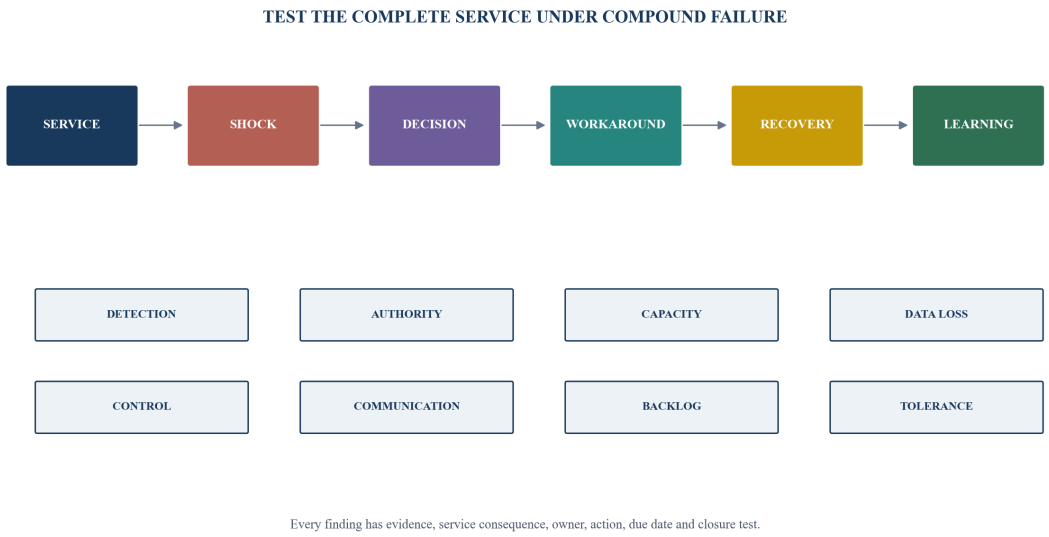
Scenario testing should challenge the complete service, not only a component. The scenario should specify initiating event, affected dependencies, timing, duration, data condition, client population, market context and complicating factors. It should be severe enough to expose decision and capacity limits while remaining plausible for the firm's operating model.

Relevant scenarios include ransomware with uncertain data integrity, identity-service failure, portfolio-system corruption, custodian channel outage, administrator file error, market-data contamination, telecommunications disruption, inaccessible premises, key-person absence, fraudulent payment instruction and the simultaneous failure of a provider and its recovery site.

The test should measure detection, assessment, authority, workaround, throughput, backlog, data loss, control exceptions, communications and recovery. Participants should work from realistic records and access. Tabletop discussion can test judgment and coordination. Technical recovery can test restoration. Simulation can test manual capacity. A mature programme combines them.

Testing should also challenge assumptions. A manual workaround may process ten instructions per hour while a volatile-market peak produces forty. A secondary data source may have different identifiers and prices. Staff named in a plan may lack current access. A vendor escalation number may reach a general support queue. Each finding should become owned remediation or an explicit tolerance decision.

Figure 4. Severe-scenario test architecture



Author framework. The test begins with a client service and measures decision quality, capacity and control through recovery.

7. Build controlled manual workarounds

Manual workarounds can preserve a service when technology or a provider fails. They can also remove automated controls and create new risks. A workable design defines which activity may continue, who can authorise it, which independent check remains, how volume is limited, how records are captured and how transactions are reconciled after recovery.

For client instructions, the firm may need alternative authenticated channels and a current authority record. For orders, it may need a verified position snapshot, mandate restrictions, dual approval and approved broker contacts. For payments, it may require enhanced callback, segregation, limits and bank confirmation. For valuation, it may use approved secondary sources and record each override.

Capacity should be measured. The number of trained people, transactions per hour, currencies, accounts, markets and exception types determines whether the workaround can keep the service inside tolerance. Staff should practise the process using current forms and access. Reliance on individual memory should be treated as a control weakness.

The recovery procedure should reconcile every manual action to restored systems. Duplicate orders, missed instructions and inconsistent timestamps are foreseeable risks. A controlled queue, unique reference, immutable record and independent reconciliation help manage the transition.

8. Treat data integrity as a recovery decision

Availability and integrity are separate. A restored system can contain corrupted positions, stale prices, incomplete client authorities or altered instructions. The recovery decision should establish which data set is authoritative, its time point, completeness, provenance and reconciliation status.

The service map should identify system of record, source feeds, calculations, copies, backups and archives. Recovery-point objectives should reflect the transaction and record obligations of the

service. Backup success should be supported by restoration and reconciliation evidence.

Cyber scenarios require containment and preservation. The firm should separate compromised credentials, protect logs, maintain decision records and coordinate specialists. Client or regulatory notification depends on applicable law and facts. The SEC's amended Regulation S-P requires covered institutions to maintain written incident-response policies addressing unauthorised access to or use of customer information, with service-provider oversight and individual-notification provisions within its scope.

Data recovery should be approved by the service and control owners, not only by technology. A portfolio service can resume when positions, restrictions, authorities and orders are sufficiently reconciled for the permitted activity. Other functions can remain restricted until their evidence is complete.

9. Plan for cyber and identity failure

Identity has become a critical shared dependency. Single sign-on, multifactor authentication, privileged access and client authentication can affect nearly every service. A single provider or administrator account can create concentration and escalation risk.

The firm should map workforce, privileged, service and client identities. It should identify which roles can approve orders, release payments, change bank data, modify restrictions, administer systems, restore backups and access confidential records. Joiner, mover and leaver controls should remain effective during disruption.

Break-glass access should be limited, independently controlled, monitored and tested. Offline or separately protected recovery credentials require strong physical and procedural safeguards. The process should record activation, activity and revocation.

The SFC's operational-resilience materials connect remote work, cybersecurity, information security and data privacy. Its more recent cyber communications also illustrate continuing risk from sophisticated attacks and service-provider dependencies. Firms should use current notices applicable to their licence and systems when updating scenarios.

10. Coordinate banks, custodians and market infrastructure

External asset managers often depend on custodian banks for assets, cash, settlement, statements, corporate actions and transaction channels. The relationship can also involve delegated authorities, client-specific mandates and multiple booking centres. Operational mapping should reach the exact account, channel and jurisdiction.

The firm should maintain current escalation contacts, authority matrices, standing settlement instructions, callback rules and alternative channels. It should test whether a disruption at the manager, bank or telecommunications provider changes access. The bank's general continuity statement does not prove that the manager's specific channel and accounts can recover within tolerance.

Market infrastructure adds time-bound dependencies. Cut-offs, settlement cycles, liquidity, margin and corporate-action deadlines can amplify delay. The incident team should know which obligations cannot wait for general recovery and which positions can be safely held.

Reconciliation remains central. Position, cash, order and confirmation records should be compared across manager, broker, custodian and administrator. During disruption, the firm should state which view is provisional and which activity is permitted.

11. Control communications as an operational service

Communication determines whether clients, staff, providers and regulators can act. The plan should define audiences, authority, channels, message owners, legal and compliance review, update frequency and record retention. It should anticipate failure of the primary channel.

Client messages should describe verified facts, service effect, permitted actions, available alternatives and next update. Technical detail should be included only when it helps the recipient make a decision. The firm should avoid unsupported recovery promises.

Staff need a common operating picture: affected services, tolerance clock, decision authority, manual permissions, security boundaries and escalation. Vendors need precise information about service consequence and required evidence. Regulators require notifications under the applicable framework and facts.

The FCA includes communications planning within operational resilience. APRA CPS 230 requires a BCP communications strategy for in-scope entities. These materials support the design principle that communication should be tested within the scenario rather than drafted after the event.

12. Establish incident command and decision rights

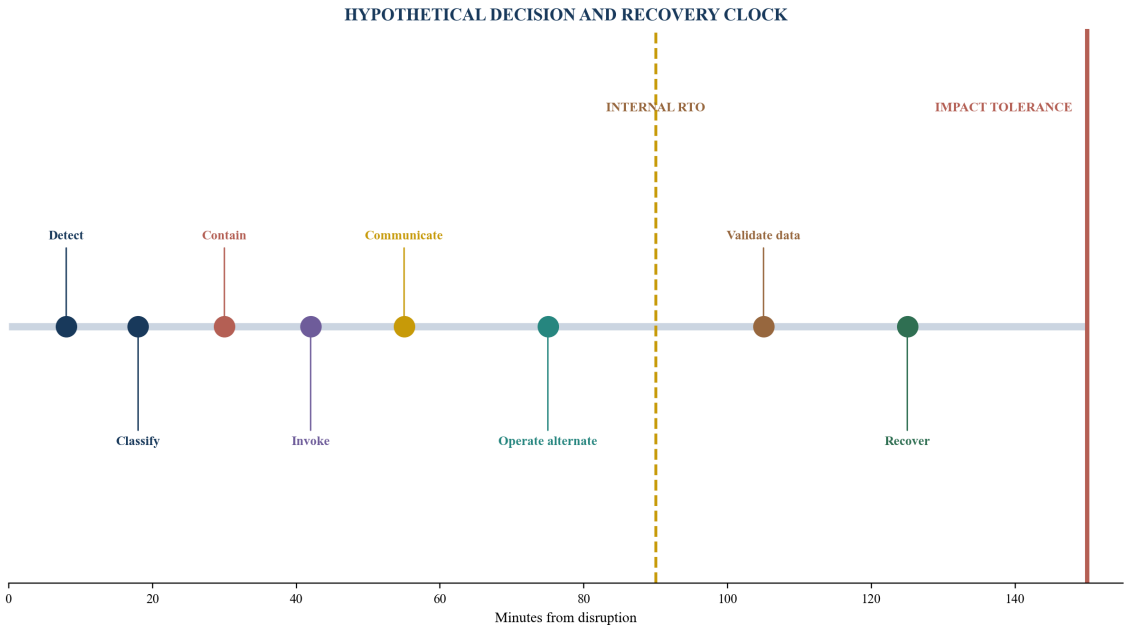
An incident team needs authority before the disruption. The framework should define who can declare an incident, restrict a service, invoke manual processing, contact clients, notify regulators, engage specialists, approve restored data and return to normal operation.

The service owner should present the client and operating consequence. Technology and providers should present system facts and recovery options. Information security should address containment and evidence. Compliance and legal specialists should assess applicable obligations. Communications should maintain consistent verified messages. Senior management should decide priorities and residual risk.

Decision logs should record time, evidence, alternatives, authority and rationale. The tolerance clock should remain visible. A technically attractive recovery can be rejected if data integrity is unresolved. A manual process can be stopped if volume or control exceptions exceed its limit.

The incident ends only after service, data and control reconciliation. Backlog, client impact, reporting, complaints, regulatory action, root-cause analysis and remediation can continue after systems return.

Figure 5. Incident decision timeline



Author framework. Minutes are hypothetical management assumptions for a severe service disruption.

13. Measure scenario performance

A test should produce decision evidence. Useful measures include time to detect, time to classify, time to invoke, time to communicate, time to restore, transactions completed, backlog, error rate, data loss, control exceptions and clients affected. The result should be compared with the approved tolerance and internal targets.

Passing within a time boundary does not cure a material control failure. A manual payment process that completes quickly with incomplete authentication should fail. A recovery that preserves controls but exceeds the impact tolerance should also fail. The scorecard should therefore separate time, capacity, integrity, control and communication.

Findings should identify the affected service and tolerance consequence. Each action requires an owner, due date, evidence and closure test. A document update is sufficient only when the finding was documentary. Access, architecture, data or capacity weaknesses require operating evidence.

The board should see trends across scenarios, real incidents and provider events. Repeated reliance on the same manual expert or extension should trigger a capacity decision.

Table 5. Hypothetical severe-scenario results

Scenario	Impact tolerance	Result	Control finding	Management action
portfolio-system outage during market stress	150 minutes; no mandate breach	service restored in 125 minutes	manual restriction check processed 55% of peak volume	train second team and automate verified offline extract
custodian channel outage	120 minutes; no duplicate order	alternate channel active in 70 minutes	two staff lacked current channel credentials	quarterly access validation and joint test
corrupted market-data feed	30 minutes to stop affected valuation	feed isolated in 16 minutes	secondary identifiers failed for 8% of positions	maintain reconciled identifier map
identity-provider failure	60 minutes for critical staff access	break-glass active in 48 minutes	approval log required manual consolidation	integrate immutable activation record
ransomware with uncertain portfolio data	no dealing until position integrity approved	verified read-only position at 95 minutes	client update missed approved 60-minute target	automate stakeholder clock and alternate channel
administrator failure before reporting date	one business day for validated recovery file	file available in six hours	recovery file omitted two corporate actions	add completeness rules and joint restoration test

All thresholds and results are hypothetical management assumptions created solely to demonstrate the method.

14. Make board information decision-useful

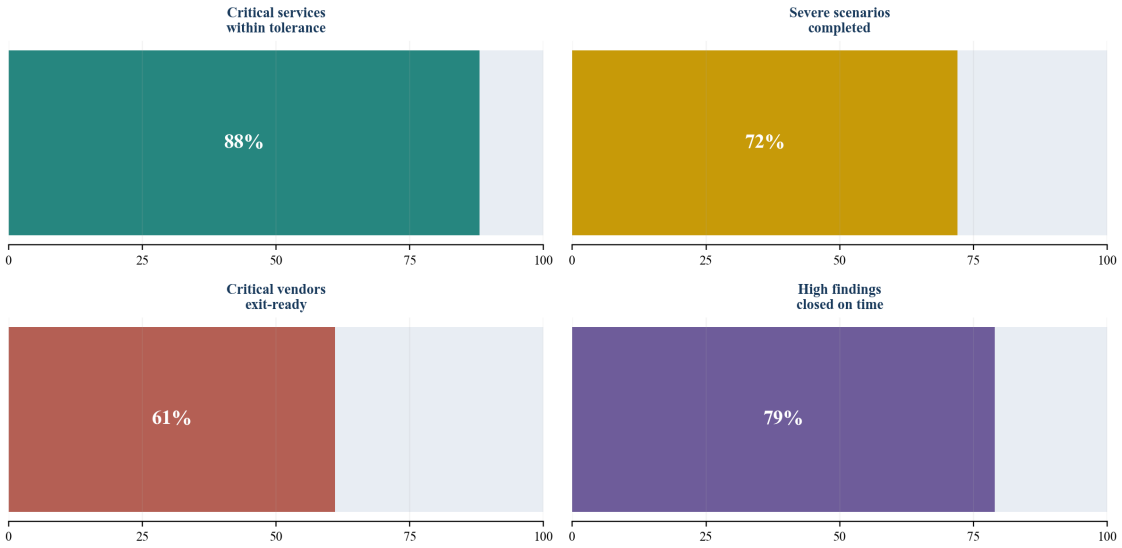
The board needs a service and risk view rather than a list of technology tickets. Reporting should show critical services, tolerance breaches, near misses, top dependencies, concentration, overdue provider actions, scenario coverage, material findings, incidents, control exceptions and remediation.

Metrics require context. A high proportion of systems tested can coexist with an untested client service. A provider may meet contractual uptime while repeated short failures cause missed market windows. A green recovery-time measure can hide data-integrity problems. The dashboard should link each measure to client outcome and tolerance.

The board should understand accepted gaps. These can include unavailable contract rights, concentrated providers, incomplete alternatives, manual-capacity limits and deferred remediation. Acceptance should identify evidence, consequence, duration, compensating control and accountable executive.

Changes in strategy, products, geographies, channels, volume and technology should trigger reassessment. Acquisition of another manager can introduce duplicate systems and hidden provider concentration. A new digital channel can create identity and data dependencies. Resilience is therefore part of change approval.

Figure 6. Operational-resilience board dashboard



Values are hypothetical management assumptions and illustrate decision-oriented reporting.

15. Keep the map current through change

Service maps decay when systems, teams, vendors, contracts and data flows change. The firm should connect resilience review to procurement, technology change, product approval, client-channel change, outsourcing, hiring, office moves, mergers and incident remediation.

A material change should identify affected services, tolerances, dependencies, tests and records. The change owner should demonstrate that the new design can remain within tolerance before full release. Temporary dual running or restricted volume can reduce transition risk when supported by evidence.

Provider changes require data and access planning. The firm should know which records must transfer, in which format, how completeness will be tested, when parallel service ends and how old access will be revoked. Exit can take longer than contractual notice because client, bank, data and regulatory dependencies must be reconciled.

Periodic certification can help owners confirm maps and alternatives, but evidence should drive closure. Staff interviews, configuration, transaction traces, test results and contract review provide stronger support than an unchecked affirmation.

16. Apply proportionality without losing the service

Independent wealth firms can have fewer people and less technology than large institutions. Proportionality should simplify governance and documentation while preserving the essential outcome: know the critical service, tolerance, dependencies, authority, workaround and evidence.

A smaller firm may assign several roles to one executive, use managed services and maintain concise maps. It still needs independent checks for sensitive decisions, current authorities, recoverable records and a credible response to key-person absence. Concentration can be more acute because one person or provider holds more operating knowledge.

The firm should prioritise services with direct client-asset, transaction, data and regulatory consequences. It can test the highest-consequence scenarios first, integrate reviews with existing committees and use provider assurance proportionately. Reliance on an assurance report should remain linked to scope, period, exceptions and the firm's own configuration.

Resource limits should appear in the risk decision. If the firm cannot operate a manual process at peak volume, it should restrict the service, add capability or accept a documented boundary through the applicable governance process.

17. Treat regional entities as one network and separate legal perimeter

International wealth firms can share technology, operations and vendors across legal entities. A disruption can cross the group while regulatory responsibilities, client contracts, records and notification rules remain local.

The service map should identify which legal entity owns the client relationship, employs decision makers, holds data, contracts with providers and performs each activity. Group support agreements should define service, authority, evidence, continuity and escalation. The local governing body should be able to understand and challenge reliance on group capability.

Scenario testing should include cross-border restrictions, time zones, data access and competing group priorities. A group recovery plan may prioritise a larger business, leaving a smaller entity outside its tolerance. Local retained capability and escalation therefore require evidence.

International comparison can improve design while local specialists determine applicable obligations. DORA, FCA, DFSA, MAS, SFC, APRA and SEC materials should not be collapsed into one legal checklist. Their recurring disciplines can support a common control taxonomy with jurisdiction-specific overlays.

18. Implement a 180-day resilience programme

During the first thirty days, define governance, scope and critical-service criteria. Identify client outcomes and provisional owners. Gather current continuity plans, vendor registers, architecture, contracts, incidents and test results. Select three services for pilot mapping.

During days 31 to 60, set tolerances and internal targets. Map people, process, technology, facility, information, bank, vendor and fourth-party dependencies. Reconcile the map through walkthroughs and transaction traces. Identify concentration and missing evidence.

During days 61 to 90, design severe scenarios and controlled workarounds. Test authority, access, capacity, data, communication and reconciliation. Record findings by service consequence and tolerance effect.

During days 91 to 120, remediate priority gaps and strengthen provider governance. Update contracts where feasible, establish alternatives, test recovery files, validate identity controls and build incident decision logs.

During days 121 to 150, expand the method to remaining critical services and legal entities. Connect maps to change, procurement, product and risk processes. Establish board metrics and escalation.

During days 151 to 180, run an integrated scenario with management, technology, providers, communications and control functions. Close material findings or record approved residual risk. Set the next testing cycle from current service risk.

Table 6. Operational-resilience implementation roadmap

Period	Primary work	Required output	Approval gate
days 1 to 30	governance, scope, service definition and pilots	service inventory, ownership and evidence baseline	approve criteria and pilot services
days 31 to 60	tolerance and dependency mapping	tolerance record, maps and gap register	approve boundaries and priority gaps
days 61 to 90	scenario and workaround testing	measured results, failures and remediation	decide restrictions and urgent investment
days 91 to 120	provider, data, identity and incident controls	updated control evidence and tested alternatives	accept, remediate or exit material dependencies
days 121 to 150	scale across services and entities	integrated register, change gates and dashboard	approve reporting and accountability
days 151 to 180	integrated simulation and closure	board pack, residual risks and next test cycle	approve operating state and continuing actions

Timing is an illustrative management sequence and should be adapted to scope, evidence and risk.

19. Use incident evidence to improve the operating model

Real incidents provide evidence that exercises cannot fully reproduce. The post-incident review should reconstruct service effect, detection, decisions, communications, recovery, backlog and control. It should distinguish initiating cause from the conditions that amplified impact.

The review should compare actual performance with tolerance and internal targets. It should identify stale maps, unknown dependencies, unavailable people, weak access, missing data, insufficient manual capacity and provider coordination gaps. Complaints and client conversations can reveal effects that system metrics missed.

Actions should change capability. Rewriting a plan does not resolve a restoration failure. A provider issue can require contract, architecture, monitoring or exit work. A decision delay can require authority and evidence changes. Closure should be tested.

Lessons should be shared across services and entities where relevant. A failure in one data feed can reveal a common dependency across valuation, reporting and risk. A missed client update can reveal a shared communication weakness. The board should see repeated themes and structural decisions.

20. Make resilience part of the client proposition

Clients entrust an external asset manager with decisions, information and access that remain important during stress. A credible resilience capability supports that relationship. The firm should be able to explain, within appropriate confidentiality boundaries, how it governs critical services, third parties, data, incidents and recovery.

Due diligence from clients, banks, insurers and regulators should be answered with attributable evidence. Service maps, tolerance methodology, test results, remediation governance, provider

controls and incident records demonstrate operating capability more clearly than broad assurances.

The commercial proposition should remain accurate. No operating model can promise uninterrupted service under every event. The firm can describe approved boundaries, tested alternatives and accountability. It can disclose material limitations through the appropriate process.

Operational resilience also supports growth. A mapped service can be evaluated before entering a new market, adding a custodian, launching a product or acquiring a manager. The firm can identify which dependency or capacity investment is required before scale creates unacceptable risk.

Conclusion

Operational resilience for an external asset manager begins with the service delivered to the client. The firm defines the outcome, sets an impact tolerance, maps the complete delivery chain and tests whether people, process, technology, information, banks and vendors can keep the service within that boundary.

Accountability remains with the firm when tasks are outsourced. Vendor control therefore extends from due diligence and contracts to concentration, fourth parties, recoverability, incident cooperation and exit. Technical recovery becomes a business decision when data integrity, authority, client impact and control are considered together.

International official materials use different legal routes and scopes. They repeatedly support service identification, tolerances, full dependency mapping, severe testing, provider oversight, communications, governance and learning. An international wealth firm can use those disciplines in a common operating model while maintaining jurisdiction-specific legal analysis.

The governing question is direct: can the firm demonstrate, with current evidence, how each critical client service will remain within tolerance through a severe disruption, which person has authority, which dependencies matter, which alternative works and which event requires restriction? A complete answer converts continuity documentation into operating capability.

References

[1] Dubai Financial Services Authority, GEN 5.3 Outsourcing, https://dfsaen.thomsonreuters.com/rulebook/annex-d-general-gen

[2] Dubai Financial Services Authority, PIB 6 Operational Risk, https://dfsaen.thomsonreuters.com/rulebook/pib-6-operational-risk

[3] Dubai Financial Services Authority, Cyber Risk Supervision Summary, https://www.dfsa.ae/what-we-do/supervision/cyber-risk-supervision/summary

[4] UK Financial Conduct Authority, Operational resilience, updated 14 July 2026, https://www.fca.org.uk/firms/operational-resilience

[5] UK Financial Conduct Authority, Operational resilience insights and observations, https://www.fca.org.uk/firms/operational-resilience/insights-observations

[6] UK Financial Conduct Authority, Operational resilience insights and observations one year on, 27 March 2026, https://www.fca.org.uk/publications/good-and-poor-practice/operational-resilience-insights-observations-one-year

[7] European Union, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32022R2554

[8] Monetary Authority of Singapore, Response to Feedback Received on Proposed Revisions to Guidelines on Business Continuity Management, June 2022, https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/bcm-guidelines/response-to-feedback-received_bcmg-second-consultation-paper-2.pdf

[9] Monetary Authority of Singapore, Guidelines on Outsourcing for Financial Institutions Other Than Banks, https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/bd/guidelines-on-outsourcing/guidelines-on-outsourcing---financial-institutions-other-than-banks.pdf

[10] Securities and Futures Commission of Hong Kong, Report on Operational Resilience and Remote Working Arrangements, October 2021, https://www.sfc.hk/-/media/EN/files/COM/Reports-and-surveys/Report_Operational-resilience-and-remote-working-arrangements_Oct-2021_EN.pdf

[11] Securities and Futures Commission of Hong Kong, Circular on Operational Resilience and Remote Working, 4 October 2021, https://apps.sfc.hk/edistributionWeb/api/circular/list-content/circular/intermediaries/supervision/doc?lang=EN&refNo=21EC41

[12] Australian Prudential Regulation Authority, CPS 230 Operational Risk Management, in force 1 July 2026, https://www.apra.gov.au/standards/cps-230

[13] United States Securities and Exchange Commission, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, https://www.sec.gov/rules-regulations/2024/06/s7-05-23

[14] International Organization of Securities Commissions, Principles on Outsourcing, October 2021, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf

About the Author

Chennakeshav Adya is an independent researcher and Managing Partner of Matchpoint Partners. His work examines strategy, capital formation, valuation, transactions and operating execution across private and public markets.